Master Thesis

Linnik's ergodic method and the distribution of integer points on discrete spheres

Théo Untrau

supervised by : Guillaume Ricotta

2nd semester 2019/2020

Introduction

This document is my master thesis, it has been written during the second semester of the year 2019/2020. It consists of an exposition of some results of the paper [EMV10], but we also try to give details on the proofs of some classical facts that are just quoted briefly in the latter. The article describes an ergodic method due to Linnik, which is used to answer the question of the equidistribution of integer points on spheres (under some conditions). More precisely, if d is a given positive integer, the 2-dimensional sphere of radius $\sqrt{d}$ is the following subset of $\mathbf{R}^3$:

$$\left\{(x,y,z) \in \mathbf{R}^3 \mid x^2+y^2+z^2 = d\right\}$$

We denote by $\mathscr{R}_3(d)$ the set of points where the three coordinates are integers :

$$\mathscr{R}_3(d) := \left\{(x,y,z) \in \mathbf{Z}^3 \mid x^2+y^2+z^2 = d\right\}$$

There are several problems about $\mathscr{R}_3(d)$ that are simply stated but remained unsolved for a long time. For example, in increasing order of fineness, one may ask :

(1) When is $\mathscr{R}_3(d)$ non-empty ? In other words : which integers can be written as a sum of three squares of integers ?

(2) If non-empty, how large does $\mathscr{R}_3(d)$ get ?

(3) If $|\mathscr{R}_3(d)|$ gets large as d goes to infinity, how are the points of $\mathscr{R}_3(d)$ distributed on the sphere of radius $\sqrt{d}$?

In this document, we answer question (1) in an almost self-contained proof, we just quote without proof the Hasse-Minkowski local-global principle, as well as some known facts on p-adic fields. The precise answer to question (1) is given by theorem 3.4.2, and states that the integers that can be written as a sum of three squares of integers are those which are not of the form $4^a(8b+7)$ for some $a, b \in \mathbf{N}$. Such integers will be called *admissible*.
We also give a lower bound to answer question (2), relying on Siegel's theorem on the value at 1 of L-functions attached to real primitive Dirichlet characters. The conclusion is that for every $\varepsilon > 0$, there exists a constant $C(\varepsilon)$, depending only on ε, such that for any $d \geqslant 2$ admissible and square-free,

$$|\mathscr{R}_3(d)| \geqslant C(\varepsilon) d^{\frac{1}{2}-\varepsilon}$$

(see section 4.4).
Finally, following [EMV10], we discuss a discrete analogue of question (3), namely the question of how the points of $\mathscr{R}_3(d)$ get distributed in the discrete sphere modulo q (under some conditions on the integer q) :

$$\mathscr{R}_3(d,q) := \left\{(\overline{x},\overline{y},\overline{z}) \in (\mathbf{Z}/q\mathbf{Z})^3 \,,\ \overline{x}^2+\overline{y}^2+\overline{z}^2 = \overline{d}\right\}$$

It is in the study of this last question that we use an ergodic approach due to Linnik.

Acknowledgements

I would like to thank some of my friends for their help on this master thesis :

Thank you David for the time you spent on my LaTeX related questions.
Thanks Émilie for giving me the code of your title page and for reading the first section, it was really helpful to have your point of view on the readability of these preliminaries. The aim was to make this subject more accessible, even for people with almost no background in number theory, so it was important for me to have your perception.
Thank you Bastien for the helpful discussion on the proof of corollary 4.1.6.
Thanks Francesco for sharing with me what you were learning about real quadratic fields, while I was studying the imaginary case, and for our discussions on Dirichlet class number formula and the upper bound for $|L(1,\chi)|$. It was great to have someone whose subject intersected mine non-trivially.
Finally, I cannot count the number of times Tibo and Thomas helped me, even if we are now studying different fields of mathematics.

I am also grateful to Alexandre, PhD student in analytic number theory, who took an interest in my subject, and directed me to books I did not know, which helped me a lot for the part on the connection between quadratic forms and ideal class group.

I would like to thank Céline Michelot, for handling the internship agreement between the University of Bordeaux and... the University of Bordeaux (!)

Finally, I wish to thank my advisor, Guillaume Ricotta, for giving me this subject which mixes different areas of mathematics that have attracted me for some time, and for his involvement in keeping in touch in spite of the lockdown.

Comments on the plan of this document

Since the first two sections do not seem to be immediately related to our questions, let us explain briefly the aim of each section and when it is used to answer questions (1), (2) and (3).

- In section 1 we collect some results from number theory that are usually taught in a graduate course on the subject. The aim is to introduce notations that are used a lot in the following sections. The statements which are really important to have in mind when reading the remainder of this master thesis are :
  - The fact that the ring of integers of a number field K is a Dedekind ring, denoted by $\mathcal{O}_K$, and the definition of the class group which follows from this fact. The class group is denoted by $\mathrm{Cl}(\mathcal{O}_K)$.
  - The fact that $\mathrm{Cl}(\mathcal{O}_K)$ is a finite abelian group. Its cardinality is called the class number of the field K.
  - The definitions and statements relative to the norm of an ideal in the ring of integers of a number field.
- Section 2 deals with Dirichlet class number formula for imaginary quadratic fields. This formula reveals a link between the class number of an imaginary quadratic field $K = \mathbf{Q}(\sqrt{-d})$ and the value at 1 of the L-function attached to a certain Dirichlet character χ_D (where D is the discriminant of the field K). Although it can be proved completely in a modern way, using only the theory of ideals, we chose to develop the connection with representations of integers by binary quadratic forms. Indeed, it is interesting from an historical perspective to see how this formula was proved at a time where the notion of ideal had not emerged yet.
- In section 3, we answer question (1) from the introduction. Some congruence conditions modulo 8 allow us to exclude some integers from the list of those which are a sum of three squares of integers. Then, to prove that the remaining integers are indeed a sum of three squares, we proceed in several steps. If d is a positive integer not of the form $4^a(8b+7)$ for some $a, b \in \mathbf{N}$,
  - we use Newton's lemma to write d as a sum of three squares in every $\mathbf{Q}_p$ for p prime,
  - then we use the Hasse-Minkowski local-global principle to find a representation of d as a sum of three squares of rational numbers,
  - and finally, we use the fact that the ring $\mathrm{B}(\mathbf{Z})$ of Hurwitz quaternions is left-euclidean to find a representation of d as a sum of three squares of rational integers.

  This is why the beginning of section 3 consists of an exposition of some generalities and arithmetic properties of quaternions. They are a powerful tool to deal with questions related to sums of three or four squares.
- Section 4 is central in this master thesis. This is where we introduce an action of the class group of $\mathbf{Q}(\sqrt{-d})$ on $\widetilde{\mathscr{R}_3}(d)^+$ (which is roughly the set of orbits for the action of $\mathrm{SO}_3(\mathbf{Z})$ on $\mathscr{R}_3(d)$ by left multiplication. These notations are introduced with more details in the core of the text). We prove that (at least when $d \equiv 1$ or $2 \bmod 4$) this action is free and transitive, and this shows that there is an explicit relation connecting $|\mathscr{R}_3(d)|$ and the class number of $\mathbf{Q}(\sqrt{-d})$. By Dirichlet class number formula (which is the subject of section 2), we can express it as the value at 1 of some L-function attached to a real primitive Dirichlet character. Then we quote without proof a famous theorem by Siegel which gives a lower bound for this value. This gives us an estimate of $|\mathscr{R}_3(d)|$ as announced in the introduction. In particular, the size of $\mathscr{R}_3(d)$ goes to infinity as d goes to infinity, so it is natural to wonder how the points get distributed on the sphere of radius $\sqrt{d}$.
- In section 5, we focus for technical reasons on a discrete analogue of this question : the distribution of the points of $\mathscr{R}_3(d)$ in the sphere modulo q denoted by $\mathscr{R}_3(d, q)$ (see the introduction). We use Linnik's ergodic method to prove that they get equidistributed.

Contents

1. Preliminaries

In this section, we give a quick review of some classical results in algebraic number theory that will be used throughout this thesis. The goal is to set the notations and to explain what will be considered as "well known" in this document. Most of these results are stated without proofs, I personally learned them in the notes [Bri20], but I will also refer to some books that contain the same statements. In this section, all the rings we consider are commutative.

1.1 Some notations and conventions

If A is a ring, $A^\times$ will always denote the set of invertible elements of A, also called the units of A. An element $a \in A$ is in $A^\times$ if and only if there exists $b \in A$ such that $ab = 1_A$ (since we are only considering commutative rings in this section, this also means that $ba = 1_A$).
Two elements $x, y \in A$ are said to be associated if there exists $u \in A^\times$ such that $y = ux$. We denote it by $x \sim y$.
We also introduce the convenient notations UFD and PID :

Definition 1.1.1. *A principal ideal domain, denoted by PID, is an integral domain A in which every ideal is principal, that is : of the form $I = xA$ for some $x \in A$.*
A unique factorization domain, denoted by UFD, is an integral domain A such that :

(i) *every non-zero element $x \in A$ can be written as a product $x = up_1 \dots p_r$ where $u \in A^\times$ and the p_i's are irreducible elements of A.*

(ii) *This decomposition is unique up to permutation and units : if $x = up_1 \dots p_r = vq_1 \dots q_s$, then $r = s$ and there exists $\sigma \in \mathfrak{S}_r$ such that for all $i \in \{1, \dots, r\}$, $q_i \sim p_{\sigma(i)}$.*

1.2 Integral extensions

First, we recall the definition of an algebra over a ring A.

Definition 1.2.1. *Let A be a ring. An A-algebra is just a ring homomorphism $\varphi\colon A \to B$. The ring B is naturally endowed with a structure of A-module : for all $a \in A$ and $b \in B$, the product $a \cdot b$ is given by $\varphi(a)b$.*

Now, if A is a ring and $\varphi\colon A \to B$ is an A-algebra, we define the notion of an integral element of B over A. An element $b \in B$ is said to be integral over A if there exists a monic polynomial P with coefficients in A such that $P(b) = 0$. For example, $\mathbf{Q}(\sqrt{2})$ is a $\mathbf{Z}$-algebra (the ring homomorphism being just the natural inclusion), and $\sqrt{2}$ is integral over $\mathbf{Z}$ since the polynomial $X^2 - 2$ is monic, with coefficients in $\mathbf{Z}$, and vanishes at $\sqrt{2}$.
The set of elements in B that are integral over A is a sub-A-algebra of B. It is called the *integral closure* of A inside B. We say that B is integral over A if all the elements of B are integral over A (i.e. if the integral closure of A in B is exactly B). When A is an integral domain, the integral closure of A (without specifying in which A-algebra) always refers to the integral closure of A in its fraction field.
The following proposition will be useful in the study of extensions of Dedekind rings, since it roughly states that the maximality of an ideal $\mathfrak{p}$ in A is equivalent to the maximality of any prime ideal $\mathfrak{P} \subseteq B$ that lies over $\mathfrak{p}$ (see the proof of proposition 1.5.6).

Proposition 1.2.2. *Let $\varphi\colon A \to B$ be an A-algebra. Suppose that B is an integral domain, that φ is injective, and that B is integral over A. In other words, we say that φ is an integral inclusion between domains. Then A is a field if and only if B is a field.*

Definition 1.2.3. *Let A be an integral domain, and K its fraction field. We say that A is integrally closed if it is integrally closed in K, that is : the only elements of K that are integral over A are the elements of A.*

An important (but not difficult) proposition is the following :

Proposition 1.2.4. *UFD's are integrally closed. In particular, PID's are integrally closed.*

Proposition 1.2.5. *Let A be an integral domain, $K := \mathrm{Frac}(A)$, and L/K an algebraic field extension. Denote by B the integral closure of A in L. If $x \in L$, there exists $a \in A \setminus \{0\}$ such that $ax \in B$. So $L = (A \setminus \{0\})^{-1} B$, which implies that $L = \mathrm{Frac}(B)$. Moreover, B is integrally closed.*

This proposition is really elementary, but will play a role when we will check that the ring of integers of a number field is a Dedekind domain. Finally, the following classical result allows us to justify easily that some element of B is not integral over A.

Proposition 1.2.6. *Assume that A is integrally closed, let $K = \mathrm{Frac}(A)$ and L/K be an algebraic extension. An element of L is integral over A if and only if its minimal polynomial over K has coefficients in A.*

Taking again $A = \mathbf{Z}$ (which is integrally closed, because $\mathbf{Z}$ is a PID), and $L = \mathbf{Q}(\sqrt{2})$, we can conclude that $\frac{1}{\sqrt{2}}$ is not integral over $\mathbf{Z}$, because its minimal polynomial over $\mathbf{Q}$ is $X^2 - \frac{1}{2}$: it is not in $\mathbf{Z}[X]$.

1.3 Traces and norms

Let A be a ring, and M a free A-module of finite rank n. Let $\mathcal{B} = (e_1, \ldots, e_n)$ be a basis of M over A. If $f \in \mathrm{End}_A(M)$ (i.e. f is an A-linear map from M to M), we can write the matrix of f in the basis $\mathcal{B}$: $\mathrm{Mat}_{\mathcal{B}}(f) = (a_{i,j})_{1 \leqslant i,j \leqslant n}$. Then we define :

$$\mathrm{Tr}(f) := \mathrm{Tr}\left((a_{i,j})_{1 \leqslant i,j \leqslant n}\right) = \sum_{i=1}^{n} a_{i,i} \ \in A, \quad \text{and} \ \det(f) := \det\left((a_{i,j})_{1 \leqslant i,j \leqslant n}\right) \in A.$$

These elements of A depend only on f and not on the choice of a basis of the A-module M.

Now, let B be a free A-algebra of rank n over A (i.e. it is free of rank n when we see B as an A-module for the natural A-module structure coming from the definition of an A-algebra). For all x in B, the multiplication by x :

$$\begin{array}{rccc} m_x & : & B & \to & B \\ & & b & \mapsto & xb \end{array}$$

belongs to $\mathrm{End}_A(B)$, so we can consider $\mathrm{Tr}(m_x)$ and $\det(m_x)$ as above.

Definition 1.3.1. *With the notations above, we define $\mathrm{Tr}_{B/A}(x) := \mathrm{Tr}(m_x)$ and $\mathrm{N}_{B/A}(x) := \det(m_x)$. They are called the trace of x and the norm of x.*

The following properties follow easily from the definition : for all $x, y \in B$, for all $a \in A$:

- $\mathrm{N}_{B/A}(xy) = \mathrm{N}_{B/A}(x)\mathrm{N}_{B/A}(y)$
- $\mathrm{Tr}_{B/A}(ax + y) = a\mathrm{Tr}_{B/A}(x) + \mathrm{Tr}_{B/A}(y)$
- $\mathrm{N}_{B/A}(a) = a^n$
- $\mathrm{Tr}_{B/A}(a) = na$

Note that if L/K is a finite field extension, L is a K-algebra, of finite dimension as a K-vector space, so we recover the notion of traces and norms of elements in field extensions. Let us state a few classical results in this context. Recall that a field extension L/K is said to be separable when it is algebraic and every element of L has its minimal polynomial over K which has only roots of multiplicity one in some algebraic closure of K.

Proposition 1.3.2. *Let L/K be a finite and separable field extension, of degree n. Let $\overline{K}$ be an algebraic closure of K. There are exactly n homomorphisms of K-algebras from L to $\overline{K}$: $\mathrm{Hom}_{K\text{-alg}}(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$. Then for all $x \in L$, we have :*

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x) \quad \textit{and} \quad \mathrm{N}_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$$

But more generally, if we do not assume that L/K is separable, we still have an expression of $\mathrm{Tr}_{L/K}(x)$ and $\mathrm{N}_{L/K}(x)$ in terms of the conjugates of x. Indeed, if L/K is a finite extension, $x \in L$, and $x_1, \dots, x_m$ are the conjugates of x over K (i.e. the roots (counted with multiplicities) of the minimal polynomial of x over K, in some algebraic closure $\overline{K}$), then :

$$\mathrm{Tr}_{L/K}(x) = [L : K(x)] \sum_{i=1}^{m} x_i \quad \text{and} \quad \mathrm{N}_{L/K}(x) = \left(\prod_{i=1}^{m} x_i \right)^{[L:K(x)]} \tag{1}$$

Complete proofs of the preceding formulas for traces and norms in field extensions can be found in [Goz10].

The last part of the following proposition will be useful in the study of units in the ring of integers of a number field.

Proposition 1.3.3. *Let A be an integrally closed domain, K its fraction field, L/K a finite extension, and B the integral closure of A in L. If $b \in B$, then $\mathrm{N}_{L/K}(b) \in A$, $\mathrm{Tr}_{L/K}(b) \in A$. Moreover, $b \in B^\times$ if and only if $\mathrm{N}_{L/K}(b) \in A^\times$.*

Proof. Since $b \in B$, it is integral over A, so its minimal polynomial has coefficients in A by proposition 1.2.6. Therefore, the conjugates of b are also integral over B, because by definition, they share the same minimal polynomial. Using the formulas given in (1) for the trace and norm, and the fact that B is a subring of L, we deduce the first part of the statement. For the second part, let us take $b \in B$, and denote by $P = X^d + a_1 X^{d-1} + \cdots + a_{d-1} X + a_d \in A[X]$ its minimal polynomial over K. Then the minimal polynomial of b^{-1} over K is $X^d + \frac{a_{d-1}}{a_d} X^{d-1} + \cdots + \frac{a_1}{a_d} X + \frac{1}{a_d}$. Thus, by proposition 1.2.6, $b^{-1} \in B$ if and only if $a_d \in A^\times$. But if we look again at the expression of the norm given in (1), we see that $\mathrm{N}_{L/K}(b) = \left((-1)^d a_d\right)^{[L:K(b)]}$, which implies that $a_d \in A^\times$ if and only if $\mathrm{N}_{L/K}(b) \in A^\times$. This concludes the proof. □

Finally, let us stress that the behaviour of the trace map is very different depending on the separability of the field extension. In fact, one can show that when L/K is not separable, the trace map $\mathrm{Tr}_{L/K}$ is zero, whereas when L/K is separable, the pairing

$$\begin{array}{ccc} L \times L & \to & K \\ (x, y) & \mapsto & \mathrm{Tr}_{L/K}(xy) \end{array}$$

is non-degenerate. This follows from Dedekind's independence theorem.

This last fact is very useful because it gives rise to the notion of dual basis with respect to the trace map. If $(x_1, \dots, x_n)$ is a basis of L/K, there exists a unique basis $(y_1, \dots, y_n)$ of L/K such that for all $1 \leqslant i, j \leqslant n$, $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{i,j}$.
This notion of a dual basis plays a central role to prove the following proposition :

Proposition 1.3.4. *Let A be an integrally closed domain, $K := \mathrm{Frac}(A)$ and L/K a finite separable field extension. Let B denote the integral closure of A in L. Then B contains a basis of L/K and it is a sub-A-module of a free A-module of rank $[L : K]$ contained in L.*

This statement implies the following result, which is very useful in number theory (when $A = \mathbf{Z}$ and $B = \mathcal{O}_K$ is the ring of integers of a number field).

Corollary 1.3.5. *Under the assumptions of the preceding proposition,*

(i) *If A is noetherian, then B is a finite A-algebra (i.e. it is finitely generated as an A-module). In particular, B is also noetherian.*

(ii) *If A is a PID, then B is a free A-module of rank $[L : K]$.*

1.4 Discriminants

Definition 1.4.1. *Let B be a free A-algebra of rank n, and let $(x_1, \dots, x_n) \in B^n$. We define the discriminant of $(x_1, \dots, x_n)$ as follows :*

$$\mathrm{D}(x_1, \dots, x_n) := \det\left((\mathrm{Tr}_{B/A}(x_i x_j))_{1 \leqslant i,j \leqslant n}\right) \in A.$$

If $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in B^n$ and $M \in \mathcal{M}_n(A)$, and if we denote $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, then

$$\mathrm{D}(y_1, \dots, y_n) = \det(M)^2 \mathrm{D}(x_1, \dots, x_n).$$

As a consequence, if $\det(M) \in A^\times$, $\mathrm{D}(x_1, \dots, x_n)A = \mathrm{D}(y_1, \dots, y_n)A$. In particular, if $(x_1, \dots, x_n)$ and $(y_1, \dots, y_n)$ are two bases of B/A, then there is a matrix $M \in \mathrm{GL}_n(A)$ such that

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

so the ideals $\mathrm{D}(x_1, \dots, x_n)A$ and $\mathrm{D}(y_1, \dots, y_n)A$ are equal.

Definition 1.4.2. *We denote by $\mathfrak{d}_{B/A}$ the ideal $\mathrm{D}(x_1, \dots, x_n)A$, where $(x_1, \dots, x_n)$ is any basis of B/A. We call this ideal the discriminant of B/A.*

Proposition 1.4.3. *Under the assumptions of definition 1.4.1, assume moreover that A is a UFD. Let $(x_1, \dots, x_n) \in B^n$. If $\mathrm{D}(x_1, \dots, x_n) \in A \setminus \{0\}$ is square-free, then $x_1, \dots, x_n$ is a basis of B over A.*

Note that in the context of number fields, A will be $\mathbf{Z}$, which is a UFD, and B will be $\mathcal{O}_K$ (the integral closure of $\mathbf{Z}$ in the number field K), so that this proposition will apply. Thus, the discriminant can be used to detect bases of $\mathcal{O}_K$ as a $\mathbf{Z}$-module.
Finally, let us give a characterization of the discriminant in a field extension, in terms of field automorphisms. This can be useful to compute discriminants in quadratic fields for examples (because in this case, the Galois group is easy to describe).

Proposition 1.4.4. *Let L/K be a finite and separable extension of degree n, and let $\overline{K}$ be an algebraic closure of K. Write $\mathrm{Hom}_{K\text{-alg}}(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$. Then for any basis $x_1, \dots, x_n$ of L/K, we have that*

$$\mathrm{D}(x_1, \dots x_n) = \left(\det\left((\sigma_i(x_j))_{1 \leqslant i,j \leqslant n}\right)\right)^2 \neq 0$$

1.5 Dedekind rings

We now recall some of the main results about Dedekind rings. These rings play a central role in number theory, since when we take the integral closure of $\mathbf{Z}$ in some number field, we don't always get a UFD (and this is the reason why some early attemps to prove Fermat's last theorem failed). However, we always get a Dedekind domain, which is not exactly a UFD, but where we also have a nice unique factorization property, at the level of ideals instead of elements.

Definition 1.5.1. *Let A be an integral domain. We say that A is a Dedekind ring if :*

(i) *A is not a field*

(ii) *A is noetherian*

(iii) *A is integrally closed*

(iv) *Every non-zero prime ideal in A is maximal.*

PID's that are not fields are Dedekind rings, but the converse is not true.
One of the main results about Dedekind rings is the following, that tells us that we have unique factorization at the level of ideals.

Theorem 1.5.2. *Let A be a Dedekind ring, and let I be a non-zero ideal of A. There exist pairwise distinct non-zero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, and positive integers $\alpha_1, \dots, \alpha_r$ such that :*

$$I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$$

This factorization is unique up to the order of factors, and the primes that appear in the decomposition are exactly the prime ideals of A that contain I.

In order to define the class group of a Dedekind ring, we need to introduce the notion of a fractional ideal.

Definition 1.5.3. *Let A be an integral domain, and K its fraction field. A fractional ideal of A is a sub-A-module I of K such that there exists $d \in A \setminus \{0\}$ such that $I \subseteq d^{-1}A$.*

We remark that a fractional ideal is nothing but a subset of K of the form $d^{-1}\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq A$. Since fractional ideals appear a lot in the theory of Dedekind rings, we sometimes just call them ideals, and say *integral* ideals when we want to stress that we speak about usual ideals of A.

We define operations on fractional ideals as it is usually done in the case of ideals :

- If I and J are two fractional ideals, we define $I+J$ as the sub-A-module of K generated by $I \cup J$.
- We define their product IJ as the sub-A-module of K generated by elements of the form xy, for $x \in I$ and $y \in J$.

It is easy to verify that IJ and $I+J$ are still fractional ideals. A simple example of a fractional ideal is the sub-A-module of K generated by an element $x \in K$: $I = xA$. Such ideals are called the principal fractional ideals.

When A is an integral domain, we will denote by $\mathrm{Fr}(A)$ the set of non-zero fractional ideals of A, and by $\mathrm{Princ}(A)$ the set of non-zero principal fractional ideals.

When I is a fractional ideal, we also define I^{-1} as $\{x \in K \mid xI \subseteq A\}$, and we say that I is invertible when the inclusion $II^{-1} \subseteq A$ is an equality. For example, a principal fractional ideal xA (for some $x \in K^\times$) is invertible, and its inverse is given by $x^{-1}A$.
A corollary of the unique factorization at the level of ideals in a Dedekind ring is the following :

Corollary 1.5.4. *Let A be a Dedekind ring. Then any non-zero fractional ideal of A is invertible.*

Using this corollary, we deduce that $\mathrm{Fr}(A)$ can be given a group structure :

$$\begin{array}{ccc} \mathrm{Fr}(A) \times \mathrm{Fr}(A) & \to & \mathrm{Fr}(A) \\ (I, J) & \mapsto & IJ \end{array}$$

where the unit element is A and the inverse of an ideal I is the ideal I^{-1} defined above. This group is abelian, and the set $\mathrm{Princ}(A)$ forms a subgroup.

Definition 1.5.5. *When A is a Dedekind ring, we define its ideal class group as the quotient*

$$\mathrm{Cl}(A) := \mathrm{Fr}(A)/\mathrm{Princ}(A).$$

Finally, to finish this section, let us recall the vocabulary of ramification in extensions of Dedekind domains.

Proposition 1.5.6. *Let A be a Dedekind ring, $K = \mathrm{Frac}(A)$, and L/K a finite and separable field extension. Denote by B the integral closure of A in L. Then B is still a Dedekind ring.*

Proof. The fact that B is noetherian comes from corollary 1.3.5 (i). It is also integrally closed by proposition 1.2.5. Finally, if $\mathfrak{P} \subseteq B$ is a non-zero prime ideal, then $\mathfrak{P} \cap A =: \mathfrak{p}$ is a non-zero prime ideal of A. Since A is a Dedekind ring, $\mathfrak{p}$ is maximal, hence $A/\mathfrak{p}$ is a field. Now, the natural morphism $A/\mathfrak{p} \to B/\mathfrak{P}$ is injective and integral, so $B/\mathfrak{P}$ is a field by proposition 1.2.2, which is what we wanted. □

For any non-zero prime ideal $\mathfrak{p}$ in A, we say that a prime ideal $\mathfrak{P}$ of B *lies above* $\mathfrak{p}$ if $\mathfrak{P} \cap A = \mathfrak{p}$. We denote it by $\mathfrak{P} \mid \mathfrak{p}$.
Any non-zero prime ideal $\mathfrak{p} \subset A$ generates an ideal $\mathfrak{p}B$ in B. By the previous proposition, B is a Dedekind ring, so we can write $\mathfrak{p}B$ as a product of non-zero prime ideals in B :

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$$

$e_{\mathfrak{P}}$ is called the ramification index of $\mathfrak{p}$ at $\mathfrak{P}$.
We also have that the natural embedding $A/\mathfrak{p} \to B/\mathfrak{P}$ is a finite field extension : we denote by $f_{\mathfrak{P}}$ its degree, which is called the residual degree of $\mathfrak{p}$ at $\mathfrak{P}$. Then we have the following theorem :

Theorem 1.5.7.

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} = [L : K]$$

1.6 Number fields

Definition 1.6.1. *A number field is a field K such that $K/\mathbf{Q}$ is a finite field extension.*

If K is a number field, we denote by $\mathcal{O}_K$ the integral closure of $\mathbf{Z}$ in K. It is called the *ring of integers* of the field K.
By corollary 1.3.5 (ii), we have the following fundamental theorem :

Theorem 1.6.2. *The ring of integers $\mathcal{O}_K$ of a number field K is a free $\mathbf{Z}$-module of rank $[K : \mathbf{Q}]$.*

In particular, we can speak about the discriminant of a basis of $\mathcal{O}_K$ over $\mathbf{Z}$. But here, the situation is better than in the general setting : not only the ideal $\mathrm{D}(x_1, \dots, x_n)\mathbf{Z}$ does not depend on the basis of $\mathcal{O}_K$ over $\mathbf{Z}$, but the number $\mathrm{D}(x_1, \dots, x_n)$ does not depend on the basis ! Indeed, if $(x_1, \dots, x_n)$ and $(y_1, \dots, y_n)$ are two bases of $\mathcal{O}_K$ over $\mathbf{Z}$, then there exists $M \in \mathrm{GL}_n(\mathbf{Z})$ such that

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

and then $\mathrm{D}(y_1, \dots, y_n) = \det(M)^2 \mathrm{D}(x_1, \dots, x_n) = \mathrm{D}(x_1, \dots, x_n)$ because $\det(M) \in \{\pm 1\}$.

Definition 1.6.3. *If K is a number field, we define its discriminant as $\mathrm{D}(x_1, \dots, x_n)$, where $(x_1, \dots, x_n)$ is any basis of $\mathcal{O}_K$ over $\mathbf{Z}$.*

Now, if K is a number field, the extension $K/\mathbf{Q}$ is separable (because $\mathbf{Q}$ has characteristic zero, so it is a perfect field), so $\mathcal{O}_K$ is a Dedekind domain by the general fact we recalled in proposition 1.5.6 (indeed, $\mathbf{Z}$ is a PID, hence a Dedekind domain).

Therefore, every non-zero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be written uniquely (up to the order of factors) as a product of non-zero prime ideals :

$$\mathfrak{a} = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

where the product runs over all the prime ideals containing $\mathfrak{a}$. In particular, the prime ideals in $\mathbf{Z}$ (which are exactly the ideals of the form $p\mathbf{Z}$ for some prime number p) may not remain prime if we look at the ideal generated in $\mathcal{O}_K$. We can write $p\mathcal{O}_K$ as a product $\prod_{\mathfrak{p}|p} \mathfrak{p}^{e_{\mathfrak{p}}}$, and as we defined in the section on Dedekind rings, we call $e_{\mathfrak{p}}$ the ramification index of p at $\mathfrak{p}$. Besides, for all $\mathfrak{p} \mid p$, the natural ring homomorphism $\mathbf{Z}/p\mathbf{Z} \to \mathcal{O}_K/\mathfrak{p}$ is a finite field extension, and we denote its degree by $f_{\mathfrak{p}}$.

Given a prime number p, it is not easy to find the factorization of $p\mathcal{O}_K$ as a product of prime ideals in $\mathcal{O}_K$. We will see an example of ramification law in the case of quadratic fields (see proposition

2.1.8). It is a situation where a simple congruence condition provides the shape of the factorization (the number of prime ideals above $p\mathcal{O}_K$ and the exponents appearing in the factorization). However, it does not give explicitly the prime ideals above some prime number p.

As $\mathcal{O}_K$ is a Dedekind ring, we can also define the ideal class group of $\mathcal{O}_K$ (as we did in the section on Dedekind rings). One central result in number theory is the following :

Theorem 1.6.4 (Finiteness of the class number). *Let K be a number field. Then $\mathrm{Cl}(\mathcal{O}_K)$ is a finite group.*

Now, we give some preliminary results in order to define the norm of an ideal of $\mathcal{O}_K$. This notion will play a role in the proof of Dirichlet's class number formula, since we will see that counting representations of integers by quadratic forms amounts to counting ideals with a prescribed norm.

Proposition 1.6.5. *If $x \in \mathcal{O}_K \setminus \{0\}$, and if we denote by (x) the ideal generated by x in $\mathcal{O}_K$, then*

$$|\mathrm{N}_{K/\mathbf{Q}}(x)| = |\mathcal{O}_K/(x)|\,.$$

Proof. First, note that since $x \in \mathcal{O}_K$, $\mathrm{N}_{K/\mathbf{Q}}(x) \in \mathbf{Z}$ by proposition 1.3.3, so that the equality we want to prove makes sense.
Let us denote by n the degree of the extension $K/\mathbf{Q}$. By theorem 1.6.2, we know that $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank n. The ideal (x) (which is by definition a sub-$\mathcal{O}_K$-module) is in particular a sub-$\mathbf{Z}$-module of $\mathcal{O}_K$. Thus, by the adapted basis theorem (for modules over a PID, in this case : $\mathbf{Z}$), there exists a basis $(e_1, \dots, e_n)$ of $\mathcal{O}_K$, an integer $r \leqslant n$, and positive integers $c_1, \dots, c_r$ such that

$$\begin{cases} c_1 \mid c_2 \mid \dots \mid c_r \\ (c_1 e_1, \dots, c_r e_r) \text{ is a basis of } x\mathcal{O}_K \text{ over } \mathbf{Z} \end{cases}$$

But since the multiplication by x : $\mathcal{O}_K \to x\mathcal{O}_K$ is an isomorphism of $\mathbf{Z}$-modules, the rank of $x\mathcal{O}_K$ is in fact also equal to n. This implies that $r = n$. Then we have $\mathcal{O}_K = e_1\mathbf{Z} \oplus \dots \oplus e_n\mathbf{Z}$ and $(x) = c_1e_1\mathbf{Z} \oplus \dots \oplus c_ne_n\mathbf{Z}$, hence

$$\mathcal{O}_K/(x) \simeq (\mathbf{Z}/c_1\mathbf{Z}) \times \dots \times (\mathbf{Z}/c_n\mathbf{Z})\,.$$

In particular, we have $|\mathcal{O}_K/(x)| = c_1c_2 \dots c_n$. But on the other hand, since $(e_1, \dots, e_n)$ is a basis of $\mathcal{O}_K$ over $\mathbf{Z}$, $(xe_1, \dots, xe_n)$ is also a basis of $x\mathcal{O}_K$! Thus, if we write each of these elements in the other basis $(c_1e_1, \dots, c_ne_n)$:

$$\begin{cases} xe_1 = a_{1,1}(c_1e_1) + \dots + a_{1,n}(c_ne_n) \\ \vdots \qquad\qquad\qquad \vdots \\ xe_n = a_{n,1}(c_1e_1) + \dots + a_{n,n}(c_ne_n) \end{cases} \tag{2}$$

the matrix $M := (a_{i,j})_{1 \leqslant i,j \leqslant n}$ that appears is in $\mathrm{GL}_n(\mathbf{Z})$. Indeed, it maps a basis of $x\mathcal{O}_K$ onto another basis of $x\mathcal{O}_K$.
Now, let us denote by $\mathcal{B}$ the basis $(e_1, \dots, e_n)$ of $\mathcal{O}_K$ over $\mathbf{Z}$ (it is in particular a basis for the extension $K/\mathbf{Q}$). Given an element $y \in K$, we denote by $\vec{y}$ the column vector in $\mathbf{Q}^n$ of its coordinates in the basis $(e_1, \dots, e_n)$ of $K/\mathbf{Q}$. Then (2) precisely states that for all $i \in \{1, \dots, n\}$,

$$\overrightarrow{xe_i} = \begin{pmatrix} a_{i,1}c_1 \\ \vdots \\ a_{i,n}c_n \end{pmatrix}$$

because $xe_i = \sum_{j=1}^{n} a_{i,j}c_je_j$. It is easy to verify that the vector $\overrightarrow{xe_i} \in \mathbf{Q}^n$ is the i-th column of the matrix C^tM, where C denotes the diagonal matrix

$$\begin{pmatrix} c_1 & & & \\ & c_1 & & \\ & & \ddots & \\ & & & c_n \end{pmatrix}$$

In other words, $C^tM\vec{e_i} = \vec{xe_i}$. This shows that C^tM is the matrix of the multiplication by x in the basis $\mathcal{B}$ of $K/\mathbf{Q}$. Therefore, $\det(C^tM) = \mathrm{N}_{K/\mathbf{Q}}(x) = \det(C)\det(M) = \pm c_1c_2\dots c_n$ (because $\det(M) \in \{\pm 1\}$ since $M \in \mathrm{GL}_n(\mathbf{Z})$). This concludes the proof. □

Proposition 1.6.6. *For all non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{a}$ is finite.*

Proof. If $\mathfrak{a}$ is a non-zero ideal, we can take an element $x \in \mathfrak{a} \setminus \{0\}$. Then $x\mathcal{O}_K \subseteq \mathfrak{a}$, so that $\mathcal{O}_K/\mathfrak{a}$ identifies with a quotient of $\mathcal{O}_K/(x)$. As the latter is finite by the previous proposition, $\mathcal{O}_K/\mathfrak{a}$ is finite. □

This proof also explains that any non-zero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank n. Indeed, for any element $x \in \mathfrak{a}\setminus\{0\}$, we have $x\mathcal{O}_K \subseteq \mathfrak{a} \subseteq \mathcal{O}_K$. It follows from the adapted basis theorem for $\mathbf{Z}$-modules that there are integers $r \leqslant s \leqslant n$ such that (x) is a free $\mathbf{Z}$-module of rank r, and $\mathfrak{a}$ a free $\mathbf{Z}$-module of rank s. But as we saw in the proof of proposition 1.6.5, (x) has rank n. This implies that this is also the case for $\mathfrak{a}$.

Definition 1.6.7. *If $\mathfrak{a} \subseteq \mathcal{O}_K$ is a non-zero ideal we define its norm as follows :*

$$\mathrm{N}(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|\,.$$

Proposition 1.6.8. *If $\mathfrak{a}, \mathfrak{b}$ are two non-zero ideals in $\mathcal{O}_K$, then $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$.*

Proof. See for instance [Sam71]. □

Proposition 1.6.9. *If $K/\mathbf{Q}$ is Galois, with Galois group denoted by G, then for all $\mathfrak{a}$ non-zero ideal in $\mathcal{O}_K$,*

$$\prod_{\sigma\in G} \sigma(\mathfrak{a}) = \mathrm{N}(\mathfrak{a})\mathcal{O}_K.$$

Proof. See [IR90], proposition 14.1.2. □

Definition 1.6.10. *Let K be a number field. We define the Dedekind zeta function of K as follows : for all $s \in \mathbf{C}$ such that $\mathrm{Re}(s) > 1$,*

$$\zeta_K(s) := \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \frac{1}{\mathrm{N}(\mathfrak{a})^s}$$

where the sum ranges over all the non-zero ideals of $\mathcal{O}_K$.

This series defines an holomorphic function on $\{s \in \mathbf{C} \mid \mathrm{Re}(s) > 1\}$. We remark that when $K = \mathbf{Q}$ we recover the standard Riemann zeta function.

Proposition 1.6.11. *The Dedekind zeta function from the previous definition has an Euler product expansion : with the notations above, for all $s \in \mathbf{C}$ such that $\mathrm{Re}(s) > 1$,*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1}$$

where the product ranges over all the non-zero prime ideals in $\mathcal{O}_K$.

Proof. See for instance [Bri]. This formula expresses in analytic terms the unique factorization of ideals into a product of prime ideals. □

2. The class number formula for imaginary quadratic fields

What we discuss in this section can be proved using only the modern language of ideals in the ring of integers of a number field. However, this is not how the class group was first thought in the case of quadratic fields. In this section, we will start by a quick review of standard facts on imaginary quadradic fields, expressed in the modern language. But then, we will also describe how Gauss defined the same class group with a very different point of view : it was defined as a set of equivalence classes of binary quadratic forms with integral coefficients. It turns out that this point of view still has some advantages, and we will use it in the proof of Dirichlet class number formula. This is also interesting from an historical perspective, since this theory of equivalence of quadratic forms was a first step in the development of the theory of rings and ideals.

2.1 Imaginary quadratic fields

In this section, we specialize the general results on number fields to the case of imaginary quadratic fields.

Definition 2.1.1. *A quadratic field K is a degree 2 extension of $\mathbf{Q}$. It can always be written as $K = \mathbf{Q}(\sqrt{d})$ for some squarefree integer d. Imaginary quadratic fields are those quadratic fields $\mathbf{Q}(\sqrt{d})$ with d negative.*

Remark. *Each time we write $\sqrt{m}$ for m negative, we mean $i\sqrt{-m}$, the root with positive imaginary part. This choice does not change the extension $\mathbf{Q}(\sqrt{d})$ (any square root of d in $\mathbf{C}$ would give the same extension), but this convention will be important when we will introduce the notion of correctly ordered basis of an ideal.*

Let $K = \mathbf{Q}(\sqrt{d})$ be an imaginary quadratic field. By theorem 1.6.2, $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank 2. In fact, we know a more precise statement : we can give a basis of $\mathcal{O}_K$ as a $\mathbf{Z}$-module.

Proposition 2.1.2. *$\mathcal{O}_K = \mathbf{Z} + \omega\mathbf{Z}$ with*

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \bmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

Note that the extension $K/\mathbf{Q}$ is Galois, and that the two automorphisms of K are the identity and the complex conjugation (indeed, since $d < 0$, the automorphism defined by $\sqrt{d} \mapsto -\sqrt{d}$ is nothing but the complex conjugation). Using proposition 1.4.4, we have that the discriminant of the field is

$$D = \left(\det \begin{pmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{pmatrix}\right)^2 = \begin{cases} 4d & \text{if } d \equiv 2,3 \bmod 4 \\ d & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

In any case, $K = \mathbf{Q}(\sqrt{D})$ and $\mathcal{O}_K = \mathbf{Z} + \frac{D+\sqrt{D}}{2}\mathbf{Z}$. Note that this shows that the discriminant of a quadratic field cannot be any integer. We will not need more than the following observation : D is necessarily congruent to 0 or 1 modulo 4.

Definition 2.1.3. *We will call a fundamental discriminant any integer that arises as the discriminant of a quadratic field.*

The units of $\mathcal{O}_K$ are also well known, and except for two exceptional cases, there are only $+1$ and -1.

Proposition 2.1.4. *Let d be a squarefree negative integer. Denote by $K := \mathbf{Q}(\sqrt{d})$ the imaginary quadratic field generated by a square root of d, and by w the number of units in $\mathcal{O}_K$. Then :*

- *if $d = -1$, $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$, hence $w = 4$.*
- *if $d = -3$, $\mathcal{O}_K^\times = \{\pm 1, \pm\mu, \pm\mu^2\}$ where $\mu = \mathrm{e}^{\frac{2i\pi}{3}}$, hence $w = 6$.*

- *if* $d = -2$ *or* $d < -3$, $\mathcal{O}_K^\times = \{\pm 1\}$, *hence* $w = 2$.

The idea to prove this proposition is to use proposition 1.3.3, which tells us that an element $a + b\sqrt{d} \in \mathcal{O}_K$ is a unit if and only if $\mathrm{N}_{K/\mathbf{Q}}(a + b\sqrt{d}) \in \{\pm 1\}$. But since $\mathrm{N}_{K/\mathbf{Q}}(a + b\sqrt{d}) = a^2 - db^2$ with d negative, there are not so many solutions. The study of units in real quadratic fields is more difficult since when d is positive, the equation $a^2 - db^2 = 1$ is a kind of Pell-Fermat equation, which can have infinitely many solutions.

As we remarked in the preliminaries on number fields, every non-zero ideal in $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank 2 (since $K/\mathbf{Q}$ is an extension of degree 2 here). We will sometimes use the phrase "(α, β) is an integral basis of $\mathfrak{a}$ " to say that (α, β) is a basis of $\mathfrak{a}$ as a $\mathbf{Z}$-module, i.e. $\mathfrak{a} = \alpha\mathbf{Z} \oplus \beta\mathbf{Z}$.

Proposition 2.1.5. *Let* $\mathfrak{a}$ *be a non-zero ideal in* $\mathcal{O}_K$*, and let* (α, β) *be an integral basis of* $\mathfrak{a}$*. Then we have :*

$$\det \begin{pmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{pmatrix} = \pm\sqrt{D}\ \mathrm{N}(\mathfrak{a}).$$

Proof. See [Hec81], theorem 76 for the analogue statement in any number field. We give a proof only in the case of imaginary quadratic fields, but the ideas are the same. We know from the section on number fields that $\mathfrak{a}$ is a free $\mathbf{Z}$-module of rank 2. By the adapted basis theorem, there exists a basis (e_1, e_2) of $\mathcal{O}_K$ over $\mathbf{Z}$, and positive integers c_1, c_2 such that

$$\begin{cases} c_1 \mid c_2 \\ (c_1 e_1, c_2 e_2) \text{ is a basis of } \mathfrak{a} \end{cases}$$

Then since $\mathcal{O}_K = e_1\mathbf{Z} \oplus e_2\mathbf{Z}$ and $\mathfrak{a} = c_1 e_1\mathbf{Z} \oplus c_2 e_2\mathbf{Z}$, we deduce that

$$\mathcal{O}_K/\mathfrak{a} \simeq (\mathbf{Z}/c_1\mathbf{Z}) \times (\mathbf{Z}/c_2\mathbf{Z})$$

hence $\mathrm{N}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| = c_1 c_2$.

Now, since $c_1 e_1$ and $c_2 e_2$ belong to $\mathfrak{a} = \alpha\mathbf{Z} \oplus \beta\mathbf{Z}$, there exists a unique $M \in \mathcal{M}_2(\mathbf{Z})$ such that

$$\begin{pmatrix} c_1 e_1 \\ c_2 e_2 \end{pmatrix} = M \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

But as $(c_1 e_1, c_2 e_2)$ is also a basis of $\mathfrak{a}$, we have that $M \in \mathrm{GL}_2(\mathbf{Z})$ in fact. In particular, it has determinant ± 1. Now, if we take the complex conjugates in this equality, and use the fact c_1, c_2 and the coefficient of M are real, we obtain :

$$\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} e_1 & \overline{e_1} \\ e_2 & \overline{e_2} \end{pmatrix} = M \begin{pmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{pmatrix}$$

Finally, we transpose this equality, take determinants, and use proposition 1.4.4 to interpret $\det \begin{pmatrix} e_1 & e_2 \\ \overline{e_1} & \overline{e_2} \end{pmatrix}$ as $\pm\sqrt{D}$, where D is the discriminant of K. This gives the announced result. □

Definition 2.1.6. *We say that a basis* (α, β) *of an ideal* $\mathfrak{a}$ *in* $\mathcal{O}_K$ *is correctly ordered if the sign is positive, that is : if we have*

$$\det \begin{pmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{pmatrix} = +\sqrt{D}\ \mathrm{N}(\mathfrak{a}).$$

Proposition 2.1.7. *If* $\mathfrak{a}$ *is a non-zero ideal in* $\mathcal{O}_K$*, with basis* (α, β) *over* $\mathbf{Z}$*, we have :*

$$\mathrm{N}(\mathfrak{a}) = \gcd\left(\mathrm{N}_{K/\mathbf{Q}}(\alpha), \mathrm{N}_{K/\mathbf{Q}}(\beta), \mathrm{Tr}_{K/\mathbf{Q}}\left(\alpha\overline{\beta}\right)\right)$$

Proof. Adapted from [EW05], chapter 4. We proceed in several steps :

- We prove that if $k \in \mathbf{Z}$ is a common divisor of $\mathrm{N}_{K/\mathbf{Q}}(\alpha), \mathrm{N}_{K/\mathbf{Q}}(\beta)$ and $\mathrm{Tr}_{K/\mathbf{Q}}\left(\alpha\overline{\beta}\right)$ in $\mathbf{Z}$, then k divides $\alpha\overline{\beta}$ and $\overline{\alpha}\beta$ in $\mathcal{O}_K$.

  To prove this, we just notice that $\mathrm{N}_{K/\mathbf{Q}}\left(\frac{\alpha\overline{\beta}}{k}\right) = \frac{1}{k^2}\mathrm{N}_{K/\mathbf{Q}}(\alpha)\mathrm{N}_{K/\mathbf{Q}}\left(\overline{\beta}\right)$. But with proposition 1.3.2 it is clear that $\mathrm{N}_{K/\mathbf{Q}}\left(\overline{\beta}\right) = \mathrm{N}_{K/\mathbf{Q}}\left(\beta\right)$. Therefore, the two norms on the right hand side are divisible by k by assumption, so we can conclude that $\mathrm{N}_{K/\mathbf{Q}}\left(\frac{\alpha\overline{\beta}}{k}\right) \in \mathbf{Z}$.
  We also have $\mathrm{Tr}_{K/\mathbf{Q}}\left(\frac{\alpha\overline{\beta}}{k}\right) = \frac{1}{k}\mathrm{Tr}_{K/\mathbf{Q}}\left(\alpha\overline{\beta}\right)$, and since we assumed that $\mathrm{Tr}_{K/\mathbf{Q}}\left(\alpha\overline{\beta}\right)$ is divisible by k, we get : $\mathrm{Tr}_{K/\mathbf{Q}}\left(\frac{\alpha\overline{\beta}}{k}\right) \in \mathbf{Z}$. Since the coefficients of the minimal polynomial of $\frac{\alpha\overline{\beta}}{k}$ over $\mathbf{Q}$ are, up to the sign, the trace and the norm we just computed, we deduce that this minimal polynomial has coefficients in $\mathbf{Z}$. By proposition 1.2.6, this implies that $\frac{\alpha\overline{\beta}}{k}$ belongs to $\mathcal{O}_K$, and this is what we wanted to show.

- Next, we prove that $\mathfrak{a}\overline{\mathfrak{a}}$ is a principal ideal of the form $k\mathcal{O}_K$, with

$$k := \gcd\left(\mathrm{N}_{K/\mathbf{Q}}(\alpha), \mathrm{N}_{K/\mathbf{Q}}(\beta), \mathrm{Tr}_{K/\mathbf{Q}}\left(\alpha\overline{\beta}\right)\right).$$

  By definition, $\mathfrak{a}\overline{\mathfrak{a}}$ contains $\alpha\overline{\alpha}$, $\beta\overline{\beta}$ and $\alpha\overline{\beta} + \overline{\alpha}\beta$. Therefore, it also contains the $\mathbf{Z}$-module generated by these three elements, which is exactly $k\mathbf{Z}$. In particular, $k \in \mathfrak{a}\overline{\mathfrak{a}}$, hence $k\mathcal{O}_K \subseteq \mathfrak{a}\overline{\mathfrak{a}}$. Conversely, $\mathfrak{a}\overline{\mathfrak{a}} = (\alpha\mathbf{Z} + \beta\mathbf{Z})\left(\overline{\alpha}\mathbf{Z} + \overline{\beta}\mathbf{Z}\right) = \alpha\overline{\alpha}\mathbf{Z} + \beta\overline{\alpha}\mathbf{Z} + \alpha\overline{\beta}\mathbf{Z} + \beta\overline{\beta}\mathbf{Z}$. But by definition, k divides $\alpha\overline{\alpha}$ and $\beta\overline{\beta}$ in $\mathbf{Z}$, hence in $\mathcal{O}_K$, and the preceding point shows that k also divides $\overline{\alpha}\beta$ and $\alpha\overline{\beta}$ in $\mathcal{O}_K$. Therefore, $\mathfrak{a}\overline{\mathfrak{a}} \subseteq k\mathcal{O}_K$, so we have equality.

- Finally, we know by proposition 1.6.9 that $\mathfrak{a}\overline{\mathfrak{a}} = \mathrm{N}(\mathfrak{a})\mathcal{O}_K$. Therefore, $\mathrm{N}(\mathfrak{a})\mathcal{O}_K = k\mathcal{O}_K$. But if we intersect with $\mathbf{Z}$ we get that $k\mathbf{Z} = \mathrm{N}(\mathfrak{a})\mathbf{Z}$, and since k and $\mathrm{N}(\mathfrak{a})$ are both positive integers, we must have equality.

□

Now, let us study the question of how prime numbers ramify in an imaginary quadratic field. By theorem 1.5.7 and the fact that in our case $[K : \mathbf{Q}] = 2$, we see that there are not many possibilities for the ramification of a prime number p : only three cases can occur.

- either p is inert : $p\mathcal{O}_K$ is a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. In this case, the ramification index of p at $\mathfrak{p}$ is 1, and so the residual degree equals 2, meaning that $\mathcal{O}_K/\mathfrak{p}$ is a degree 2 extension of $\mathbf{Z}/p\mathbf{Z}$. In particular we have $\mathrm{N}(\mathfrak{p}) = p^2$.
- or p is totally ramified : $p = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p} \subset \mathcal{O}_K$. In this case the ramification index at $\mathfrak{p}$ is 2, so the residual degree is 1, meaning that the inclusion $\mathbf{Z}/p\mathbf{Z} \to \mathcal{O}_K/\mathfrak{p}$ is also surjective. In particular, we have $\mathrm{N}(\mathfrak{p}) = p$.
- or p is split : $p = \mathfrak{p}\mathfrak{p}'$ for some distinct prime ideals $\mathfrak{p}, \mathfrak{p}' \subset \mathcal{O}_K$. In this case, the residual degree at each of these two primes has to be one, so that $\mathrm{N}(\mathfrak{p}) = p = \mathrm{N}(\mathfrak{p}')$.

Proposition 2.1.8. *Let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic field with discriminant denoted by D. If p is a prime number, we have :*

- *p is split if and only if $\left(\frac{D}{p}\right) = 1$*
- *p is inert if and only if $\left(\frac{D}{p}\right) = -1$*
- *p is totally ramified if and only if $\left(\frac{D}{p}\right) = 0$*

where $\left(\frac{\cdot}{p}\right)$ denotes the Kronecker symbol. For odd primes p, it is just the usual Legendre symbol, but for $p = 2$, it is another convention, that we explain in appendix B.

Proof. For this exact statement, see [Hec81], theorem 90. The proof of this ramification law is also nicely done in [Sam71], but the result is expressed in terms of $\left(\frac{d}{\cdot}\right)$ instead of $\left(\frac{D}{\cdot}\right)$, so it requires some little changes.

□

According to the definition of the Kronecker symbol, we can give a reformulation of the ramification law for the prime 2 :

- 2 is split if and only if $D \equiv 1 \bmod 8$
- 2 is inert if and only if $D \equiv 5 \bmod 8$
- 2 is totally ramified if and only if $D \equiv 0 \bmod 4$.

Note that the ramification law for the prime 2 seems to miss some possible congruences for D, but in fact it does not. Indeed, as we already observed, a discriminant of a quadratic field can only be congruent to 0 or 1 modulo 4.

2.2 Classical theory of binary quadratic forms

The main interest of this section is the study of binary quadratic forms with integral coefficients. Namely, we will focus on forms

$$\varphi(X, Y) = aX^2 + bXY + cY^2$$

where $(a, b, c) \in \mathbf{Z}^3$.

Definition 2.2.1. *If φ is a binary quadratic form as above, we define its discriminant D as follows : $D := b^2 - 4ac$.*

Note that D can only be congruent to 0 or 1 modulo 4.
We remark that the matrix of φ in the canonical basis of $\mathbf{R}^2$ is $\mathrm{Mat}_\varphi := \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$, which has determinant $ac - \frac{b^2}{4}$, so that the discriminant of φ is nothing but $-4\det(\mathrm{Mat}_\varphi)$. This will be useful to prove that easily that the discriminant is invariant under some group action that we are going to define on the set of quadratic forms.
Since our aim is to use this point of view to prove Dirichlet class number formula for *imaginary* quadratic fields, we restrict to the case where $D < 0$.
There are some natural questions about these forms :

- Which integers are represented by φ (that is : for which $m \in \mathbf{Z}$ does there exist $(u, v) \in \mathbf{Z}^2$ such that $\varphi(u, v) = m$?) For instance, if $\varphi(X, Y)$ is given by $X^2 + Y^2$, this is the famous question of which integers are the sum of two squares.
- Once we know that φ represents some integer m, how many pairs (u, v) satisfy $\varphi(u, v) = m$?

For instance, in the case of the form $\varphi(X, Y) = X^2 + Y^2$, we have the following result :

Theorem 2.2.2. *Let n be a positive integer. Write*

$$n := \prod_{p \text{ prime}} p^{v_p(n)}$$

We have that n is the sum of two squares if and only if for all prime p such that $p \equiv 3 \bmod 4$, $v_p(n)$ is even. Moreover, the numbers of pairs $(u, v) \in \mathbf{Z}^2$ such that $n = u^2 + v^2$ is $4(d_1(n) - d_3(n))$, where $d_i(n)$ denotes the number of positive divisors of n that are congruent to $i \bmod 4$.

Let us come back to the general case of a binary quadratic form $\varphi(X,Y) = aX^2 + bXY + cY^2$ with negative discriminant D. We remark that

$$4a\varphi(X,Y) = 4a^2 + 4abXY + 4acY^2 = (2aX + bY)^2 + (4ac - b^2)Y^2 = (2aX + bY)^2 + |D|Y^2.$$

Therefore, φ is either definite positive (if $a > 0$) or definite negative (if $a < 0$). Since replacing φ by $-\varphi$ turns a positive form into a negative one, and conversely, the study of the integers represented by a form with negative discriminant can be reduced to the case where φ is positive definite (i.e. $a > 0$). Finally, to study the question of which integers are represented by a given form, we can assume that the form is *primitive*, i.e. that $\gcd(a,b,c) = 1$. Indeed, if d denotes $\gcd(a,b,c)$, then $\frac{1}{d}\varphi$ is primitive, and to get the set of integers represented by φ, it suffices to multiply by d the set of integers represented by $\frac{1}{d}\varphi$.

This is why we introduce the following set, for all D negative integer such that $D \equiv 0, 1 \bmod 4$:

$$\mathcal{Q}_D^+ := \left\{ \begin{array}{c} \text{primitive binary quadratic forms } \varphi(X,Y) = aX^2 + bXY + cY^2 \\ \text{such that } a > 0 \text{ and } b^2 - 4ac = D \end{array} \right\}$$

Note that $\mathcal{Q}_D^+$ is non-empty, since the following quadratic form :

$$\varphi(X,Y) := \begin{cases} X^2 - DY^2 & \text{if } D \equiv 0 \bmod 4 \\ X^2 + XY + \frac{1-D}{4}Y^2 & \text{if } D \equiv 1 \bmod 4 \end{cases}$$

is an element of $\mathcal{Q}_D^+$. We will call it the *principal* quadratic form of discriminant D (this terminology will make more sense when we will explain the link between these quadratic forms and ideals in $\mathbf{Q}(\sqrt{D})$). Maybe it is also worth insisting on the fact that elements in $\mathcal{Q}_D^+$ are assumed to be primitive, although it does not appear in the notation.

This remark on the existence of a principal form of discriminant D shows that an integer is the discriminant of a binary quadratic form if and only if it is congruent to 0 or 1 modulo 4. This motivates the following definition.

Definition 2.2.3. *An integer $\Delta \in \mathbf{Z}$ is said to be a discriminant if $\Delta \equiv 0 \bmod 4$ or $\Delta \equiv 1 \bmod 4$.*

Now, let us denote by Γ the modular group $\mathrm{SL}_2(\mathbf{Z})$. We define, for all $\varphi \in \mathcal{Q}_D^+$ and $\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma$,

$$\varphi^\sigma(X,Y) := \varphi(\alpha X + \beta Y, \gamma X + \delta Y)$$

Proposition 2.2.4. *For all $\sigma \in \Gamma$ and for all $\varphi \in \mathcal{Q}_D^+$, we have that $\varphi^\sigma \in \mathcal{Q}_D^+$. Moreover, if $\sigma, \tau \in \Gamma$, then $\varphi^{\sigma\tau} = (\varphi^\sigma)^\tau$, hence*

$$\begin{array}{ccc} \Gamma \times \mathcal{Q}_D^+ & \to & \mathcal{Q}_D^+ \\ (\sigma, \varphi) & \mapsto & \varphi^\sigma \end{array}$$

defines a right group action of Γ on $\mathcal{Q}_D^+$.

Proof. First, we take $\varphi \in \mathcal{Q}_D^+$ and $\sigma \in \Gamma$, and we want to check that φ^σ is still in $\mathcal{Q}_D^+$. We write

$$\sigma := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \text{ and } \varphi(X,Y) := aX^2 + bXY + cY^2 \text{ (as before).}$$

In terms of matrices, we have

$$\varphi(X,Y) = \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

and

$$\varphi^\sigma(X,Y) = \begin{pmatrix} X & Y \end{pmatrix} {}^t\sigma \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \sigma \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Therefore, the matrix of the quadratic form φ^σ is :

$$ {}^t\sigma \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \sigma.$$

Computing the determinant of this matrix (using the fact that σ has determinant 1) shows that φ^σ has the same discriminant as φ.

Besides,

$$\begin{aligned} \varphi^\sigma(X,Y) &= \varphi(\alpha X + \beta Y, \gamma X + \delta Y) \\ &= \cdots \\ &= a_\sigma X^2 + b_\sigma XY + c_\sigma Y^2 \end{aligned}$$

with

$$\begin{cases} a_\sigma = a\alpha^2 + b\alpha\gamma + c\gamma^2 = \varphi(\alpha, \gamma) \\ b_\sigma = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ c_\sigma = a\beta^2 + b\beta\delta + c\delta^2 = \varphi(\beta, \delta). \end{cases}$$

This shows that the coefficients of φ^σ are still integers. Moreover, since φ is positive definite, $a_\sigma > 0$, so that φ^σ is also positive definite (note that to go from $a_\sigma > 0$ to φ^σ positive definite, we use the fact that the discriminant is negative, so it is important to prove first that the discriminant is preserved). Finally, it remains to show that φ^σ is still primitive. But from the equations for $a_\sigma, b_\sigma, c_\sigma$, we see that $\gcd(a,b,c)$ divides the coefficients of φ^σ. Thus, if we do the same computations with σ^{-1} instead of σ, we would prove that $\gcd(a_\sigma, b_\sigma, c_\sigma)$ divides all the coefficients of φ, hence divides $\gcd(a,b,c) = 1$, so φ^σ is also primitive, and this finishes the proof that the action of Γ stabilizes $\mathcal{Q}_D^+$. The second part of the statement is straightforward. □

Two elements of $\mathcal{Q}_D^+$ are said to be equivalent if they are in the same Γ-orbit, i.e. $\varphi \sim \psi$ if and only if there exists $\sigma \in \Gamma$ such that $\psi = \varphi^\sigma$. We will denote by $[\varphi]$ the orbit of φ under the action of Γ, that is :

$$[\varphi] = \{\varphi^\sigma,\ \sigma \in \Gamma\} = \{\psi \in \mathcal{Q}_D^+ \mid \psi \sim \varphi\}.$$

It is not hard to prove that two equivalent forms represent the same integers, so that we only need to study a representative set for this action to study representations of integers by elements of $\mathcal{Q}_D^+$.

Definition 2.2.5. *A binary quadratic form $\varphi(X,Y) = aX^2 + bXY + cY^2 \in \mathcal{Q}_D^+$ is said to be reduced if its coefficients satisfy $-a < b \leqslant a \leqslant c$ and $b \geqslant 0$ if $a = c$.*

We are going to prove that every element in $\mathcal{Q}_D^+$ is equivalent to a unique reduced form, so that the set of reduced forms is a representative set for the equivalence classes of $\mathcal{Q}_D^+$ under the action of Γ. However, this strange condition on the relative sizes of the coefficients does not seem natural at all. So we start by explaining why this is a natural choice of representatives.
In fact every binary quadratic form $\varphi \in \mathcal{Q}_D^+$ can be factored into a product of two linear factors over $\mathbf{C}$:

$$\varphi(X,Y) = aX^2 + bXY + cY^2 = a(X + z_\varphi Y)(X + \overline{z_\varphi} Y)$$

where $z_\varphi = \frac{b+\sqrt{D}}{2a}$, and we choose the root $\sqrt{D} := i\sqrt{-D}$ so that $z_\varphi \in \mathbf{H} = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$. This gives us a natural way associate a unique point in $\mathbf{H}$ with each form in $\mathcal{Q}_D^+$. We call z_φ the principal root of φ. Now, the nice thing is that Γ also acts on $\mathbf{H}$ in the following way :

$$\begin{array}{ccc} \Gamma \times \mathbf{H} & \to & \mathbf{H} \\ \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, z \right) & \mapsto & \frac{\alpha z + \beta}{\gamma z + \delta} \end{array}$$

and this action is compatible with the action on quadratic forms !

Proposition 2.2.6. *Let $\varphi \in \mathcal{Q}_D^+$, and let $\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma$. Then the principal root of φ^σ is $\frac{\alpha z_\varphi + \beta}{\gamma z_\varphi + \delta}$.*

Proof. Since Γ is generated by the two matrices $S := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, it suffices to prove the statement for the action of these matrices. Still denoting $\varphi(X,Y) = aX^2 + bXY + cY^2$, we prove the statement for the matrix T. We have that $\varphi^T(X,Y) = \varphi(-Y,X) = cX^2 - bXY + aY^2$, so that its principal root is $\frac{-b+\sqrt{D}}{2c}$. Let us show that this is also the image of z_φ after the action of T : namely $\frac{-1}{z_\varphi}$.

$$\frac{-1}{z_\varphi} = \frac{-2a}{b+\sqrt{D}} = \frac{-2a(b-\sqrt{D})}{(b+\sqrt{D})(b-\sqrt{D})} = \frac{-2a(b-\sqrt{D})}{b^2-D} = \frac{-2a(b-\sqrt{D})}{b^2-(b^2-4ac)} = \frac{-b+\sqrt{D}}{2c}.$$

This proves the statement for the action of the matrix T, and similar computations give the result for the matrix S, hence the conclusion. □

Using this observation together with the usual knowledge of the action of Γ on $\mathbf{H}$, we see that each $\varphi \in \mathcal{Q}_D^+$ is equivalent to a unique form whose principal root is in the standard fundamental domain for the action of Γ on $\mathbf{H}$:

$$\mathscr{D} := \left\{ z \in \mathbf{H} \mid -\frac{1}{2} < \mathrm{Re}(z) < 0, |z| > 1 \right\} \cup \left\{ z \in \mathbf{H} \mid 0 \leqslant \mathrm{Re}(z) \leqslant \frac{1}{2}, |z| \geqslant 1 \right\}$$

And in fact, a simple computation shows that the condition to have the principal root in $\mathscr{D}$ is exactly equivalent to the condition to be a reduced form (see definition 2.2.5). This shows that the set of reduced forms is indeed a representative set for $\mathcal{Q}_D^+/\sim$.

Proposition 2.2.7. *For a given discriminant $D < 0$, there are only finitely many reduced forms with discriminant D. In other words, the quotient $\mathcal{Q}_D^+/\sim$ is finite.*

Proof. Let $\varphi(X,Y) = aX^2 + bXY + cY^2$ be a reduced form of discriminant D. Then $|b| \leqslant a \leqslant c$, so that $4b^2 \leqslant 4ac$. Replacing $4ac$ by $b^2 - D$ we obtain : $4b^2 \leqslant b^2 - D$, hence $|b| \leqslant \sqrt{\frac{-D}{3}}$. Thus, there are only finitely many choices for b (recall that we require $b \in \mathbf{Z}$), and for each b, there are only finitely many $(a,c) \in \mathbf{Z}^2$ such that $b^2 - D = 4ac$. □

Definition 2.2.8. *We denote by $h(D)$ the number of equivalence classes of forms in $\mathcal{Q}_D^+$, i.e. the number of elements in $\mathcal{Q}_D^+/\sim$. It is called the class number of discriminant D. This is also the number of reduced forms with discriminant D.*

Now, to study representations of integers by quadratic forms, the notion of *automorphs* is important. For a given $\varphi \in \mathcal{Q}_D^+$, we say that $\sigma \in \Gamma$ is an automorph of φ if $\varphi^\sigma = \varphi$. In terms of matrices,this means that ${}^t\sigma \mathrm{Mat}_\varphi \sigma = \mathrm{Mat}_\varphi$.

Proposition 2.2.9. *Let D be a negative discriminant. Then each $\varphi \in \mathcal{Q}_D^+$ has exactly w automorphisms, where w is the number of units in $\mathbf{Q}(\sqrt{D})$.*

Proof. See [Str08], lemma 5.5 and corollary 5.6. □

Note that thanks to proposition 2.1.4, we know exactly w :

$$w = \begin{cases} 4 \text{ if } D = -1 \\ 6 \text{ if } D = -3 \\ 2 \text{ otherwise} \end{cases} \tag{3}$$

We started this section on quadratic forms by some motivating questions. One of them was the question of which integers are represented by a given quadratic form. In fact, this question is quite difficult, and we will only give conditions for an integer to be represented by *some* binary quadratic form of discriminant D (not by a fixed form).

Definition 2.2.10. *Let φ be a binary quadratic form. We say that an integer m is properly represented by φ if there exist $u, v \in \mathbf{Z}$, coprime, such that $\varphi(u, v) = m$.*

The following proposition gives a very simple condition for m to be properly represented by *some* form of discriminant D.

Proposition 2.2.11. *Let $m \in \mathbf{Z}$ be a positive integer. Then there exists $\varphi \in \mathcal{Q}_D^+$ such that m is properly represented by φ if and only if D is a square modulo $4m$.*

Proof. [Str08], lemma 5.10. (where the statement is also more precise). □

Now, given a discriminant $D < 0$, let us denote by $\mathcal{S} = \{\varphi_1, \dots, \varphi_h\}$ a representative set for $\mathcal{Q}_D^+/\sim$ (in particular, $h = h(D)$ is the class number). For all $i \in \{1, \dots, h\}$, we denote by $r_i(n)$ the number of distinct representations of n by φ_i :

$$r_i(n) := |\left\{(x, y) \in \mathbf{Z}^2 \mid \varphi_i(x, y) = n\right\}|$$

Note that this number is finite. Indeed, if φ is a binary quadratic form with discriminant $D < 0$, say $\varphi(X, Y) = aX^2 + bXY + cY^2$, and if (x, y) is a representation of some integer n by φ, then : $ax^2+bxy+cy^2 = n$. This implies that $4a^2x^2+4abxy+4acy^2 = 4an$ so that $(2ax+by)^2-(b^2-4ac)y^2 = 4an$ i.e. $(2ax + by)^2 + |D|y^2 = 4an$. But a, b, c, n being fixed, it is clear that there are only finitely many $(x, y) \in \mathbf{Z}^2$ satisfying this last equality.
Finally, we also introduce the notation $R_D(n)$ for the number of representations of n by a representative set of $\mathcal{Q}_D^+/\sim$. Explicitly :

$$R_D(n) := \sum_{i=1}^{h} r_i(n).$$

Theorem 2.2.12. *Let $n \in \mathbf{Z}$ be a positive integer such that $\gcd(n, D) = 1$. Then :*

$$R_D(n) = w \sum_{m|n} \left(\frac{D}{m}\right)$$

where w is given by (3) and $\left(\frac{D}{\cdot}\right)$ is the Kronecker symbol (see appendix B).

Proof. See [Str08], theorem 5.9 for a proof only based on quadratic forms. We chose to give an alternative proof later, using the connection between this theory and the modern point of view on the class group (in terms of ideals). □

2.3 Unification of the two points on view on the class group

This section is mostly based on [Hec81].

Associating a quadratic form with an ideal : Let $K := \mathbf{Q}(\sqrt{d})$ be an imaginary quadratic field, with discriminant D. We are given an ideal $\mathfrak{a} \subset \mathcal{O}_K$, and the question is : how do we define an associated element of $\mathcal{Q}_D^+$?

Let us consider a correctly ordered $\mathbf{Z}$-basis (α, β) of $\mathfrak{a}$ (see definition 2.1.6). We assign to the ideal $\mathfrak{a}$ the following form (which depends on $\mathfrak{a}$ but also on the basis) :

$$\varphi_{\mathfrak{a},(\alpha,\beta)}(X, Y) := \frac{\mathrm{N}_{K/\mathbf{Q}}(\alpha X + \beta Y)}{\mathrm{N}(\mathfrak{a})} = \frac{(\alpha X + \beta Y)(\overline{\alpha} X + \overline{\beta} Y)}{\mathrm{N}(\mathfrak{a})}.$$

Let us check that this form is indeed in $\mathcal{Q}_D^+$. If we expand the numerator, we get :

$$\begin{aligned}(\alpha X + \beta Y)(\overline{\alpha} X + \overline{\beta} Y) &= \alpha\overline{\alpha}X^2 + (\alpha\overline{\beta} + \beta\overline{\alpha})XY + \beta\overline{\beta}Y^2 \\ &= \mathrm{N}_{K/\mathbf{Q}}(\alpha)X^2 + \mathrm{Tr}_{K/\mathbf{Q}}(\alpha\overline{\beta})XY + \mathrm{N}_{K/\mathbf{Q}}(\beta)Y^2\end{aligned}$$

But thanks to proposition 2.1.7, we know that the gcd of these three coefficients is exactly $\mathrm{N}(\mathfrak{a})$, so $\varphi_{\mathfrak{a},(\alpha,\beta)}(X,Y)$ has coefficients in $\mathbf{Z}$ and it is primitive.
Moreover, since we are working with imaginary quadratic fields, the norm of a non-zero element is always positive, so the leading coefficient of $\varphi_{\mathfrak{a},(\alpha,\beta)}(X,Y)$ is positive. Finally, let us prove that the discriminant of this form is D. By definition, it is

$$\frac{\left(\alpha\overline{\beta}+\beta\overline{\alpha}\right)^2-4\alpha\overline{\alpha}\beta\overline{\beta}}{\mathrm{N}(\mathfrak{a})^2}.$$

But this equals

$$\frac{\left(\alpha\overline{\beta}-\beta\overline{\alpha}\right)^2}{\mathrm{N}(\mathfrak{a})^2},$$

which is exactly D by proposition 2.1.5.
This concludes the proof that the form we associate with the ideal $\mathfrak{a}$ and the basis (α,β) is indeed in $\mathcal{Q}_D^+$.

Associating an ideal with a quadratic form : Now let D be a fundamental negative discriminant (see definition 2.1.3). Let d be a negative squarefree integer such that $K:=\mathbf{Q}(\sqrt{d})$ has discriminant D. We assume that we are given a binary quadratic form $\varphi\in\mathcal{Q}_D^+$, and we are wondering how we can define an associated ideal in $\mathcal{O}_K$.
We write

$$\varphi(X,Y)=aX^2+bXY+cY^2=a(X+z_\varphi Y)(X+\overline{z_\varphi}Y)$$

where $z_\varphi=\frac{b+\sqrt{D}}{2a}$ is the principal root of φ. We assign to φ the ideal

$$\mathfrak{a}_\varphi:=a\left(\mathbf{Z}+\overline{z}_\varphi\mathbf{Z}\right)$$

which is indeed contained in $\mathcal{O}_K$ since $a\in\mathbf{Z}\subseteq\mathcal{O}_K$ and $\overline{z}_\varphi=\frac{b-\sqrt{D}}{2}=\frac{b+D}{2}-\frac{D+\sqrt{D}}{2}\in\mathbf{Z}+\frac{D+\sqrt{D}}{2}\mathbf{Z}=\mathcal{O}_K$ since $b+D=b+(b^2-4ac)\equiv 0 \bmod 2$.
Note that $\mathfrak{a}_\varphi$ is a priori only a sub-$\mathbf{Z}$-module of $\mathcal{O}_K$, and not clearly an ideal : there is something to prove here. We want to show that $\mathfrak{a}_\varphi\mathcal{O}_K\subseteq\mathfrak{a}_\varphi$. Since $\mathcal{O}_K=\mathbf{Z}+\frac{D+\sqrt{D}}{2}\mathbf{Z}$, we have :

$$\begin{aligned}\mathfrak{a}_\varphi\mathcal{O}_K&=\left(a\mathbf{Z}+\frac{b-\sqrt{D}}{2}\mathbf{Z}\right)\left(\mathbf{Z}+\frac{D+\sqrt{D}}{2}\mathbf{Z}\right)\\&\subseteq\underbrace{a\mathbf{Z}+\frac{b-\sqrt{D}}{2}\mathbf{Z}}_{=\mathfrak{a}_\varphi}+a\frac{D+\sqrt{D}}{2}\mathbf{Z}+\left(\frac{b-\sqrt{D}}{2}\right)\left(\frac{D+\sqrt{D}}{2}\right)\mathbf{Z}.\end{aligned}$$

So it just remains to prove that $a\frac{D+\sqrt{D}}{2}$ and $\left(\frac{b-\sqrt{D}}{2}\right)\left(\frac{D+\sqrt{D}}{2}\right)$ are also in $\mathfrak{a}_\varphi$.

- $a\frac{D+\sqrt{D}}{2}=a\frac{D+b}{2}-a\frac{b-\sqrt{D}}{2}\in a\mathbf{Z}+\frac{b-\sqrt{D}}{2}\mathbf{Z}$ because $D+b=b^2-4ac+b\equiv 0 \bmod 2$.
- $\left(\frac{b-\sqrt{D}}{2}\right)\left(\frac{D+\sqrt{D}}{2}\right)=\left(\frac{b-\sqrt{D}}{2}\right)\left(\frac{D+b-b+\sqrt{D}}{2}\right)=\frac{b^2-D}{4}+\left(\frac{D-b}{2}\right)\left(\frac{b-\sqrt{D}}{2}\right)\in a\mathbf{Z}+\frac{b-\sqrt{D}}{2}\mathbf{Z}$ because $b^2-D=4ac$ so $\frac{b^2-D}{4}\in a\mathbf{Z}$ and $D-b=b^2-4ac-b\equiv 0 \bmod 2$ so $\frac{D-b}{2}\in\mathbf{Z}$.

Thus, $\mathfrak{a}_\varphi$ is an ideal of $\mathcal{O}_K$.

Connection between the two points of view : With the notations above, the aim is to prove that there is a bijection between $\mathrm{Cl}(\mathcal{O}_K)$ and $\mathcal{Q}_D^+/\sim$. More precisely, we are going to show that the two associations we described above induce bijections inverse one to the other at the level of classes. Let us explain how it works. We take $[I]\in\mathrm{Cl}(\mathcal{O}_K)$, and we choose $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$ that is equivalent to I (i.e. such that there exists $\lambda\in K^\times$ such that $\mathfrak{a}=(\lambda)I$). Then we choose (α,β) a correctly ordered $\mathbf{Z}$-basis of $\mathfrak{a}$, and we define the form $\varphi_{\mathfrak{a},(\alpha,\beta)}$ as above. Finally, we take the class of $\varphi_{\mathfrak{a},(\alpha,\beta)}$ in $\mathcal{Q}_D^+/\sim$.

There are many things to verify :

(i) First, we have to check that the class of $\varphi_{\mathfrak{a},(\alpha,\beta)}$ does not depend on the choice of a correctly ordered basis (α,β). This will prove that we have a well defined map form the set of integral ideals of $\mathcal{O}_K$ to $\mathcal{Q}_D^+/\sim$:

$$\mathfrak{a} \mapsto [\varphi_{\mathfrak{a}}]$$

(ii) Then we have to verify that two equivalent integral ideals are mapped to the same class of binary quadratic forms. This will prove that the map

$$[I] \in \mathrm{Cl}(\mathcal{O}_K) \mapsto [\varphi_{\mathfrak{a}}]$$

does not depend on the choice of an integral ideal $\mathfrak{a}$ in $[I]$.

(iii) Once we know that we have a well defined map from $\mathrm{Cl}(\mathcal{O}_K)$ to $\mathcal{Q}_D^+/\sim$, it remains to explain why this map is a bijection.

Proof. (i) Let $\mathfrak{a}$ be a non-zero ideal in $\mathcal{O}_K$, and let (α,β) and (γ,δ) be two correctly ordered bases of $\mathfrak{a}$ (which is a free $\mathbf{Z}$-module of rank 2). Then there exists $\sigma \in \mathrm{GL}_2(\mathbf{Z})$ such that $\begin{pmatrix}\gamma & \delta\end{pmatrix} = \begin{pmatrix}\alpha & \beta\end{pmatrix}\sigma$. Then

$$\begin{pmatrix}\gamma & \delta\\ \overline{\gamma} & \overline{\delta}\end{pmatrix} = \begin{pmatrix}\alpha & \beta\\ \overline{\alpha} & \overline{\beta}\end{pmatrix}\sigma$$

and so if we take the determinant in this equality, we get : $\sqrt{D}\mathrm{N}(\mathfrak{a}) = \sqrt{D}\mathrm{N}(\mathfrak{a})\det(\sigma)$. Thus, $\det(\sigma) = 1$ i.e. $\sigma \in \mathrm{SL}_2(\mathbf{Z})$. Denote $\sigma := \begin{pmatrix}a & b\\ c & d\end{pmatrix}$. We have

$$\begin{aligned}\varphi_{\mathfrak{a},(\gamma,\delta)}(X,Y) &= \frac{\mathrm{N}_{K/\mathbf{Q}}(\gamma X+\delta Y)}{\mathrm{N}(\mathfrak{a})}\\ &= \frac{\mathrm{N}_{K/\mathbf{Q}}\left((\alpha a+\beta c)X+(\alpha b+\beta d)Y\right)}{\mathrm{N}(\mathfrak{a})}\\ &= \frac{\mathrm{N}_{K/\mathbf{Q}}(\alpha(aX+bY)+\beta(cX+dY))}{\mathrm{N}(\mathfrak{a})}\\ &= \varphi_{\mathfrak{a},(\alpha,\beta)}(aX+bY,cX+dY) = \varphi^{\sigma}_{\mathfrak{a},(\alpha,\beta)}(X,Y)\end{aligned}$$

Thus $\varphi_{\mathfrak{a},(\gamma,\delta)} = \varphi^{\sigma}_{\mathfrak{a},(\alpha,\beta)}$, and $\sigma \in \mathrm{SL}_2(\mathbf{Z})$, so they are in the same equivalence class. Therefore, the class of the form we assign to an ideal $\mathfrak{a}$ and a correctly ordered basis (α,β) actually does not depend on the choice of such a basis, so we just denote $[\varphi_{\mathfrak{a}}]$ instead of $\left[\varphi_{\mathfrak{a},(\alpha,\beta)}\right]$.

(ii) Now, suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are two integral ideals of $\mathcal{O}_K$ that define the same class in $\mathrm{Cl}(\mathcal{O}_K)$. Let $\lambda \in K^\times$ be such that $\mathfrak{a} = (\lambda)\mathfrak{b}$. Let (α,β) be a basis of $\mathfrak{a}$ and (γ,δ) be a basis of $\mathfrak{b}$. Then $(\lambda\gamma,\lambda\delta)$ is a basis of $(\lambda)\mathfrak{b} = \mathfrak{a}$. So there exists

$$\sigma := \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z})$$

such that $\begin{pmatrix}\alpha & \beta\end{pmatrix}\sigma = \begin{pmatrix}\lambda\gamma & \lambda\delta\end{pmatrix}$. But then we have

$$\begin{pmatrix}\alpha & \beta\\ \overline{\alpha} & \overline{\beta}\end{pmatrix}\sigma = \begin{pmatrix}\lambda\gamma & \lambda\delta\\ \overline{\lambda\gamma} & \overline{\lambda\delta}\end{pmatrix}.$$

Taking the determinant of this equality gives $\sqrt{D}\mathrm{N}(\mathfrak{a})\det(\sigma) = |\lambda|^2\sqrt{D}\mathrm{N}(\mathfrak{b})$ (since (α,β) and (γ,δ) are respectively correctly ordered bases of $\mathfrak{a}$ and $\mathfrak{b}$). This implies that $\det(\sigma) > 0$, and since we already know that $\det(\sigma) \in \{\pm 1\}$ (because $\sigma \in \mathrm{GL}_2(\mathbf{Z})$), we deduce that $\sigma \in \mathrm{SL}_2(\mathbf{Z})$. We also deduce that

$$|\lambda|^2 = \frac{\mathrm{N}(\mathfrak{a})}{\mathrm{N}(\mathfrak{b})}. \tag{4}$$

Then :

$$\begin{aligned}\varphi^{\sigma}_{\mathfrak{a},(\alpha,\beta)}(X,Y) &= \frac{\mathrm{N}_{K/\mathbf{Q}}(\alpha(aX+bY)+\beta(cX+dY))}{\mathrm{N}(\mathfrak{a})} \\ &= \frac{\mathrm{N}_{K/\mathbf{Q}}((\alpha a+\beta c)X+(\alpha b+\beta d)Y)}{\mathrm{N}(\mathfrak{a})} \\ &= \frac{\mathrm{N}_{K/\mathbf{Q}}(\lambda\gamma X+\lambda\delta Y)}{\mathrm{N}(\mathfrak{a})} \\ &= \frac{\mathrm{N}_{K/\mathbf{Q}}(\lambda)\mathrm{N}_{K/\mathbf{Q}}(\gamma X+\delta Y)}{\mathrm{N}(\mathfrak{a})}\end{aligned}$$

and using the fact that $\mathrm{N}_{K/\mathbf{Q}}(\lambda) = \lambda\overline{\lambda} = |\lambda|^2$ and equality (4), we conclude that $\varphi^{\sigma}_{\mathfrak{a},(\alpha,\beta)}(X,Y) = \varphi_{\mathfrak{b},(\gamma,\delta)}(X,Y)$. Therefore, $[\varphi_{\mathfrak{a}}] = [\varphi_{\mathfrak{b}}]$ in $\mathcal{Q}^+_D/\sim$.

(iii)

- *Surjectivity :* Let $\varphi = aX^2+bXY+cY^2 \in \mathcal{Q}^+_D$. We want to show that there exists an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that $[\varphi_{\mathfrak{a}}] = [\varphi]$.
  Consider $\mathfrak{a} := a\mathbf{Z} + \frac{b-\sqrt{D}}{2}\mathbf{Z} = a(\mathbf{Z}+\overline{z}_{\varphi}\mathbf{Z})$. This is an ideal of $\mathcal{O}_K$ as we proved above. Since $\sqrt{D}$ is not real, $\left(a, \frac{b-\sqrt{D}}{2}\right)$ is a $\mathbf{Z}$-basis of $\mathfrak{a}$. Therefore, the norm of $\mathfrak{a}$ is given by proposition 2.1.7, and is easily seen as the content of the form :

  $$\left(aX+\frac{b-\sqrt{D}}{2}Y\right)\left(aX+\frac{b+\sqrt{D}}{2}Y\right).$$

  But this form is nothing but $a\varphi(X,Y)$, and so it has content a (as φ is primitive). Thus, $\mathrm{N}(\mathfrak{a}) = a$. Now, a direct computation shows that the basis $\left(a, \frac{b-\sqrt{D}}{2}\right) =: (\alpha,\beta)$ is correctly ordered, and that

  $$\varphi_{\mathfrak{a},(\alpha,\beta)}(X,Y) = \varphi.$$

  This shows that $[\varphi_{\mathfrak{a}}] = [\varphi]$.
- *Injectivity :* Let $\mathfrak{a}$, $\mathfrak{b}$ be two ideals of $\mathcal{O}_K$, take (α,β) (resp. (γ,δ)) a correctly ordered basis for $\mathfrak{a}$ (resp. for $\mathfrak{b}$), and suppose that $\varphi_{\mathfrak{a},(\alpha,\beta)} \sim \varphi_{\mathfrak{b},(\gamma,\delta)}$. The aim is to show that there exists $\lambda \in K^{\times}$ such that $\mathfrak{a} = (\lambda)\mathfrak{b}$. For brevity, let us denote :

  $$F(X,Y) := \varphi_{\mathfrak{a},(\alpha,\beta)}(X,Y) = \frac{\mathrm{N}_{K/\mathbf{Q}}(\alpha X+\beta Y)}{\mathrm{N}(\mathfrak{a})}$$

  and

  $$G(X,Y) := \varphi_{\mathfrak{b},(\gamma,\delta)} = \frac{\mathrm{N}_{K/\mathbf{Q}}(\gamma X+\delta Y)}{\mathrm{N}(\mathfrak{b})}$$

  The assumption $F \sim G$ gives us a matrix $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ such that $G = F^{\sigma}$, i.e.

  $$\frac{(\gamma X+\delta Y)(\overline{\gamma}X+\overline{\delta}Y)}{\mathrm{N}(\mathfrak{b})} = \frac{((\alpha a+\beta c)X+(\alpha b+\beta d)Y)\left((\overline{\alpha}a+\overline{\beta}c)X+(\overline{\alpha}b+\overline{\beta}d)Y\right)}{\mathrm{N}(\mathfrak{a})}.$$

  By looking at the zeros of the polynomial $G(X,1)$, we see that $\frac{\alpha a+\beta c}{\alpha b+\beta d} = \frac{\gamma}{\delta}$ or $\frac{\overline{\gamma}}{\overline{\delta}}$, so there exists $\lambda \in K^{\times}$ such that :

  $$\begin{cases} \alpha a+\beta c = \lambda\gamma \\ \alpha b+\beta d = \lambda\delta \end{cases} \quad \text{or} \quad \begin{cases} \alpha a+\beta c = \lambda\overline{\gamma} \\ \alpha b+\beta d = \lambda\overline{\delta} \end{cases}$$

  However, in the second case, we would have :

$$\begin{pmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda\overline{\gamma} & \lambda\overline{\delta} \\ \overline{\lambda}\gamma & \overline{\lambda}\delta \end{pmatrix}.$$

Since $ad - bc = 1$, taking the determinant leads to $\mathrm{N}(\mathfrak{a})\sqrt{D} = -|\lambda|^2\mathrm{N}(\mathfrak{b})\sqrt{D}$, hence a sign contradiction. Thus, only the first case can happen. In this case, we have that $(\lambda\gamma, \lambda\delta)$ is deduced from (α, β) by multiplication by $\sigma \in \mathrm{SL}_2(\mathbf{Z})$. This implies that $(\lambda\gamma, \lambda\delta)$ is also a basis of $\mathfrak{a}$, hence $\mathfrak{a} = (\lambda)\mathfrak{b}$ and this concludes the proof.

□

Remark. *We can use this bijection to endow $\mathcal{Q}_D^+/\sim$ with a group structure, which corresponds to the composition law originally considered by Gauss. This composition law is discussed at the beginning of chapter 22 of [IK04]. Quite recently, Manjul Bhargava discovered a very elegant way to look at Gauss composition law, see [Bha04].*

Counting representations of an integer : We still assume that D is a negative fundamental discriminant, and denote by $K = \mathbf{Q}(\sqrt{d})$ an imaginary quadratic field of discriminant D. As in the end of section 2.2, let us denote by $\mathcal{S} := \{\varphi_1, \dots, \varphi_h\}$ a representative set for $\mathcal{Q}_D^+/\sim$. We also use again the notation $r_i(n)$ for the number of representations of n by a quadratic form φ_i, that is :

$$r_i(n) := |\left\{(x, y) \in \mathbf{Z}^2 \mid \varphi_i(x, y) = n\right\}|.$$

We are interested in the total number of representations of n by our complete system of representatives of $\mathcal{Q}_D^+/\sim$:

$$R_D(n) := \sum_{i=1}^{h} r_i(n).$$

In fact, we are going to show that this is more or less equivalent to counting ideals of $\mathcal{O}_K$ with norm equal to n. More precisely, we have the following theorem.

Theorem 2.3.1. *Let $w := \left|\mathcal{O}_K^\times\right|$ be the number of units in $\mathcal{O}_K$ (see proposition 2.1.4). Let us denote by $\rho_i(n)$ the set of representations of n by φ_i, so that $r_i(n) = |\rho_i(n)|$. There is a surjective w-to-1 map from the disjoint union of the sets $\rho_i(n)$ to the set of integral ideals $\mathfrak{a}$ of $\mathcal{O}_K$ such that $\mathrm{N}(\mathfrak{a}) = n$. In particular, $R_D(n) = w\ \#\{\mathfrak{a}$ integral ideal in $\mathcal{O}_K \mid \mathrm{N}(\mathfrak{a}) = n\}$.*

Proof. (Adapted from [Tao14]). Let us stress that in this statement, we use the notion of disjoint union for sets that are non necessarily pairwise disjoint. Indeed, if (x, y) is a representation of n by φ_i and φ_j for some $i \neq j$, we will map it to two different ideals, one when we consider (x, y) as an element of $\rho_i(n)$, and one other ideal when we consider (x, y) as an element of $\rho_j(n)$.

For all $i \in \{1, \dots, h\}$, if we write

$$\varphi_i(X, Y) = a_i X^2 + b_i XY + c_i Y^2$$

let us denote by (α_i, β_i) the basis $\left(a_i, \frac{b_i - \sqrt{D}}{2}\right)$ of $\mathfrak{a}_{\varphi_i}$ (the ideal associated with φ_i, as described in the paragraph about associating an ideal to a quadratic form). Then we proved (see the point (iii) of the paragraph connecting the two points of view on the class group) :

$$\varphi_{\mathfrak{a}_{\varphi_i}, (\alpha_i, \beta_i)} = \varphi_i$$

Now, let us explain how to assign an ideal of norm n to any representation of n by one of the φ_i's. Let (x, y) be a representation of n by $\varphi_i \in \mathcal{S}$. Then we have that

$$\begin{aligned} n &= \varphi_i(x, y) \\ &= \varphi_{\mathfrak{a}_{\varphi_i}, (\alpha_i, \beta_i)}(x, y) \\ &= \frac{\mathrm{N}_{K/\mathbf{Q}}(\alpha_i x + \beta_i y)}{\mathrm{N}(\mathfrak{a}_{\varphi_i})} \end{aligned}$$

Using the fact that $\mathcal{O}_K$ is a Dedekind domain, and that $(\alpha_i x + \beta_i y)\,\mathcal{O}_K \subseteq \mathfrak{a}_{\varphi_i}$, we can deduce that there is a unique ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ such that

$$(\alpha_i x + \beta_i y)\,\mathcal{O}_K = \mathfrak{a}_{\varphi_i}\mathfrak{b}. \tag{5}$$

But if we take the norms, we get $\mathrm{N}\left((\alpha_i x + \beta_i y)\,\mathcal{O}_K\right) = \mathrm{N}_{K/\mathbf{Q}}(\alpha_i x + \beta_i y) = \mathrm{N}(\mathfrak{a}_{\varphi_i})\mathrm{N}(\mathfrak{b})$ on one hand, and on the other hand, we also have $\mathrm{N}_{K/\mathbf{Q}}\left(\alpha_i x + \beta_i y\right) = n\mathrm{N}(\mathfrak{a}_{\varphi_i})$. Therefore, this unique ideal $\mathfrak{b}$ has norm n, and this is the ideal we assign to the representation (x, y).

Now, we need to explain that the map we define this way is indeed w to 1. First of all, equation (5) tells us that $[\mathfrak{b}] = [\mathfrak{a}_{\varphi_i}]^{-1}$ in $\mathrm{Cl}(\mathcal{O}_K)$. This implies that if (x, y) and (u, v) are two representations of n by different forms (φ_i and φ_j for $i \neq j$), then they will never be mapped to the same ideal. Therefore, we just need to show the to following points :

- if $\mathfrak{b}$ arises from a representation of n by some φ_i, then there are exactly w representations of n by φ_i that lead to the same ideal $\mathfrak{b}$.
- every integral ideal $\mathfrak{b}$ in $\mathcal{O}_K$ of norm n arises in this way (i.e. comes from a representation of n by one of the φ_i's).

Suppose that $\mathfrak{b}$ comes from a representation (x, y) of n by φ_i. Then the other representations (u, v) of n by φ_i leading to the same ideal $\mathfrak{b}$ are exactly those for which $(\alpha_i u + \beta_i v)\,\mathcal{O}_K = (\alpha_i x + \beta_i y)\,\mathcal{O}_K$. But two principal ideals are equal if and only if their generators are the same modulo multiplication by a unit. So the other representations (u, v) are exactly the (u, v) such that $\alpha_i u + \beta_i v = \mu(\alpha_i x + \beta_i y)$ for any $\mu \in \mathcal{O}_K^\times$. Since each μ gives a different element of $\mathfrak{a}_{\varphi_i}$ (we recall that $\mathfrak{a}_{\varphi_i}$ is an ideal of $\mathcal{O}_K$, so it is stable under multiplication by elements of $\mathcal{O}_K$) and since (α_i, β_i) is a $\mathbf{Z}$-basis of $\mathfrak{a}_{\varphi_i}$, we have the following :
For all $\mu \in \mathcal{O}_K^\times$ there exists a unique $(u, v) \in \mathbf{Z}^2$ such that $\alpha_i c + \beta_i d = \mu(\alpha_i x + \beta_i y)$. This proves that there are exactly w representations of n by φ_i that are mapped to $\mathfrak{b}$.

Finally, let $\mathfrak{b}$ be an integral ideal of norm n, and let us prove that there exists a representation of n by one of the φ_i's that is mapped to $\mathfrak{b}$.

As $\mathcal{S} = \{\varphi_1, \ldots, \varphi_h\}$ is a representative set for $\mathcal{Q}_D^+/\sim$, the associated ideals describle completely the class group :

$$\mathrm{Cl}(\mathcal{O}_K) = \{\ [\mathfrak{a}_{\varphi_i}]\,,\ 1 \leqslant i \leqslant h\}$$

Therefore, there exists a unique $i \in \{1, \ldots, h\}$ such that $[\mathfrak{b}] = [\mathfrak{a}_{\varphi_i}]^{-1}$. Then the ideal $\mathfrak{a}_{\varphi_i}\mathfrak{b}$ is a principal ideal of $\mathcal{O}_K$, contained in $\mathfrak{a}_{\varphi_i} = \alpha_i\mathbf{Z} + \beta_i\mathbf{Z}$. So there exists $(x, y) \in \mathbf{Z}^2$ such that

$$\mathfrak{a}_{\varphi_i}\mathfrak{b} = (\alpha_i x + \beta_i y)\mathcal{O}_K. \tag{6}$$

Then if we take the norms in this equality and use the fact that $\mathrm{N}(\mathfrak{b}) = n$ and that for all $z \in \mathcal{O}_K$, $\mathrm{N}(z\mathcal{O}_K) = \mathrm{N}_{K/\mathbf{Q}}(z)$, we get that (x, y) is a representation of n by the form $\varphi_{\mathfrak{a}_{\varphi_i},(\alpha_i,\beta_i)} = \varphi_i$. Besides, equality (6) tells us that this representation of n is mapped to the ideal $\mathfrak{b}$, and this finishes the proof. □

Thanks to this theorem, we will be able to prove the simple expression for $R_D(n)$ stated without proof in theorem 2.2.12. A key step is the following lemma.

Lemma 2.3.2. *Let $K = \mathbf{Q}(\sqrt{d})$ be an imaginary quadratic field (in fact the result also holds in any number field). For all $n \in \mathbf{N}^*$, let us denote by $F(n)$ the number of integral ideals of $\mathcal{O}_K$ of norm n. Then F is a multiplicative function, that is : for all a, b coprime integers, $F(ab) = F(a)F(b)$.*

Proof. For all $c \in \mathbf{N}^*$, let us denote by $\mathscr{I}(c)$ the set of ideals $\mathfrak{c}$ in $\mathcal{O}_K$ such that $\mathrm{N}(\mathfrak{c}) = c$ (so that $F(c) = |\mathscr{I}(c)|$).
Let us prove that when a and b are coprime positive integers, the map

$$\begin{array}{ccc} \mathscr{I}(a) \times \mathscr{I}(b) & \to & \mathscr{I}(ab) \\ (\mathfrak{a}, \mathfrak{b}) & \mapsto & \mathfrak{ab} \end{array}$$

is a bijection (this will show the multiplicativity of F). First of all, this map is well-defined, because for all $(\mathfrak{a}, \mathfrak{b}) \in \mathscr{I}(a) \times \mathscr{I}(b)$, $\mathrm{N}(\mathfrak{ab}) = ab$ thanks to proposition 1.6.8.
Now, let $\mathfrak{c} \in \mathscr{I}(ab)$, and let us prove that we can write $\mathfrak{c} = \mathfrak{ab}$ with $\mathrm{N}(\mathfrak{a}) = a$ and $\mathrm{N}(\mathfrak{b}) = b$, and $\mathfrak{a}$ and $\mathfrak{b}$ uniquely determined.
If such a factorization exists, let us write $\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_s^{\alpha_s}$ and $\mathfrak{b} = \mathfrak{p}_{s+1}^{\alpha_{s+1}} \dots \mathfrak{p}_{s+t}^{\alpha_{s+t}}$ (using the fact that $\mathcal{O}_K$ is a Dedekind domain, so we have an essentially unique factorization of ideals into products of non-zero prime ideals). For the moment, we don't know whether or not the same prime ideals appear in the factorization of $\mathfrak{a}$ and $\mathfrak{b}$. There could exist $i \in \{1, \dots, s\}$ and $j \in \{1, \dots, t\}$ such that $\mathfrak{p}_i = \mathfrak{p}_{s+j}$. But in fact, we are going to prove that this cannot happen. For all i, we denote by p_i the unique prime on which $\mathfrak{p}_i$ lies above, that is : the unique rational prime such that $\mathfrak{p}_i \cap \mathbf{Z} = p_i\mathbf{Z}$. Then the norm of $\mathfrak{p}_i$ is some positive power of p_i (just because $\mathbf{Z}/p_i\mathbf{Z} \to \mathcal{O}_K/\mathfrak{p}_i$ is a finite field extension). As a and b are coprime, the equalities $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p}_1)^{\alpha_1} \dots \mathrm{N}(\mathfrak{p}_s)^{\alpha_s} = a$ and $\mathrm{N}(\mathfrak{b}) = \mathrm{N}(\mathfrak{p}_{s+1})^{\alpha_{s+1}} \dots \mathrm{N}(\mathfrak{p}_{s+t})^{\alpha_{s+t}} = b$ show that all the $\mathfrak{p}_i$'s are distinct, since they lie above distinct primes. Therefore, the factorization $\mathfrak{c} = \mathfrak{ab} = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_s^{\alpha_s} \mathfrak{p}_{s+1}^{\alpha_{s+1}} \dots \mathfrak{p}_{s+t}^{\alpha_{s+t}}$ is the factorization of $\mathfrak{c}$ into a product of distinct non-zero prime ideals. This shows that $\mathfrak{a}$ and $\mathfrak{b}$ are uniquely determined : if we write the factorization of $\mathfrak{c}$, the ideal $\mathfrak{a}$ is the product of the prime factors that lie above the prime divisors of a, whereas $\mathfrak{b}$ is the product of the prime factors that lie above the prime divisors of b. Conversely, one checks that with this choice, we obtain $\mathfrak{a} \in \mathscr{I}(a)$ and $\mathfrak{b} \in \mathscr{I}(b)$. □

Thanks to the multiplicativity of F, we just need to focus on the study of $F(p^k)$ for p prime. This is the aim of the next proposition.

Proposition 2.3.3. *For all p prime and $k \in \mathbf{N}$,*

$$F(p^k) = \sum_{i=0}^{k} \left(\frac{D}{p^i}\right) = 1 + \sum_{i=1}^{k} \left(\frac{D}{p}\right)^i$$

Proof. See [Hec81], lemma just before theorem 148.
First, let us recall an argument that we already used in the proof of the previous lemma : if $\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$ (factorization as a product of distinct non-zero prime ideals), and if we denote by p_i the prime $\mathfrak{p}_i$ lies above, then $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p}_1)^{\alpha_1} \dots \mathrm{N}(\mathfrak{p}_s)^{\alpha_s}$ and each $\mathrm{N}(\mathfrak{p}_i)$ is a power of p_i. Thus, if an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ has norm equal to p^k for some prime number p, this means that the only prime ideals that appear in the factorization of $\mathfrak{a}$ are lying above p.

Now, let us start the proof of the proposition. Let p be a fixed prime number, and $k \geqslant 1$. If $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$ such that $\mathrm{N}(\mathfrak{a}) = p^k$, then by what we just recalled, this means that $\mathfrak{a}$ is a product of prime ideals lying above p. Thanks to proposition 2.1.8, we have three distinct cases :

(i) $\left(\frac{D}{p}\right) = -1$: in this case, p is inert, meaning that the ideal $p\mathcal{O}_K =: \mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$. Since the ideals lying above p are exactly the ideals that appear in the factorization of $p\mathcal{O}_K$ as a product of non-zero prime ideals, we get that $\mathfrak{p}$ is the only prime ideal lying above p. Thus, $\mathfrak{a}$ has to be of the form $\mathfrak{p}^u$ for some $u \geqslant 0$. Then $p^k = \mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p}^u) = \mathrm{N}(p^u\mathcal{O}_K) = p^{2u}$. Therefore, if k is even, there is exactly one ideal in $\mathcal{O}_K$ of norm p^k (and it is the ideal generated by $p^{\frac{k}{2}}$ in $\mathcal{O}_K$). If k is odd, then there is no ideal of norm p^k in $\mathcal{O}_K$. Thus :

$$F(p^k) = \begin{cases} 1 \text{ if } k \text{ is even} \\ 0 \text{ if } k \text{ is odd} \end{cases}$$

in agreement with the equality in the proposition.

(ii) $\left(\frac{D}{p}\right) = 0$: in this case, p is totally ramified i.e. $p\mathcal{O}_K = \mathfrak{p}^2$ for some non-zero prime ideal $\mathfrak{p}$. As above, this means that an ideal $\mathfrak{a}$ of norm p^k is necessarily a power of $\mathfrak{p}$: $\mathfrak{a} = \mathfrak{p}^u$. Then $p^k = \mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p})^u$. But $\mathrm{N}(\mathfrak{p}) = p$ (see the section 2.1, where we recalled some facts about imaginary quadratic fields), hence $u = k$. Therefore, there is a unique ideal of norm p^k, and it is $\mathfrak{a} := \mathfrak{p}^k$. So

$$F(p^k) = 1 = 1 + \sum_{i=1}^{k} \left(\frac{D}{p}\right)^i$$

(iii) $\left(\frac{D}{p}\right) = +1$: in this case, p is split, that is $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for two distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Then an ideal $\mathfrak{a}$ of norm p^k is necessarily of the form $\mathfrak{p}_1^u\mathfrak{p}_2^v$ for some $u, v \in \mathbf{N}$. But the condition $\mathrm{N}(\mathfrak{a}) = p^k$ combined with fact that $\mathrm{N}(\mathfrak{p}_1) = p = \mathrm{N}(\mathfrak{p}_2)$ implies that $u + v$ must be equal to k. Thus, we have $k + 1$ possibilities for (u, v) (namely the tuples $(i, k - i)$, for $i \in \{0, \ldots, k\}$). This shows that there are $k + 1$ ideals of norm p^k. So

$$F(p^k) = k + 1 = 1 + \sum_{i=1}^{k} \left(\frac{D}{p}\right)^i$$

and this finishes the proof.

□

Corollary 2.3.4. *Using the multiplicativity of F and the previous proposition, we deduce that for all $n \in \mathbf{N}^*$,*

$$F(n) = \sum_{m|n} \left(\frac{D}{m}\right)$$

Combining this result and the link between F and the number of representations of n by a complete system of non-equivalent binary quadratic form (theorem 2.3.1), we finally have a proof of theorem 2.2.12, in the case where D is fundamental discriminant (and, to me, it looks like we don't need the assumption $\gcd(n, D) = 1$ anymore).

Theorem 2.3.5. *Let D be a negative fundamental discriminant, and let $n \in \mathbf{Z}$ be a positive integer. Then :*

$$R_D(n) = w \sum_{m|n} \left(\frac{D}{m}\right)$$

where w is given by (3) and $\left(\frac{D}{\cdot}\right)$ is the Kronecker symbol (see appendix B).

Proof. Follows immediately from the preceding corollary and theorem 2.3.1. □

According to a semester project report [PG12], to have a nice correspondence between forms of discriminant D and ideals in quadratic fields when D is not a fundamental discriminant, one needs to work with orders in quadratic fields, and not only ring of integers.

2.4 Dirichlet class number formula for imaginary quadratic fields

For this section, the following references have been of great help : [PG12], who took inspiration from [Gra07] (and the latter refers to the book of Davenport [Dav80]).

The aim is to prove the following theorem, which makes a connection between the value at 1 of the Dirichlet L-function associated with the character $\left(\frac{D}{\cdot}\right)$ and the class number of the imaginary quadratic field $K = \mathbf{Q}(\sqrt{D})$.

Theorem 2.4.1 (Dirichlet class number formula). *Let D be a negative fundamental discriminant, $K = \mathbf{Q}(\sqrt{d})$ an imaginary quadratic field with discriminant D. Let us denote by $\chi_D := \left(\frac{D}{\cdot}\right)$ the Kronecker symbol (see appendix B). Then*

$$L(1, \chi_D) = \frac{2\pi}{w\sqrt{|D|}} |\mathrm{Cl}(\mathcal{O}_K)|$$

where w still denotes the number of units in $\mathcal{O}_K$.

Proof. With the notations introduced before, the main idea is to evaluate in two different ways the quantity

$$\lim_{N\infty} \frac{1}{N} \sum_{n=1}^{N} R_D(n).$$

- *The first way :* we replace $R_D(n)$ by its expression in terms of χ_D (theorem 2.3.5). This gives

$$\frac{1}{N}\sum_{n=1}^{N} R_D(n) = \frac{1}{N}\sum_{n=1}^{N} w \sum_{m|n} \chi_D(m) = \frac{w}{N} \sum_{1\leqslant m_1 \leqslant N} \underbrace{\sum_{1\leqslant m_2 \leqslant \frac{N}{m_1}}}_{\left\lfloor \frac{N}{m_1} \right\rfloor \text{ terms}} \chi_D(m_1)$$

$$= \frac{w}{N} \sum_{1\leqslant m\leqslant N} \left\lfloor \frac{N}{m} \right\rfloor \chi_D(m)$$

We would like to approximate $\left\lfloor \frac{N}{m} \right\rfloor$ by $\frac{N}{m}$, in order to have a partial sum of $L(1, \chi_D)$. The problem is that if we are not subtle, we will get

$$\left| \sum_{1\leqslant m\leqslant N} \left\lfloor \frac{N}{m} \right\rfloor \chi_D(m) - \sum_{1\leqslant m\leqslant N} \frac{N}{m} \chi_D(m) \right| \leqslant \sum_{1\leqslant m\leqslant N} \underbrace{\left| \left\lfloor \frac{N}{m} \right\rfloor - \frac{N}{m} \right|}_{\leqslant 1} \underbrace{|\chi_D(m)|}_{\leqslant 1} \leqslant N$$

which is not a sufficiently good inequality to conclude that :

$$\lim_{N\infty} \frac{1}{N} \sum_{1\leqslant m\leqslant N} \left\lfloor \frac{N}{m} \right\rfloor \chi_D(m) \;=\; \lim_{N\infty} \frac{1}{N} \sum_{1\leqslant m\leqslant N} \frac{N}{m} \chi_D(m) = L(1, \chi_D).$$

Thus, we split the sum at some rank k (to be determined later), and control differently the first terms and the last terms.

$$\sum_{1\leqslant m\leqslant N} \left\lfloor \frac{N}{m} \right\rfloor \chi_D(m) = \sum_{1\leqslant m\leqslant k} \left\lfloor \frac{N}{m} \right\rfloor \chi_D(m) + \sum_{k< m\leqslant N} \left\lfloor \frac{N}{m} \right\rfloor \chi_D(m).$$

For the lowest values, we use just approximate $\left\lfloor \frac{N}{m} \right\rfloor$ by $\frac{N}{m}$ as follows :

$$\left| \sum_{1\leqslant m\leqslant k} \left\lfloor \frac{N}{m} \right\rfloor \chi_D(m) - \sum_{1\leqslant m\leqslant k} \frac{N}{m} \chi_D(m) \right| \leqslant \sum_{1\leqslant m\leqslant k} \underbrace{\left| \left\lfloor \frac{N}{m} \right\rfloor - \frac{N}{m} \right|}_{\leqslant 1} \underbrace{|\chi_D(m)|}_{\leqslant 1} \leqslant k \tag{7}$$

whereas for the highest values we proceed like this :

$$\sum_{k< m\leqslant N} \left\lfloor \frac{N}{m} \right\rfloor \chi_D(m) = \sum_{k< m\leqslant N} \sum_{1\leqslant \ell\leqslant \frac{N}{m}} \chi_D(m) = \sum_{1\leqslant \ell< \frac{N}{k}} \sum_{k< m\leqslant \frac{N}{\ell}} \chi_D(m)$$

So that :

$$\left|\sum_{k<m\leqslant N}\left\lfloor\frac{N}{m}\right\rfloor\chi_D(m)\right| \leqslant \sum_{1\leqslant\ell<\frac{N}{k}}\underbrace{\left|\sum_{k<m\leqslant\frac{N}{\ell}}\chi_D(m)\right|}_{\leqslant|D| \text{ by lemma A.4}} \leqslant \frac{|D|N}{k} \tag{8}$$

Thus, if we choose $k := \lfloor\sqrt{N}\rfloor$, we obtain :

$$\begin{aligned}\sum_{1\leqslant m\leqslant N}\left\lfloor\frac{N}{m}\right\rfloor\chi_D(m) &= \sum_{1\leqslant m\leqslant\lfloor\sqrt{N}\rfloor}\left\lfloor\frac{N}{m}\right\rfloor\chi_D(m) + \sum_{\lfloor\sqrt{N}\rfloor<m\leqslant N}\left\lfloor\frac{N}{m}\right\rfloor\chi_D(m)\\ &\underset{N\infty}{=} \sum_{1\leqslant m\leqslant\lfloor\sqrt{N}\rfloor}\frac{N}{m}\chi_D(m) + O(\sqrt{N}) + O(\sqrt{N})\end{aligned}$$

thanks to (7) and (8). Note that the implied constants in the "$O(\sqrt{N})$" can depend on D since we work with a fixed discriminant. Then :

$$\begin{aligned}\frac{1}{N}\sum_{n=1}^{N}R_D(n) &= \frac{w}{N}\sum_{1\leqslant m\leqslant N}\left\lfloor\frac{N}{m}\right\rfloor\chi_D(m)\\ &\underset{N\infty}{=} \frac{w}{N}\left(\sum_{1\leqslant m\leqslant\lfloor\sqrt{N}\rfloor}\frac{N}{m}\chi_D(m) + O(\sqrt{N})\right)\\ &\underset{N\infty}{=} w\sum_{1\leqslant m\leqslant\lfloor\sqrt{N}\rfloor}\frac{\chi_D(m)}{m} + o(1)\end{aligned}$$

and so :

$$\frac{1}{N}\sum_{n=1}^{N}R_D(n) \underset{N\infty}{\longrightarrow} wL(1,\chi_D) \tag{9}$$

(here we used the fact that the L-function associated with χ_D is still well-defined at 1. This is a consequence of the general fact that we recall in appendix A, proposition A.8).

- *The second way :* we use the definition of $R_D(n)$. Let us denote by $\mathcal{S} := \{\varphi_1, \ldots, \varphi_h\}$ a complete system of non-equivalent forms modulo the action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathcal{Q}_D^+$ (for instance, one can take the φ_i's reduced in the sense of definition 2.2.5). Note that $h = |\mathrm{Cl}(\mathcal{O}_K)|$ by the correspondence we proved between binary quadratic forms and the class group. We recall that we introduced the notation

$$r_i(n) := \left\{(x,y)\in\mathbf{Z}^2 \mid \varphi_i(x,y) = n\right\}.$$

and that $R_D(n)$ was defined as the sum of the numbers $r_i(n)$. Thus,

$$\frac{1}{N}\sum_{n=1}^{N}R_D(n) = \frac{1}{N}\sum_{n=1}^{N}\sum_{i=1}^{h}r_i(n) = \sum_{i=1}^{h}\frac{1}{N}\sum_{n=1}^{N}r_i(n)$$

Now, we are going to prove that $\dfrac{1}{N}\displaystyle\sum_{n=1}^{N}r_i(n)$ converges as N goes to infinity, and that the limit does not depend on i. Let us denote $\varphi_i = aX^2 + bXY + cY^2$, with $b^2 - 4ac = D$ and $a > 0$. Then the sum $1 + \displaystyle\sum_{n=1}^{N}r_i(n)$ equals the number of pairs of integers (u,v) belonging to the domain

$$\mathscr{E} := \left\{(x,y)\in\mathbf{R}^2 \mid ax^2 + bxy + cy^2 \leqslant N\right\}$$

(the $+1$ is just here to count the solution $(0,0)$, which is the only representation of 0 by φ_i since we work with forms that are positive definite).

As in the famous Gauss circle problem, we can prove that the number of integer points in the domain $\mathscr{E}$ (which is the area of the plane delimited by an ellipse) is the area of the domain + an error term of the size of the perimeter. This can be proved by covering $\mathscr{E}$ by unit squares centered at the integer points. I refer to [PG12] for more details on this part. In the end, we get that

$$1+\sum_{n=1}^{N} r_i(n) \underset{N\infty}{=} \text{Area}(\mathscr{E}) + O(\sqrt{N})$$

We don't do the computation and take as a fact that

$$\text{Area}(\mathscr{E}) = \frac{2\pi}{\sqrt{|D|}}N$$

so that $\frac{1}{N}\sum_{n=1}^{N} r_i(n) \underset{N\infty}{\longrightarrow} \frac{2\pi}{\sqrt{|D|}}$. This is indeed independent of i, and so we deduce that

$$\frac{1}{N}\sum_{n=1}^{N} R_D(n) \underset{N\infty}{\longrightarrow} \frac{2\pi h}{\sqrt{|D|}} \tag{10}$$

Comparing the limits obtained via the two methods (equations (9) and (10)) gives the Dirichlet class number formula for imaginary quadratic fields :

$$L(1,\chi_D) = \frac{2\pi}{w\sqrt{|D|}}|\text{Cl}(\mathcal{O}_K)|$$

□

Besides, there is a strong connection between $L(\,\cdot\,,\chi_D)$ and the zeta fonction of $K=\mathbf{Q}(\sqrt{d})$.

Proposition 2.4.2. *For all $s\in\mathbf{C}$ such that $\text{Re}(s)>1$,*

$$\zeta_K(s) = \zeta(s)L(s,\chi_D)$$

Proof. Let $s\in\mathbf{C}$ such that $\text{Re}(s)>1$. By proposition 1.6.11, we have

$$\zeta_K(s) = \prod_{\mathfrak{p}}\left(1-\frac{1}{\text{N}(\mathfrak{p})^s}\right)^{-1}$$

We split this product in three parts : a product over the prime ideals lying over a split rational prime, a product over the prime ideals lying over a totally ramified rational prime, and a product over the inert primes.

$$\zeta_K(s) = \prod_{p \text{ split}}\prod_{\mathfrak{p}|p}\left(1-\frac{1}{\text{N}(\mathfrak{p})^s}\right)^{-1} \times \prod_{p \text{ tot. ram.}}\prod_{\mathfrak{p}|p}\left(1-\frac{1}{\text{N}(\mathfrak{p})^s}\right)^{-1} \times \prod_{p \text{ inert}}\prod_{\mathfrak{p}|p}\left(1-\frac{1}{\text{N}(\mathfrak{p})^s}\right)^{-1}$$

We can replace $\text{N}(\mathfrak{p})$ by its value, according to the paragraph above proposition 2.1.8. This gives :

$$\zeta_K(s) = \prod_{p \text{ split}}\underbrace{\prod_{\mathfrak{p}|p}\left(1-\frac{1}{p^s}\right)^{-1}}_{\text{two factors}} \times \prod_{p \text{ tot. ram.}}\underbrace{\prod_{\mathfrak{p}|p}\left(1-\frac{1}{p^s}\right)^{-1}}_{\text{only one factor}} \times \prod_{p \text{ inert}}\underbrace{\prod_{\mathfrak{p}|p}\left(1-\frac{1}{p^{2s}}\right)^{-1}}_{\text{only one factor}}$$

hence

$$\begin{aligned}\zeta_K(s) &= \prod_{p \text{ split}} \left(1-\frac{1}{p^s}\right)^{-2} \times \prod_{p \text{ tot. ram.}} \left(1-\frac{1}{p^s}\right)^{-1} \times \prod_{p \text{ inert}} \left(1-\frac{1}{p^{2s}}\right)^{-1} \\ &= \prod_{p} \left(1-\frac{1}{p^s}\right)^{-1} \times \prod_{p \text{ split}} \left(1-\frac{1}{p^s}\right)^{-1} \prod_{p \text{ inert}} \left(1+\frac{1}{p^s}\right)^{-1}\end{aligned}$$

Here we used the identity $1-\frac{1}{p^{2s}} = \left(1-\frac{1}{p^s}\right)\left(1+\frac{1}{p^s}\right)$. In this last factorization of ζ_K, the first product is the Euler product of the Riemann Zeta function, and the second part is exactly

$$\prod_p \left(1-\frac{\chi_D(p)}{p^s}\right)^{-1}$$

which is equal to $L(s,\chi_D)$ by proposition A.6 (in the appendix on L-functions). This gives the result. □

Since we know that ζ has an analytic continuation to $\mathbf{C}$ with a single pole at $s=1$, where the residue equals 1, we deduce the following corollary :

Corollary 2.4.3. *Let $K = \mathbf{Q}(\sqrt{d})$ be an imaginary quadratic field with discriminant D. Then we have :*

$$\text{res}_{s=1}\zeta_K(s) = \frac{2\pi}{w\sqrt{|D|}}|\text{Cl}(\mathcal{O}_K)|$$

We proved this statement only for imaginary quadratic fields, but in fact if K is any number field, a similar analytic formula for the class number also holds. A precise statement and a proof can be found in [Lan94].

3. Sums of three squares

The aim of this section is to start the core of this master thesis, namely the study of integer points on spheres. We answer the first question that arises when studying such a problem : "when are there integer points on a sphere ?".

The sphere of radius $\sqrt{d}$ is the set of points $(x, y, z) \in \mathbf{R}^3$ such that $x^2 + y^2 + z^2 = d$. We will denote by $\mathscr{R}_3(d)$ the set of integers points :

$$\mathscr{R}_3(d) = \{(x, y, z) \in \mathbf{Z}^3 \mid x^2 + y^2 + z^2 = d\}$$

The question we try to answer in this section is "for which values of d is $\mathscr{R}_3(d)$ non-empty ?"
In other words, which integers can be written as the sum of three squares of integers ?
Once we know when it is non-empty, the next natural question is to estimate the size of this set. That is why we also introduce a notation for the number of integer points : $r_3(d) := |\mathscr{R}_3(d)|$.

In this thesis, we focus on the case of two-dimensional spheres, but the question is also interesting in other dimensions. For all $m \in \mathbf{N}^*$, we will denote $\mathscr{R}_m(d)$ the set of $(x_1, \ldots, x_m) \in \mathbf{Z}^m$ such that $x_1^2 + \cdots + x_m^2 = d$ and by $r_m(d)$ the cardinality of $\mathscr{R}_m(d)$: the number of representations of d as a sum of m squares.

For spheres of dimension 1, the question becomes : which integers are the sum of two squares ? (or equivalently : when is $\mathscr{R}_2(d)$ non-empty ?). The classical way to answer this question is to work in the ring $\mathbf{Z}[i]$ of gaussian integers, where the question becomes : which numbers arise as the norm of a gaussian integer ? By multiplicativity of the norm, it is even sufficient to answer the question : which prime numbers arise as the norm of a gaussian integer ? We obtain the following reformulation of theorem 2.2.2 :

Theorem 3.0.1. *For all $d \in \mathbf{N}^*$, $\mathscr{R}_2(d)$ is non-empty if and only if every prime factor p of d satisfying $p \equiv 3 \bmod 4$ appears with an even power in the factorization of d. Moreover, the number of representations of d as a sum of two squares is also known :*

$$r_2(d) := |\mathscr{R}_2(d)| = 4(d_1(d) - d_3(d))$$

where $d_i(d)$ denotes the number of divisors of d (not necessarily prime) that are congruent to i modulo 4.

Proof. At the end of [RMS18], there is a nice problem, with a lot of intermediate questions leading to this result, starting almost from highschool level. □

For three-dimensional spheres, the result is also well known, and there is an elegant proof due to Venkov ([Ven22], [Ven29]) which follows exactly the steps of the proof of the two-square theorem, except that the ring $\mathbf{Z}[i]$ is replaced by the (non-commutative) ring of Hurwitz quaternions (we give more details in the sequel).

Theorem 3.0.2. *Every natural number $d \in \mathbf{N}$ is a sum of four squares, i.e. for all $d \in \mathbf{N}$, $\mathscr{R}_4(d)$ is non-empty. Moreover, there is also a formula for the number of representations :*

$$r_4(d) = |\mathscr{R}_4(d)| = 8 \sum_{m|d,\ 4\nmid m} m$$

Proof. For the fact that every integer $d \geqslant 0$ is a sum of four squares, the proof based on quaternions is detailed in [Hin08], chapter III, or also in [Sam71]. For the number of representations (this part of the statement is called Jacobi's four-square theorem), many methods and references are given in this mathoverflow discussion :
https://mathoverflow.net/questions/84897/proofs-of-jacobis-four-square-theorem. □

Now, our aim in this section is to get a statement similar to theorems 3.0.1 and 3.0.2 for sums of three squares. We start by reminders on Hurwitz quaternions, since they will be useful at the end of the proof. Indeed, using a local-global principle, we will be able to deduce, starting from representations as sums of three squares in $\mathbf{Q}_p$, representations of an integer as a sum of three squares in $\mathbf{Q}$. Then, it is the fact that the ring of Hurwitz quaternions is euclidean (and some corollaries of this fact) that will allow us to deduce representations as sums of three squares in $\mathbf{Z}$.

3.1 Quaternions

This section contains generalities on quaternions, that one can find in [Sam71] section 5.7, or [Hin08], chapter III (in both references, the aim is to prove the four-square theorem using quaternions). However, we use the same notations as in [EMV10], because it is our main reference for the proof of the three-square theorem.

We denote by $\mathrm{B}(\mathbf{Q})$ the $\mathbf{Q}$-algebra of Hamilton quaternions. It is a $\mathbf{Q}$-vector space of dimension 4, with a basis denoted by $(1, i, j, k)$. The multiplication in $\mathrm{B}(\mathbf{Q})$ is defined by the rules :

$$i^2 = j^2 = k^2 = -1 \text{ and } ij = -ji = k.$$

Endowed with this multiplication, $\mathrm{B}(\mathbf{Q})$ is a non-commutative $\mathbf{Q}$-algebra. The elements of $\mathrm{B}(\mathbf{Q})$ are called quaternions. They can all be written uniquely as $u + ai + bj + ck$ with $(u, a, b, c) \in \mathbf{Q}^4$.

Definition 3.1.1. *If $x = u + ai + bj + ck \in \mathrm{B}(\mathbf{Q})$, we define :*

- *its conjugate* $\overline{x} := u - ai - bj - ck$
- *it reduced trace* $\mathrm{Tr}(x) := x + \overline{x} = 2u$
- *its reduced norm* $\mathrm{N}(x) := x\overline{x} = u^2 + a^2 + b^2 + c^2$

Note that for all $x, y \in \mathrm{B}(\mathbf{Q})$, we have $\overline{x+y} = \overline{x} + \overline{y}$ but $\overline{xy} = \overline{y}\ \overline{x}$ (it reverses the order of multiplication).

One can view $\mathrm{B}(\mathbf{Q})$ as a subset of $\mathcal{M}_2(\mathbf{C})$ by identifying 1 with $\mathbf{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, i with $I := \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}$, j with $J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and k with $K := \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$. Then $\mathrm{B}(\mathbf{Q})$ is the sub-$\mathbf{Q}$-vector space of $\mathcal{M}_2(\mathbf{C})$ generated by these four matrices :

$$\mathrm{B}(\mathbf{Q}) = \left\{ u\mathbf{1} + aI + bJ + cK,\ (u, a, b, c) \in \mathbf{Q}^4 \right\}$$

It is easy to verify that the trace of a quaternion coincides with the trace of the associated matrix, and that its norm is nothing but the determinant of the associated matrix when we see $\mathrm{B}(\mathbf{Q})$ as a subset of $\mathcal{M}_2(\mathbf{C})$ under the above identifications. This gives an easy proof of the following properties.

Proposition 3.1.2. *If $x, y \in \mathrm{B}(\mathbf{Q})$, then*

- $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$
- $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$
- $x^2 - \mathrm{Tr}(x)x + \mathrm{N}(x) = 0$.

We also have that $\mathrm{B}(\mathbf{Q})$ is a division ring : for every $x \in \mathrm{B}(\mathbf{Q}) \setminus \{0\}$, $\mathrm{N}(x) > 0$ and we have $x\frac{\overline{x}}{\mathrm{N}(x)} = 1$. As $\frac{\overline{x}}{\mathrm{N}(x)}$ belongs to $\mathrm{B}(\mathbf{Q})$, this shows that any non-zero quaternion is invertible, and its inverse is given by $\frac{\overline{x}}{\mathrm{N}(x)}$. Therefore, the set of units in $\mathrm{B}(\mathbf{Q})$, denoted by $\mathrm{B}^\times$, is nothing but $\mathrm{B}(\mathbf{Q}) \setminus \{0\}$. It is a non commutative group for the multiplication of quaternions, and it is not hard to prove that its center,

denoted by $\mathcal{Z}(\mathrm{B}^\times)$, is $\mathbf{Q}^\times 1$. We will often forget the "1" because we see $\mathbf{Q}$ as a subset of $\mathrm{B}(\mathbf{Q})$ by identifying $\mathbf{Q}$ and $\mathbf{Q}1$. We also introduce the notation

$$\mathrm{PB}^\times := \mathrm{B}^\times/\mathcal{Z}(\mathrm{B}^\times) = \mathrm{B}^\times/\mathbf{Q}^\times \tag{11}$$

Since elements of $\mathbf{Q}^\times$ commute with all the other quaternions, conjugation by those elements is the identity of $\mathrm{B}^\times$. This is why the group that we are naturally led to consider when working with inner automorphisms of $\mathrm{B}^\times$ is $\mathrm{PB}^\times$. We will see this in section 4.1.

Definition 3.1.3. *We denote by* $\mathrm{B}^{(0)}(\mathbf{Q})$ *the set of trace-free quaternions, also called pure quaternions :*

$$\mathrm{B}^{(0)}(\mathbf{Q}) := \{x \in \mathrm{B}(\mathbf{Q}) \mid \mathrm{Tr}(x) = 0\} = \{ai + bj + ck,\ (a,b,c) \in \mathbf{Q}^3\}$$

Finally, we also introduce the ring of Hurwitz quaternions :

$$\mathrm{B}(\mathbf{Z}) := \mathbf{Z}1 + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k + \mathbf{Z}\delta, \quad \text{where } \delta := \frac{1+i+j+k}{2}$$

It is the set of quaternions $u + ai + bj + ck$ where u, a, b, c are either all in $\mathbf{Z}$ or all in $\mathbf{Z} + \frac{1}{2}$.
It is not hard to check that $\mathrm{B}(\mathbf{Z})$ is a subring of $\mathrm{B}(\mathbf{Q})$, and a free $\mathbf{Z}$-module of rank 4 (a basis is given by i, j, k, δ) : we say that it is an order of $\mathrm{B}(\mathbf{Q})$. This order looks less natural to consider than $\mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k$, but it has nicer properties. First of all, the norms of elements in $\mathrm{B}(\mathbf{Z})$ reach exactly the same integers as the norms of elements in $\mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k$, i.e.

$$\mathrm{N}(\mathrm{B}(\mathbf{Z})) = \mathrm{N}(\mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k) = \{u^2 + a^2 + b^2 + c^2,\ (u,a,b,c) \in \mathbf{Z}^4\}.$$

This is an important fact in the proof of the four-square theorem, since the right-hand side is exactly the set of numbers that can be written as a sum or four squares, but on the left hand side, the ring $\mathrm{B}(\mathbf{Z})$ has nice properties. The main result is that $\mathrm{B}(\mathbf{Z})$ is (both left and right)-euclidean. Let us make this statement more precise.

Theorem 3.1.4. $\mathrm{B}(\mathbf{Z})$ *is left-euclidean with respect to the reduced norm i.e. for all* $x \in \mathrm{B}(\mathbf{Z})$ *and* $y \in \mathrm{B}(\mathbf{Z}) \setminus \{0\}$ *there exists a unique* $(q, r) \in \mathrm{B}(\mathbf{Z})^2$ *such that*

$$\begin{cases} x = qy + r \\ \mathrm{N}(r) < \mathrm{N}(y) \end{cases}$$

Similarly, $\mathrm{B}(\mathbf{Z})$ *is right-euclidean with respect to the reduced norm (the property required is the same, just replace* $x = qy + r$ *by* $x = yq + r$*).*

Proof. See [Hin08], chapter III. □

In particular, this implies that every left ideal is principal (and similarly for right ideals).

Corollary 3.1.5. *Let* $\mathfrak{a} \subseteq \mathrm{B}(\mathbf{Z})$ *be a left ideal (i.e. an additive subgroup of* $\mathrm{B}(\mathbf{Z})$ *such that* $\mathrm{B}(\mathbf{Z})\mathfrak{a} \subseteq \mathfrak{a}$ *: we just require stability under multiplication on the left by elements of the ring). Then there exists* $y \in \mathfrak{a}$ *such that* $\mathfrak{a} = \mathrm{B}(\mathbf{Z})y$*. Similarly, any right ideal* $\mathfrak{b}$ *of* $\mathrm{B}(\mathbf{Z})$ *is of the form* $y\mathrm{B}(\mathbf{Z})$ *for some* $y \in \mathfrak{b}$*.*

Proof. The proof is the same proof as in the commutative case, when we show that an euclidean ring is a PID. Let $\mathfrak{a}$ be a left ideal of $\mathrm{B}(\mathbf{Z})$. If $\mathfrak{a} = \{0\}$ then we just have to take $y = 0$. Otherwise, when $\mathfrak{a} \neq \{0\}$, there is an element of minimal non-zero norm : let us denote by $y \in \mathfrak{a}$ such an element. It satisfies

$$\mathrm{N}(y) = \min_{y' \in \mathfrak{a} \setminus \{0\}} \mathrm{N}(y').$$

Then of course $\mathrm{B}(\mathbf{Z})y \subseteq \mathfrak{a}$ (just because $y \in \mathfrak{a}$ and $\mathfrak{a}$ is a left ideal). Conversely, if $x \in \mathfrak{a}$, let us write the euclidean division of x by y (theorem 3.1.4) : there exists a unique $(q, r) \in \mathrm{B}(\mathbf{Z})$ such that

$$\begin{cases} x = qy + r \\ \mathrm{N}(r) < \mathrm{N}(y) \end{cases}$$

Then $r = x - qy \in \mathrm{B}(\mathbf{Z})$ and its norm is less than $\mathrm{N}(y)$. By minimality of $\mathrm{N}(y)$, this implies that $r = 0$, hence $x = qy \in \mathrm{B}(\mathbf{Z})y$. This proves that $\mathfrak{a} = \mathrm{B}(\mathbf{Z})y$. The case of right ideals goes the same way. □

Corollary 3.1.6. *If $M \subseteq \mathrm{B}(\mathbf{Q})$ is a finitely generated left $\mathrm{B}(\mathbf{Z})$-module, then M is of the form $\mathrm{B}(\mathbf{Z})z$ for some $z \in \mathrm{B}(\mathbf{Q})$. Similarly, any finitely generated right $\mathrm{B}(\mathbf{Z})$-module is of the form $z\mathrm{B}(\mathbf{Z})$.*

Proof. Let $M = \mathrm{B}(\mathbf{Z})x_1 + \cdots + \mathrm{B}(\mathbf{Z})x_n$ be a finitely generated left $\mathrm{B}(\mathbf{Z})$-submodule of $\mathrm{B}(\mathbf{Q})$. For all $m \in \{1, \ldots, n\}$, we can write $x_m = u_m + a_m i + b_m j + c_m k$ for some $(u_m, a_m, b_m, c_m) \in \mathbf{Q}^4$. Therefore, if we multiply by some integer r sufficiently large to clear all the denominators of the u_m, a_m, b_m, c_m for all m, then $rM \subseteq \mathrm{B}(\mathbf{Z})$ and so rM is a left ideal in $\mathrm{B}(\mathbf{Z})$. So we can find $y \in \mathrm{B}(\mathbf{Z})$ such that $rM = \mathrm{B}(\mathbf{Z})y$ by the preceding corollary. Thus, $M = \mathrm{B}(\mathbf{Z})z$ with $a := \frac{y}{r} \in \mathrm{B}(\mathbf{Q})$. Note that we used the fact that $\frac{1}{r}\mathrm{B}(\mathbf{Z}) = \mathrm{B}(\mathbf{Z})\frac{1}{r}$, which is true because $\mathbf{Q}1$ is contained in the center of $\mathrm{B}(\mathbf{Q})$ (it is fact equal to the center). □

Corollary 3.1.7. *If R is a subring of $\mathrm{B}(\mathbf{Q})$ which is finitely generated as a $\mathbf{Z}$-module, then it is conjugate to a subring of $\mathrm{B}(\mathbf{Z})$.*

Proof. Let $R = \mathbf{Z}x_1 + \cdots + \mathbf{Z}x_n$ be a subring of $\mathrm{B}(\mathbf{Q})$, finitely generated as a $\mathbf{Z}$-module. Then $R\mathrm{B}(\mathbf{Z})$, the right $\mathrm{B}(\mathbf{Z})$-submodule of $\mathrm{B}(\mathbf{Q})$ generated by R, consists of the finite sums of elements of the form xy, where $x \in R$ and $y \in \mathrm{B}(\mathbf{Z})$. It is easy to see that $x_1, \ldots, x_n$ generate $R\mathrm{B}(\mathbf{Z})$ as a $\mathrm{B}(\mathbf{Z})$-module. The preceding corollary then shows that there exists $z \in \mathrm{B}(\mathbf{Q})$ such that $R\mathrm{B}(\mathbf{Z}) = z\mathrm{B}(\mathbf{Z})$. This implies

$$z^{-1}Rz \subseteq z^{-1}RR\mathrm{B}(\mathbf{Z}) \subseteq z^{-1}R\mathrm{B}(\mathbf{Z}) = z^{-1}z\mathrm{B}(\mathbf{Z}) = \mathrm{B}(\mathbf{Z})$$

So $z^{-1}Rz$ is a subring of $\mathrm{B}(\mathbf{Z})$, and this concludes the proof. □

Finally, another important fact about the arithmetic of $\mathrm{B}(\mathbf{Z})$ is that the units are well known.

Proposition 3.1.8. *The group of units in the ring $\mathrm{B}(\mathbf{Z})$, denoted by $\mathrm{B}(\mathbf{Z})^\times$ is exactly the set of elements of norm 1. The explicit list is as follows :*

$$\mathrm{B}(\mathbf{Z})^\times = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}$$

Proof. Recall that a quaternion $z = u1 + ai + bj + ck$ is in $\mathrm{B}(\mathbf{Z})$ if and only if u, a, b, c are either all in $\mathbf{Z}$ or all in $\mathbf{Z} + \frac{1}{2}$. From this it is easy to see that the norm of a Hurwitz quaternion in always in $\mathbf{N}$.

- If $z \in \mathrm{B}(\mathbf{Z})$ is invertible (in $\mathrm{B}(\mathbf{Z})$), then there exists $z' \in \mathrm{B}(\mathbf{Z})$ such that $zz' = 1$. Then by multiplicativity of the norm : $\mathrm{N}(z)\mathrm{N}(z') = 1$. But since $\mathrm{N}(z), \mathrm{N}(z') \in \mathbf{N}$, this implies that $\mathrm{N}(z) = \mathrm{N}(z') = 1$.
- Conversely, if $z \in \mathrm{B}(\mathbf{Z})$ has norm 1, then $z\overline{z} = 1$, and $\overline{z} \in \mathrm{B}(\mathbf{Z})$ since $\mathrm{B}(\mathbf{Z})$ is clearly stable under conjugation. Thus, $z \in \mathrm{B}(\mathbf{Z})^\times$ and $z^{-1} = \overline{z}$.

Now it is easy to see which elements of $\mathrm{B}(\mathbf{Z})$ have norm 1, and this leads to the explicit list given. □

3.2 Sums of three squares in $\mathbf{Q}_p$

As we said at the beginning of the section, the strategy to prove the three-square theorem is to use a local-global principle, together with the fact that finding representations as a sum of three squares is easier in $\mathbf{Q}_p$ than in $\mathbf{Q}$. The reason why we can find roots of polynomials more easily in $\mathbf{Q}_p$ is because Newton's lemma holds in such fields. This lemma is sometimes called Hensel's lemma too. Let us give a statement for complete non-archimedean valued fields, $\mathbf{Q}_p$ with the p-adic value being a field of this kind.

Theorem 3.2.1 (Newton's lemma)**.** *Let $(K, |\cdot|)$ be a complete non-archimedean valued field, with ring of integers $\mathcal{O}_K$. Let $P \in \mathcal{O}_K[X]$ and $\alpha \in \mathcal{O}_K$. Assume there exists $\varepsilon \in [0, 1[$ such that*

$$|P(\alpha)| \leqslant \varepsilon |P'(\alpha)|^2$$

Then, there exists a unique $\tilde{\alpha} \in \mathcal{O}_K$ such that $P(\tilde{\alpha}) = 0$ and $|\alpha - \tilde{\alpha}| \leqslant \varepsilon |P'(\alpha)|$.

Proof. See for instance the notes [Bri20]. □

Let us see how this lemma can be used to study sums of three squares in $\mathbf{Q}_p$. The reference [Gam06] helped me understanding the next two propositions. First, we assume that p is odd.

Proposition 3.2.2. *Let p be an odd prime and $d \in \mathbf{Z}$. Then d is the sum of three squares in $\mathbf{Z}_p$ (so it is a sum of three squares in $\mathbf{Q}_p$).*

Proof. We look at the equation $x^2 + y^2 + z^2 = d$. We choose to look for solutions $(x, y, z) \in \mathbf{Z}_p^3$ with $z = 1$. Then the question is to show that there are p-adic integers $x, y \in \mathbf{Z}_p$ such that $x^2 + y^2 + 1 = d$, i.e. $x^2 + 1 = d - y^2$. But while x runs over $\mathbf{F}_p$, x^2 takes $\frac{p+1}{2}$ distinct values in $\mathbf{F}_p$ (because when p is odd, there are $\frac{p-1}{2}$ squares in $\mathbf{F}_p^\times$ and $\frac{p-1}{2}$ non-squares. So if we also count zero, which is a square, we obtain that the number of squares in $\mathbf{F}_p$ is $\frac{p+1}{2}$). This implies that $x^2 + 1$ also takes $\frac{p+1}{2}$ distinct values in $\mathbf{F}_p$. The same argument shows that while y runs over $\mathbf{F}_p$, $d - y^2$ takes $\frac{p+1}{2}$ distinct values in $\mathbf{F}_p$. In other words, if we denote

$$A := \{x^2 + 1,\ x \in \mathbf{F}_p\} \text{ and } B := \{d - y^2,\ y \in \mathbf{F}_p\}$$

we have $|A| = |B| = \frac{p+1}{2}$. As $|A \cup B| = |A| + |B| - |A \cap B| \leqslant p$ (because $A \cup B \subseteq \mathbf{F}_p$), this implies that $A \cap B \neq \emptyset$.
Let $x, y \in \mathbf{Z}$ be such that that their reduction modulo p (denoted $\overline{x}, \overline{y}$) satisfy $\overline{x}^2 + 1 = d - \overline{y}^2$ in $\mathbf{F}_p$. Then the polynomial $P(Z) := Z^2 + x^2 + y^2 - d$ is in $\mathbf{Z}[Z] \subseteq \mathbf{Z}_p[Z]$. Moreover, $1 \in \mathbf{Z} \subseteq \mathbf{Z}_p$ and $|P(1)|_p \leqslant \frac{1}{p}$ because by the choice of x and y, $1+x^2+y^2-d$ is divisible by p. Besides, $\frac{1}{p} = \frac{1}{p}|P'(1)|_p^2$ since $P'(1) = 2$, which has p-adic absolute value equal to 1 since p is odd. Thus, we have $|P(1)|_p \leqslant \varepsilon |P'(1)|_p^2$, with $\varepsilon = \frac{1}{p} \in [0, 1[$, so Newton's lemma applies. In particular, it tells us that there exists $z \in \mathbf{Z}_p$ such that $P(z) = 0$. Then $(x, y, z) \in \mathbf{Z}_p^3$ is a representation of d as a sum of three squares in $\mathbf{Z}_p$. □

Now, let us deal with the case $p = 2$.

Proposition 3.2.3. *If $d \in \mathbf{Z}$ is not of the form $4^a(8b + 7)$, then it is the sum of three squares in $\mathbf{Q}_2$.*

Proof. Let us write $d = 4^a d'$ with $4 \nmid d'$ (we just factorize the highest power of 4 that we can). Then it is sufficient to show that d' is a sum of three squares in $\mathbf{Q}_2$. Indeed, if we can write $d' = x^2 + y^2 + z^2$, then

$$d = 4^a d' = (2^a x)^2 + (2^a y)^2 + (2^a z)^2$$

so it is also a sum of three squares in $\mathbf{Q}_2$. Now since d' is not divisible by 4, and not congruent to 7 modulo 8 by assumption, we have $d' \equiv 1, 2, 3, 5, 6 \bmod 8$. Now, we have the following table :

x	y	z	$x^2 + y^2 + z^2 \bmod 8$
0	0	1	1
0	1	1	2
1	1	1	3
2	0	1	5
2	1	1	6

which tells us that for any possible value of d' modulo 8, there exist $x, y \in \mathbf{Z}$ such that $x^2 + y^2 + 1 \equiv d' \bmod 8$. Then, the polynomial $P(Z) := Z^2 + x^2 + y^2 - d'$ belongs to $\mathbf{Z}[Z] \subseteq \mathbf{Z}_2[Z]$ and satisfies $8 \mid P(1)$, so $|P(1)|_2 \leqslant \frac{1}{8}$. On the other hand, $P'(1) = 2$, so $|P'(1)|_2 = \frac{1}{2}$. Thus, $|P(1)|_2 \leqslant \varepsilon |P'(1)|^2$ with $\varepsilon = \frac{1}{2} \in [0, 1[$. So we can apply Newton's lemma to obatin the existence of a root $z \in \mathbf{Z}_2$ for the polynomial P. Then $(x, y, z) \in \mathbf{Z}_2^3$ is a representation of d' as a sum of three squares in $\mathbf{Q}_2$. □

3.3 Hasse-Minkowski local-global principle

In order to prove the three-square theorem, we will use a well known local-global principle. In this section, we just state the result and refer to [Ser70], or [Gam06] for a proof.

This theorem is about representations of rationals by quadratic forms over $\mathbf{Q}$, so we start by introducing some notations and vocabulary about quadratic forms.

Let K be field of characteristic different from 2, and let V be a vector space over K. Then a quadratic form on V is a map $q\colon V \to K$ satisfying

(i) for all $x \in V$ and all $\lambda \in K$, $q(\lambda x) = \lambda^2 q(x)$.

(ii) the map $(x, y) \in V \times V \mapsto q(x + y) - q(x) - q(y)$ is a bilinear form.

We also define the bilinear form associated with q to be the map $b\colon (x, y) \mapsto \frac{1}{2}(q(x + y) - q(x) - q(y))$ (here we use the assumption $\mathrm{char}(K) \neq 2$). This form is clearly symmetric. Two vectors $x, y \in V$ are said to be *orthogonal* (with respect to the quadratic form q) if $b(x, y) = 0$. Finally, we say that q is *non-degenerate* when the only vector which is orthogonal to every vector of V is 0 i.e. when the implication "$b(x, \cdot) = 0_{V^*} \implies x = 0_V$" holds for all $x \in V$.

Definition 3.3.1. *Let $\alpha \in K^\times$. We say that a quadratic form $q\colon V \to K$ represents α if there exists $x \in V$ such that $q(x) = \alpha$.*

We will only work with the quadratic form "sum of three squares" over $\mathbf{Q}^3$. In this case, the base field is $\mathbf{Q}$, and the vector space is $V := \mathbf{Q}^3$. The quadratic form we study is (writing $x = (x_1, x_2, x_3)$) :

$$\begin{array}{ccccc} q_3 & : & \mathbf{Q}^3 & \to & \mathbf{Q} \\ & & x & \mapsto & x_1^2 + x_2^2 + x_3^2 \end{array}$$

The bilinear form associated with q_3 is the standard dot product on $\mathbf{Q}^3$:

$$b_3(x, y) = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = x_1y_1 + x_2y_2 + x_3y_3$$

so that q_3 is non-degenerated.

Although we will only need Hasse-Minkowski theorem for the quadratic form q_3, let us give the statement in a slightly more general setting :
Let $q\colon \mathbf{Q}^n \to \mathbf{Q}$ be a quadratic form in n variables. It can be the "diagonal form" :

$$x = (x_1, \ldots, x_n) \mapsto x_1^2 + \cdots + x_n^2$$

but also any homogeneous polynomial of degree 2, in n variables, with coefficients in $\mathbf{Q}$. For any prime number p, we can view $\mathbf{Q}$ as a subfield of the field $\mathbf{Q}_p$ of p-adic numbers, so the homogeneous polynomial defining q can also be seen as a polynomial with coefficients in $\mathbf{Q}_p$. Thus, we may extend q to a quadratic form on $\mathbf{Q}_p^n$, just by applying the same polynomial to entries $(x_1, \ldots, x_n) \in \mathbf{Q}_p^n$. Similarly, the inclusion of $\mathbf{Q}$ inside $\mathbf{R}$ allows us to extend q to a quadratic form on $\mathbf{R}^n$. We will still denote these quadratic forms by q : they are given by the same homogeneous polynomial with coefficients in $\mathbf{Q}$, we just apply the polynomial to entries in a larger field. With this little abuse of notation, if $a \in \mathbf{Q}^\times$, we will say that q represents a over $\mathbf{Q}_p$ (resp. $\mathbf{R}$), if there exists $(x_1, \ldots, x_n)$ in $\mathbf{Q}_p^n$ (resp. over $\mathbf{R}^n$) such that $q(x_1, \ldots, x_n) = a$.

Theorem 3.3.2 (Hasse-Minkowski). *Let $n \geqslant 2$ and let $q\colon \mathbf{Q}^n \to \mathbf{Q}$ be a non-degenerate quadratic form. Then for all $a \in \mathbf{Q}^\times$, q represents a over $\mathbf{Q}$ if and only if it represents a over $\mathbf{R}$ and over $\mathbf{Q}_p$ for every prime number p.*

In other words, if we apply this to the quadratic form q_3 : for all $a \in \mathbf{Q}^\times$, the equation

$$x_1^2 + x_2^2 + x_3^2 = a$$

has a solution (x_1, x_2, x_3) in $\mathbf{Q}^3$ if and only if it has a solution in $\mathbf{R}^3$ and a solution in $\mathbf{Q}_p^3$ for every prime p.

3.4 The three-square theorem

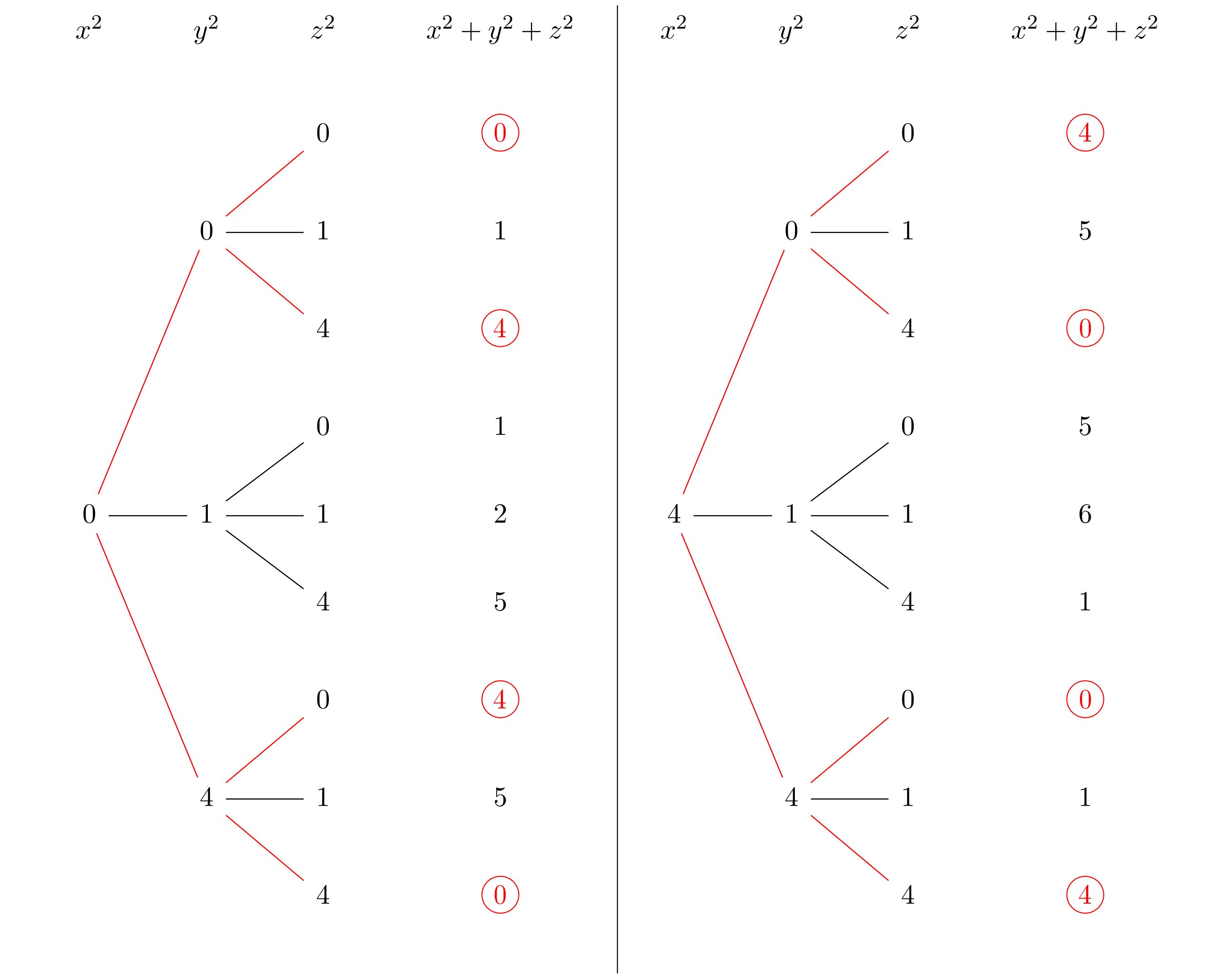
We can finally prove the three-square theorem. The question was studied by Legendre, but the proof he gave in 1798 was incomplete, because he assumed the existence of primes in arithmetic progressions, and this result was only proved by Dirichlet 40 years later. The first complete proof was published by Gauss in his *Disquisitiones Arithmeticae* (1801). We start by a lemma on squares modulo 8.

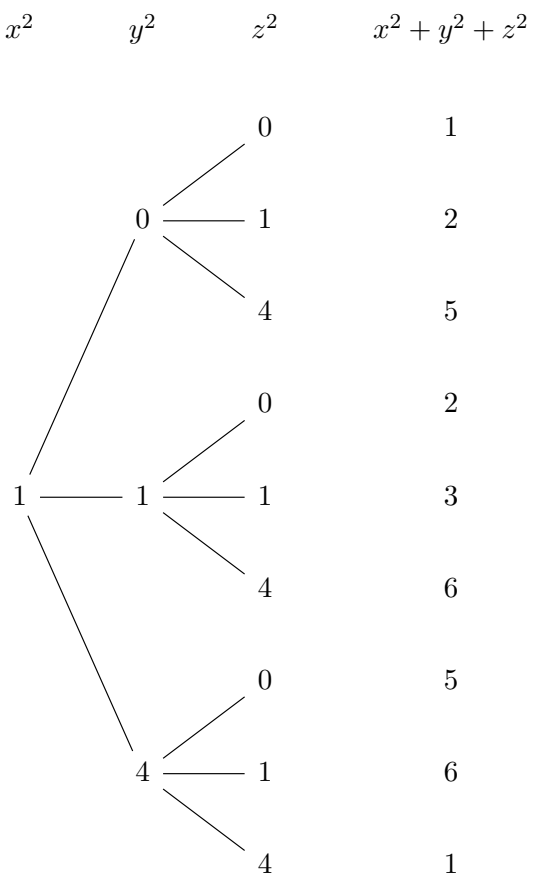
Lemma 3.4.1. *If $x, y, z \in \mathbf{Z}$, $x^2 + y^2 + z^2 \not\equiv 7 \bmod 8$. Moreover, $x^2 + y^2 + z^2 \equiv 0, 4 \bmod 8$ if and only if x, y and z are even.*

Proof. Reducing modulo 8 all the x^2 for $x \in \{0, \ldots, 7\}$ leads to the following table :

$x \bmod 8$	0	1	2	3	4	5	6	7
$x^2 \bmod 8$	0	1	4	1	0	1	4	1

In particular, for all $x \in \mathbf{Z}$, $x^2 \equiv 0, 1$ or $4 \bmod 8$. From this, one can just check every possibility and see that for all $x, y, z \in \mathbf{Z}$, $x^2 + y^2 + z^2 \not\equiv 7 \bmod 8$: the following trees list all the possibilities for $x^2 + y^2 + z^2$ modulo 8.





Moreover, we notice that $x^2+y^2+z^2 \equiv 0, 4 \bmod 8$ if and only if x^2, y^2 and z^2 are not congruent to 1 modulo 8, and this happens if and only if x, y and z are all even numbers. □

Theorem 3.4.2 (Legendre-Gauss). *An integer $d \in \mathbf{N}$ is the sum of three squares if and only if it is not of the form $4^a(8b+7)$ for some $a, b \in \mathbf{N}$.*

Proof. First, let us explain why the condition is necessary. Assume for a contradiction that there exists a number of the form $4^a(8b+7)$ which is representable as a sum of three squares. Define a_0 as follows :

$$a_0 := \min\{a \in \mathbf{N} \mid \exists b \in \mathbf{N}, 4^a(8b+7) \text{ is a sum of three squares}\}.$$

Then $a_0 \geqslant 1$ because a number of the form $8b+7$ cannot be a sum of three squares (by the previous lemma). Let $b \in \mathbf{N}$ and $(x, y, z) \in \mathbf{Z}^3$ be such that $4^{a_0}(8b+7) = x^2+y^2+z^2$. Since $a_0 \geqslant 1$, $x^2+y^2+z^2$ is divisible by 4, so it is congruent to 0 or 4 modulo 8. But this is only possible if x, y and z are even (by lemma 3.4.1). Then we can divide by 4 and get :

$$4^{a_0-1}(8b+7) = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$$

Since x, y and z are even, this is a representation of $4^{a_0-1}(8b+7)$ as a sum of three squares, which contradicts the minimality of a_0. Thus, no integer of the form $4^a(8b+7)$ is representable as a sum of three squares.

Conversely, if d is not of the form $4^a(8b+7)$, then for any prime p, the equation $x^2+y^2+z^2 = d$ has a solution $(x, y, z) \in \mathbf{Q}_p^3$ (by propositions 3.2.2 and 3.2.3). Moreover, since $d \geqslant 0$, it also has a solution in $\mathbf{R}$. Therefore, the Hasse-Minkowski local global principle gives us a solution in $\mathbf{Q}^3$: there exists $(a, b, c) \in \mathbf{Q}^3$ such that $a^2+b^2+c^2 = d$. In other words, there exists $z \in \mathrm{B}^{(0)}(\mathbf{Q})$ such that $\mathrm{N}(z) = d$. Since z is a pure quaternion, we have $\overline{z} = -z$, hence $\mathrm{N}(z) = z\overline{z} = -z^2$, so we deduce that $z^2 = -d$. In particular, $\mathbf{Z}[z] = \mathbf{Z} + \mathbf{Z}z$, so that $\mathbf{Z}[z]$ is finitely generated as a $\mathbf{Z}$-module. As it is also a subring of $\mathrm{B}(\mathbf{Q})$, corollary 3.1.7 implies that it is conjugate to a subring of $\mathrm{B}(\mathbf{Z})$. Let $q \in \mathrm{B}(\mathbf{Z})$ be such that

$q\mathbf{Z}[z]q^{-1} \subseteq \mathrm{B}(\mathbf{Z})$. Then in particular $qzq^{-1} \in \mathrm{B}(\mathbf{Z})$, but qzq^{-1} also belongs to $\mathrm{B}^{(0)}(\mathbf{Q})$ because being trace-free is stable under conjugation (if we see $\mathrm{B}(\mathbf{Q}) \subseteq \mathcal{M}_2(\mathbf{C})$, this is just saying that two similar matrices have the same trace). Thus, $qzq^{-1} \in \mathrm{B}^{(0)}(\mathbf{Q}) \cap \mathrm{B}(\mathbf{Z}) = \{ai + bj + ck,\ (a,b,c) \in \mathbf{Z}^3\}$ and $\mathrm{N}(qzq^{-1}) = \mathrm{N}(z) = d$, which proves that d is the sum of three squares of integers. □

Definition 3.4.3. *An integer that can be represented as a sum of three squares of integers will be called admissible.*

To get back to the notations of the introduction of this section on sums of squares : d is admissible if and only if $\mathscr{R}_3(d)$ is non empty.

4. Counting representations as a sum of three squares

We know from theorem 3.4.2 that $\mathscr{R}_3(d)$ is non empty if and only if d is not of the form $4^a(8b+7)$ for some $a, b \in \mathbf{N}$. The question we want to study now is the size of $\mathscr{R}_3(d)$. We will only study the case where d is square-free, in particular d is congruent to 1, 2, 3, 5 or 6 modulo 8 (the other possibilities are either excluded by the "square-free" assumption, or by the condition in theorem 3.4.2). In fact we can split the situation in two cases : either $d \equiv 1, 2 \bmod 4$, or $d \equiv 3 \bmod 8$. There is a slight difference between the two cases, and we will only give a full proof in the first case.

Given an admissible, square-free integer $d \geqslant 2$, such that $d \equiv 1, 2 \bmod 4$, we will denote by K the field $\mathbf{Q}(\sqrt{-d})$. As we will see, there is an action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\widetilde{\mathscr{R}_3}(d)^+$, where $\widetilde{\mathscr{R}_3}(d)^+$ is the quotient of $\mathscr{R}_3(d)$ under the natural action of $\mathrm{SO}_3(\mathbf{Z})^+$ (the notations are introduced in the section below). We prove in section 4.3 that this action is free and transitive, and this will lead to a surprising and beautiful relation between the class number of $K = \mathbf{Q}(\sqrt{-d})$ and $|\mathscr{R}_3(d)|$.

4.1 Geometric aspects of quaternions

In this section, we explain in detail some identifications that are useful to understand the action that will allow us to count the number of representations of an integer as a sum of three squares. This will give us a geometric point of view on some algebraic operations involving quaternions.

As $\mathrm{B}(\mathbf{Q})$ is not commutative, the action of $\mathrm{B}^\times$ $(= \mathrm{B}(\mathbf{Q}) \setminus \{0\})$ on $\mathrm{B}(\mathbf{Q})$ by conjugation is often non trivial. For all $x \in \mathrm{B}^\times$, we define

$$\begin{array}{rccc} \gamma_x & : & \mathrm{B}(\mathbf{Q}) & \to & \mathrm{B}(\mathbf{Q}) \\ & & z & \mapsto & xzx^{-1} \end{array}$$

(the "conjugation by x"). It is a $\mathbf{Q}$-linear map from $\mathrm{B}(\mathbf{Q})$ to itself, which is invertible (the inverse being $\gamma_{x^{-1}}$). Of course if $q \in \mathbf{Q}^\times$ and $x \in \mathrm{B}^\times$, we have $\gamma_{qx} = \gamma_x$ (because $\mathbf{Q}^\times = Z(\mathrm{B}^\times)$). Thus, the automorphism γ_x only depends on the class of x in the quotient $\mathrm{PB}^\times$. We denote the class of x by $[x]$. This just means

$$[x] = \left\{qx,\ q \in \mathbf{Q}^\times\right\}.$$

Then we have a group action of $\mathrm{PB}^\times$ on $\mathrm{B}(\mathbf{Q})$:

$$\begin{array}{ccc} \mathrm{PB}^\times \times \mathrm{B}(\mathbf{Q}) & \to & \mathrm{B}(\mathbf{Q}) \\ ([x], z) & \mapsto & \gamma_x(z) = xzx^{-1} \end{array}$$

Since trace-free quaternions are stable by conjugation by any element, this allows us to restric the action to $\mathrm{B}^{(0)}(\mathbf{Q})$:

$$\begin{array}{ccc} \mathrm{PB}^\times \times \mathrm{B}^{(0)}(\mathbf{Q}) & \to & \mathrm{B}^{(0)}(\mathbf{Q}) \\ ([x], z) & \mapsto & \gamma_x(z) = xzx^{-1} \end{array}$$

Now, $(\mathrm{B}^{(0)}(\mathbf{Q}), \mathrm{N})$ is a quadratic space which is isometric to $(\mathbf{Q}^3, \|\cdot\|_2^2)$ (where $\|\cdot\|_2$ denotes the restriction of the usual euclidean norm on $\mathbf{R}^3$, restricted to $\mathbf{Q}^3$). Indeed,

$$(a, b, c) \in \mathbf{Q}^3 \mapsto ai + bj + ck \in \mathrm{B}^{(0)}(\mathbf{Q})$$

defines an isometry between those quadratic spaces. Note that even if we sometimes say that there is a "natural" way to identify $\mathrm{B}^{(0)}(\mathbf{Q})$ and $\mathbf{Q}^3$, it is only natural once we have chosen the basis of $\mathrm{B}^{(0)}(\mathbf{Q})$ to be (i, j, k). Once we have made this identification, we may wonder what is the counterpart in $\mathbf{Q}^3$ of the action of $\mathrm{PB}^\times$ on $\mathrm{B}^{(0)}(\mathbf{Q})$?

Indeed, we can think of the automorphism γ_x as an invertible linear map on $\mathbf{Q}^3$ i.e. an element of $\mathrm{GL}(\mathbf{Q}^3)$. But is it any kind of linear map ?

Definition 4.1.1. *We denote by* $\mathrm{O}_3(\mathbf{Q})$ *the linear isometries of* $(\mathbf{Q}^3, \|\cdot\|_2^2)$*, that is : the subgroup of* $\mathrm{GL}(\mathbf{Q}^3)$ *made of the endomorphisms* $f\colon \mathbf{Q}^3 \to \mathbf{Q}^3$ *such that for all* $x \in \mathbf{Q}^3$, $\|f(x)\|_2^2 = \|x\|_2^2$.

We denote by $\mathrm{SO}_3(\mathbf{Q})$ *the subgroup of* $\mathrm{O}_3(\mathbf{Q})$ *made of the elements with determinant equal to 1.*

By multiplicativity of the norm, we have : for all $x \in \mathrm{B}^\times$, for all $z \in \mathrm{B}^{(0)}(\mathbf{Q})$, $\mathrm{N}(xzx^{-1}) = \mathrm{N}(z)$, so that γ_x acts on $\mathrm{B}^{(0)}(\mathbf{Q})$ by isometry. So if we transport this in $\mathbf{Q}^3$ via our natural identification, we see that γ_x (seen as a transformation of $\mathbf{Q}^3$) is an element of $\mathrm{O}_3(\mathbf{Q})$. In fact, it is even an element in $\mathrm{SO}_3(\mathbf{Q})$, but this is less immediate. We will need some extra work to understand this.

First, let us remark that the quadratic form N on $\mathrm{B}^{(0)}(\mathbf{Q})$ is an euclidean norm : it comes from an inner product on the $\mathbf{Q}$-vector space $\mathrm{B}^{(0)}(\mathbf{Q})$. Indeed, if $x = ai + bj + ck$ and $y = di + ej + fk$ are two elements of $\mathrm{B}^{(0)}(\mathbf{Q})$, define

$$\langle x, y\rangle := \frac{\mathrm{Tr}(x\overline{y})}{2}$$

Then a simple computation shows that $\langle x, y\rangle = ad + be + cf$, so that under the identification between $\mathrm{B}^{(0)}(\mathbf{Q})$ and $\mathbf{Q}^3$, this inner product is just the usual euclidean inner product on $\mathbf{Q}^3$.

Definition 4.1.2. *If* $(E, \langle\cdot,\cdot\rangle)$ *is an inner product space, a reflection of* E *is a linear isometry* $s\colon E \to E$ *with a hyperplane as a set of fixed points, and which acts as* $-\mathrm{id}$ *on the orthogonal complement.*

In this setting, if $x \in E \setminus \{0\}$, let us denote by τ_x the reflection with hyperplane $x^\perp$. Then it takes the following form : for all $y \in E$,

$$\tau_x(y) = y - 2\frac{\langle y, x\rangle}{\|x\|^2}x$$

where $\|\cdot\|$ denotes the norm associated with the inner product $\langle\cdot,\cdot\rangle$ i.e. $\|x\|^2 = \langle x, x\rangle$.

So if we go back to our space $(\mathrm{B}^{(0)}(\mathbf{Q}), \mathrm{N})$, reflections take the following form :
For all $x \in \mathrm{B}^{(0)}(\mathbf{Q})$, the reflection of $\mathrm{B}^{(0)}(\mathbf{Q})$ with hyperplan $x^\perp$ is the map τ_x given by the explicit expression : for all $h \in \mathrm{B}^{(0)}(\mathbf{Q})$,

$$\tau_x(h) = h - \frac{\mathrm{Tr}(h\overline{x})}{\mathrm{N}(x)}x$$

But if we come back to the definition of the trace and norm of a quaternion, we can simplify this expression as follows :

$$\begin{aligned}\tau_x(h) &= h - \left(h\overline{x} + \overline{h\overline{x}}\right)(x\overline{x})^{-1}x \\ &= h - h\overline{x}\ \overline{x}^{-1}x^{-1}x - \overline{\overline{x}}\,\overline{h}\overline{x}^{-1}x^{-1}x \\ &= -x\overline{h}\overline{x}^{-1}\end{aligned}$$

But as x and h are in $\mathrm{B}^{(0)}(\mathbf{Q})$, we have $\overline{x} = -x$ and $\overline{h} = -h$, hence $\tau_x(h) = -xhx^{-1} = -\gamma_x(h)$.

With this description of the reflections in $\mathrm{B}^{(0)}(\mathbf{Q})$, we are ready to prove that $\mathrm{B}^\times$ acts by *positive* isometries on $\mathbf{Q}^3$. We just need a last very famous result, that we will not prove here.

Theorem 4.1.3 (Cartan-Dieudonné)**.** *If* (E, q) *is a* n*-dimensional non degenerate quadratic space, then every linear isometry of* (E, q) *is a product of at most* n *reflections.*

Proof. see for instance [Per96], chapter VIII. We will not use the full result, in fact we just need to know that any isometry is a product of reflections, the fact that it is a product of "at most n" can be forgotten for our immediate purpose. □

Proposition 4.1.4. *For all* $x \in \mathrm{B}^\times$, γ_x *(seen as a transformation of* $\mathbf{Q}^3$*) belongs to* $\mathrm{SO}_3(\mathbf{Q})$.

Proof. Assume for a contradiction that there exists $x \in \mathrm{B}^\times$ such that $\gamma_x \in \mathrm{O}_3(\mathbf{Q}) \setminus \mathrm{SO}_3(\mathbf{Q})$. Then by Cartan-Dieudonné's theorem, we can write γ_x as a product of reflections : $\gamma_x = \tau_{x_1} \dots \tau_{x_r}$ where $x_1, \dots, x_r \in \mathrm{B}^{(0)}(\mathbf{Q}) \setminus \{0\}$. Now because reflections have determinant -1 and γ_x too, we must have r odd. Using the expression of reflections in $\mathrm{B}^{(0)}(\mathbf{Q})$ we just discussed above, and the fact that r is odd, we get that for all $h \in \mathrm{B}^{(0)}(\mathbf{Q})$, $\gamma_x(h) = -(x_1 \dots x_r)h(x_1 \dots x_r)^{-1}$. Let us put $y := x_1 \dots x_r$. As $\overline{h} = -h$, we have :

$$\text{for all } h \in \mathrm{B}^{(0)}(\mathbf{Q}),\ \gamma_x(h) = y\overline{h}y^{-1}$$

But this equality also holds when $h \in \mathbf{Q}$, since both sides equal h in this case (using the fact that the elements of $\mathbf{Q}$ commute with all the other quaternions). Since $\mathrm{B}(\mathbf{Q}) = \mathbf{Q}1 \oplus \mathrm{B}^{(0)}(\mathbf{Q})$, we deduce that for all $h \in \mathrm{B}(\mathbf{Q})$, $\gamma_x(h) = y\overline{h}y^{-1}$. This is impossible because on the left hand side we have γ_x, which is a surjective multiplicative function of h, whereas on the right hand side, we have an anti-multiplicative function of h (recall that for all $w, z \in \mathrm{B}(\mathbf{Q})$, $\overline{wz} = \overline{z}\ \overline{w}$), which is also surjective. To make the contradiction clearer maybe : Let us denote by f_y the map $h \mapsto y\overline{h}y^{-1}$. We just proved that $f_y = \gamma_x$. Now let us take $h, h' \in \mathrm{B}(\mathbf{Q})$ such that $\gamma_x(h) = i$ and $\gamma_x(h') = j$. Then $\gamma_x(hh') = \gamma_x(h)\gamma_x(h') = ij = k$. But on the other hand, we also have $\gamma_x(hh') = f_y(hh') = f_y(h')f_y(h) = \gamma_x(h')\gamma_x(h) = ji = -k$, hence a contradiction. □

Proposition 4.1.5. *The map*

$$\begin{array}{ccc} \mathrm{PB}^\times & \to & \mathrm{SO}_3(\mathbf{Q}) \\ [x] & \mapsto & \gamma_x \end{array}$$

is a group isomorphism.

Proof. It is easy to prove that it is a group homomorphism. To prove the injectivity, it suffices to remark that if γ_x is the identity on $\mathrm{B}^{(0)}(\mathbf{Q})$, then x commutes with all the elements in $\mathrm{B}(\mathbf{Q})$, so $x \in \mathcal{Z}(\mathrm{B}^\times)$, and this precisely tells us that $[x]$ is the unit element in $\mathrm{PB}^\times$. Finally, let us prove the surjectivity. Let $\sigma \in \mathrm{SO}_3(\mathbf{Q})$. Then by Cartan-Dieudonné's theorem, σ is a product of reflections. For determinant reasons, it is the product of an even number of reflections in $\mathrm{B}^{(0)}(\mathbf{Q})$. So there exists r even, and $x_1, \dots, x_r \in \mathrm{B}^{(0)}(\mathbf{Q}) \setminus \{0\}$ such that $\sigma = \tau_{x_1} \dots \tau_{x_r}$. By the description of reflections in $\mathrm{B}^{(0)}(\mathbf{Q})$, we know that for all $m \in \{1, \dots, r\}$, for all $h \in \mathrm{B}^{(0)}(\mathbf{Q})$, $\tau_{x_m}(h) = -\gamma_{x_m}(h)$. This implies (since r is even) that for all $h \in \mathrm{B}^{(0)}(\mathbf{Q})$, $\sigma(h) = \gamma_{x_1 \dots x_r}(h)$. Thus, the isometry $\sigma \in \mathrm{SO}_3(\mathbf{Q})$ indeed arises as the conjugation by some element in $\mathrm{B}^\times$. □

Corollary 4.1.6. *If $x, y \in \mathrm{B}^{(0)}(\mathbf{Q})$ have the same norm, then there exists $z \in \mathrm{B}^\times$ such that $y = zxz^{-1}$.*

Proof. With the isomorphism of proposition 4.1.5, we can see this question more geometrically. What we have to prove is that if $x, y \in \mathbf{Q}^3$ are such that $\|x\|_2^2 = \|y\|_2^2$, then there exists $\sigma \in \mathrm{SO}_3(\mathbf{Q})$ such that $y = \sigma(x)$. If $x = y$, then $\sigma = \mathrm{id}$ works. Now, when $x \neq y$, the reflection s of $\mathbf{Q}^3$ with hyperplane $(y - x)^\perp$ maps x to y. Indeed, since $\|x\|_2^2 = \|y\|_2^2$ we have

$$\langle y + x, y - x \rangle = \|y\|_2^2 - \langle y, x \rangle + \langle x, y \rangle - \|x\|_2^2 = 0$$

so $y + x \in (y - x)^\perp$. Therefore,

$$\begin{cases} s(y + x) = y + x \\ s(y - x) = x - y \end{cases}$$

hence $s(x) = y$. Now the problem is that s is a reflection, so it is not in $\mathrm{SO}_3(\mathbf{Q})$. Let t be any reflection with respect to an hyperplane containing x and y (it is the hyperplane spanned by x and y when they are not colinear, but in the case where $x = -y$, we just take an hyperplane containing the line generated by x and y). Then $t \circ s \in \mathrm{SO}_3(\mathbf{Q})$ since we compose two reflections, and $(t \circ s)(x) = t(y) = y$ since t is the identity on a plane containing x and y. So we can take $\sigma := t \circ s$ and it gives us a rotation of $\mathbf{Q}^3$ mapping x to y. □

Now, inside $\mathrm{B}^\times$ we have a particular subgroup : the group of invertible Hurwitz quaternions $\mathrm{B}(\mathbf{Z})^\times$. What is the geometrical effect (on $\mathbf{Q}^3$) of the conjugation by those particular elements ? This is what we will try to answer now.

Definition 4.1.7. *We denote by* $\mathrm{O}_3(\mathbf{Z})$ *the subgroup of* $\mathrm{O}_3(\mathbf{Q})$ *made of the isometries that preserve the lattice* $\mathbf{Z}^3$*. Similarly, we denote by* $\mathrm{SO}_3(\mathbf{Z})$ *the elements of* $\mathrm{O}_3(\mathbf{Z})$ *that have determinant* 1*.*

Let us make a few remarks on this definition. We denote by

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},\ e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

the canonical basis of $\mathbf{Q}^3$. By definition, an element of $\mathrm{O}_3(\mathbf{Q})$ is a linear map $u\colon \mathbf{Q}^3 \to \mathbf{Q}^3$ which preserves the standard inner product on $\mathbf{Q}^3$:

$$\forall x, y \in \mathbf{Q}^3,\ \langle u(x), u(y)\rangle = \langle x, y\rangle$$

From this, it is easy to see that the image of the canonical basis of $\mathbf{Q}^3$ by u is still an orthonormal basis. Thus, the matrix of u in the canonical basis of $\mathbf{Q}^3$ is a matrix whose three columns form an orthonormal basis of $(\mathbf{Q}^3, \langle\cdot,\cdot\rangle)$. Now, among those matrices, which ones are in $\mathrm{O}_3(\mathbf{Z})$? If $M \in \mathrm{O}_3(\mathbf{Q})$ has to preserve $\mathbf{Z}^3$, then the image of e_1, which is the first column of M, has to be in $\mathbf{Z}^3$, but also has to be of norm 1. Thus, it is of the form

$$\begin{pmatrix} \pm 1 \\ 0 \\ 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 \\ \pm 1 \\ 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 \\ 0 \\ \pm 1 \end{pmatrix}$$

If we apply the same argument to e_2 and e_3, we see that the columns of M are all of the form above, and since they have to be orthogonal, we get that M is a permutation matrix where we allow signs.

Proposition 4.1.8. $|\mathrm{O}_3(\mathbf{Z})| = 48$ *and* $|\mathrm{SO}_3(\mathbf{Z})| = 24$*.*

Proof. Choosing $M \in \mathrm{O}_3(\mathbf{Z})$, it is the choice of a (3×3) permutation matrix : there are $3! = 6$ such choices, and then we can choose to put either $+1$ or -1 for each non-zero entry of the permutation matrix, so we have $2^3 = 8$ possibilities. This gives $|\mathrm{O}_3(\mathbf{Z})| = 6 \times 8 = 48$. To show that $|\mathrm{SO}_3(\mathbf{Z})| = 24$, there are several ways to see it. For instance one can say that the determinant is a surjective group homomorphism $\mathrm{O}_3(\mathbf{Z}) \to \{\pm 1\}$, and the kernel is exactly $\mathrm{SO}_3(\mathbf{Z})$. Another way to get the result is to say that when we have to choose if we put a $+1$ or a -1 for the entry in the last column, we don't have the choice anymore since the value of the determinant is prescribed. □

Every element of $\mathrm{SO}_3(\mathbf{Z})$ permutes the three coordinate lines in $\mathbf{Q}^3$. Indeed, if $\sigma \in \mathrm{SO}_3(\mathbf{Z})$, each e_i is mapped to $\pm e_j$ for some j, and so if we forget about the signs, and just remember the axes, we see that σ induces a permutation of the axes. Let us detail an example to see what happens. Take $\sigma \in \mathrm{SO}_3(\mathbf{Z})$ the element with matrix in the canonical basis of $\mathbf{Q}^3$:

$$M := \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

It satisfies $\sigma(e_1) = -e_2$, $\sigma(e_2) = e_1$ and $\sigma(e_3) = e_3$. So σ exchanges the "x-axis" ($\mathbf{Q}e_1$) and the "y-axis" ($\mathbf{Q}e_2$), while the z-axis remains invariant. The induced permutation on the coordinate lines is the transposition $\begin{pmatrix} 1 & 2 \end{pmatrix}$.

Definition 4.1.9. *We denote by* $\mathrm{SO}_3(\mathbf{Z})^+$ *the subset of* $\mathrm{SO}_3(\mathbf{Z})$ *made of the rotations which induce an even permutation of the axes.*

As we said before, each matrix of $\mathrm{SO}_3(\mathbf{Z})$ can be constructed as follows : we start from a (3×3) permutation matrix, and then we allow some coefficients that are equal to 1 to take the value -1, with the restriction that the determinant should be equal to 1. Then the elements of $\mathrm{SO}_3(\mathbf{Z})^+$ are exactly those we construct in this way starting from the matrix of an even permutation. Since the elements of

$\mathfrak{S}_3$ with signature 1 are the identity, and the two 3-cycles $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ and $\begin{pmatrix}1 & 3 & 2\end{pmatrix}$, it is easy to deduce the list of the elements in $\mathrm{SO}_3(\mathbf{Z})^+$. Indeed, the matrices attached to our three even permutations are

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix} \text{ and } \begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}$$

and by 3-linearity of the determinant, only the changes of an even number of signs will preserve the determinant. From the first one we deduce the following elements of $\mathrm{SO}_3(\mathbf{Z})^+$:

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix} \text{ and } \begin{pmatrix}-1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

From the second one we deduce :

$$\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0 & -1\\ 1 & 0 & 0\\ 0 & -1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0 & -1\\ -1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix} \text{ and } \begin{pmatrix}0 & 0 & 1\\ -1 & 0 & 0\\ 0 & -1 & 0\end{pmatrix}$$

while the last one gives us :

$$\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}, \begin{pmatrix}0 & -1 & 0\\ 0 & 0 & -1\\ 1 & 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1 & 0\\ 0 & 0 & -1\\ -1 & 0 & 0\end{pmatrix} \text{ and } \begin{pmatrix}0 & -1 & 0\\ 0 & 0 & 1\\ -1 & 0 & 0\end{pmatrix}$$

The twelve matrices we just enumerated form the set $\mathrm{SO}_3(\mathbf{Z})^+$.

The reason why we introduce this subset of $\mathrm{SO}_3(\mathbf{Z})$ is because it is exactly how the elements of $\mathrm{B}(\mathbf{Z})^\times$ act on $\mathbf{Q}^3$. Let us give a more precise statement.

Proposition 4.1.10. *The group homomorphism*

$$\begin{array}{ccc}\mathrm{B}(\mathbf{Z})^\times & \to & \mathrm{SO}_3(\mathbf{Q})\\ x & \mapsto & \gamma_x\end{array}$$

induces an isomorphism $\mathrm{B}(\mathbf{Z})^\times/\{\pm 1\} \xrightarrow{\sim} \mathrm{SO}_3(\mathbf{Z})^+$.

Proof. I did not find a more elegant proof than just doing the (quite tedious) computations, I am open to any suggestion. Recall that

$$\mathrm{B}(\mathbf{Z})^\times = \left\{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\right\},$$

and that we have the following rules for the multiplication in $\mathrm{B}(\mathbf{Q})$:

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i \text{ and } ki = -ik = j.$$

Let $z := u + ai + bj + ck$ be an element of $\mathrm{B}(\mathbf{Q})$.

- First, let us see how the conjugation by i acts on the z. We have :

$$\begin{aligned} izi^{-1} &= iz(-i) = i(u + ai + bj + ck)(-i) = (ui + ai^2 + bij + cik)(-i)\\ &= -(ui - a + bk - cj)i = u + ai - bj - ck \end{aligned}$$

  Similar computations can be done to deduce jzj^{-1} and kzk^{-1}.

- Now, for the other "type" of units in $\mathrm{B}(\mathbf{Z})$, let us explain with $\varepsilon := \frac{1+i+j+k}{2}$ (because the other units look the same, up to some signs changes). Since $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$, it has norm 1 and we have $\varepsilon^{-1} = \bar{\varepsilon}$ (this is a first important thing to notice, computing ε^{-1} is not difficult). Thus,

$$\varepsilon z \varepsilon^{-1} = \frac{1}{4}(1+i+j+k)(u+ai+bj+ck)(1-i-j-k)$$

  Then the computation is a bit tedious, but in the end a lot of terms simplify and we obtain $\varepsilon z \varepsilon^{-1} = u + ci + aj + bk$.

I checked the two examples above, and for the other units I chose to trust the following table, given in [Han81]. Note that for all $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$, $\gamma_\varepsilon = \gamma_{-\varepsilon}$, so we just need to do do the computations for half of the units.

ε	$\varepsilon(u+ai+bj+ck)\varepsilon^{-1}$
1	$u+ai+bj+ck$
i	$u+ai-bj-ck$
j	$u-ai+bj-ck$
k	$u-ai-bj+ck$
$\frac{1+i+j+k}{2}$	$u+ci+aj+bk$
$\frac{-1+i-j+k}{2}$	$u+ci-aj-bk$
$\frac{-1+i+j-k}{2}$	$u-ci+aj-bk$
$\frac{-1-i+j+k}{2}$	$u-ci-aj+bk$
$\frac{1-i-j-k}{2}$	$u+bi+cj+ak$
$\frac{1+i+j-k}{2}$	$u+bi-cj-ak$
$\frac{1-i+j+k}{2}$	$u-bi+cj-ak$
$\frac{1+i-j+k}{2}$	$u-bi-cj+ak$

From this table we easily deduce the result stated in the proposition. Indeed, let us consider (for instance) $\varepsilon := \frac{1+i+j-k}{2}$. Since $\gamma_\varepsilon(u+ai+bj+ck) = u+bi-cj-ak$, we deduce that the isometry of $\mathbf{Q}^3$ corresponding to γ_ε is :

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} b \\ -c \\ -a \end{pmatrix}$$

whose matrix in the canonical basis of $\mathbf{Q}^3$ is

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix} \in \mathrm{SO}_3(\mathbf{Z})^+$$

We do the same for each $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$, and we see that the γ_ε's always induce a transformation of $\mathbf{Q}^3$ which is in $\mathrm{SO}_3(\mathbf{Z})^+$, and that, in fact, they reach all the elements in $\mathrm{SO}_3(\mathbf{Z})^+$. This shows that the group homomorphism

$$\begin{array}{ccc} \mathrm{B}(\mathbf{Z})^\times & \to & \mathrm{SO}_3(\mathbf{Z})^+ \\ \varepsilon & \mapsto & \gamma_\varepsilon \end{array}$$

is well defined and surjective. Now γ_ε is the identity of $\mathbf{Q}^3$ if and only if $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times \cap \mathcal{Z}(\mathrm{B}^\times) = \mathrm{B}(\mathbf{Z})^\times \cap \mathbf{Q}^\times = \{\pm 1\}$, hence the isomorphism claimed in the proposition.

□

Corollary 4.1.11. *We have* $\mathrm{SO}_3(\mathbf{Z}) = \mathrm{SO}_3(\mathbf{Z})^+ \sqcup \gamma_{1+i}\mathrm{SO}_3(\mathbf{Z})^+$. *In other words, a matrix* $M \in \mathrm{SO}_3(\mathbf{Z})$ *can be realized as the conjugation by a quaternion* $v \in \mathrm{B}(\mathbf{Z})^\times \sqcup (1+i)\mathrm{B}(\mathbf{Z})^\times$.

Proof. It suffices to check that the conjugation by $1+i$ gives a rotation γ_{1+i} which is in $\mathrm{SO}_3(\mathbf{Z})$ but not in $\mathrm{SO}_3(\mathbf{Z})^+$. A similar computation as the ones above shows that γ_{1+i} is the rotation of $\mathbf{Q}^3$ with matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

in the canonical basis of $\mathbf{Q}^3$. This is an element of $\mathrm{SO}_3(\mathbf{Z})$, and it is not in $\mathrm{SO}_3(\mathbf{Z})^+$ since in terms of permutation of the axes, it just permutes the y-axis and the z-axis, and the transposition $\begin{pmatrix} 2 & 3 \end{pmatrix}$, as any transposition, has signature -1. □

4.2 Definition of an action of an ideal class group on the representations

Let $d \geqslant 2$ be a square-free admissible integer. We denote by K the imaginary quadratic field $\mathbf{Q}(\sqrt{-d})$. We recall that $\mathscr{R}_3(d)$ denotes the set

$$\{(a,b,c) \in \mathbf{Z}^3 \mid a^2+b^2+c^2 = d\}$$

and that it can be seen as a subset of $\mathrm{B}^{(0)}(\mathbf{Q})$: the set of all the pure quaternions $z := ai+bj+ck$, where $(a,b,c) \in \mathbf{Z}^3$, such that $\mathrm{N}(z) = d$. It will be convenient to introduce a notation for the pure quaternions with coefficients in $\mathbf{Z}$:

$$\mathrm{B}^{(0)}(\mathbf{Z}) := \mathrm{B}^{(0)}(\mathbf{Q}) \cap \mathrm{B}(\mathbf{Z}) = \{ai+bj+ck,\ (a,b,c) \in \mathbf{Z}^3\}$$

With this notation, we can see $\mathscr{R}_3(d)$ as the following subset of $\mathrm{B}^{(0)}(\mathbf{Q})$:

$$\mathscr{R}_3(d) = \{x \in \mathrm{B}^{(0)}(\mathbf{Z}) \mid \mathrm{N}(x) = d\} = \{x \in \mathrm{B}^{(0)}(\mathbf{Z}) \mid x^2 = -d\}$$

where the second equality comes from the fact that for pure quaternions, $\overline{x} = -x$, so $\mathrm{N}(x) = x\overline{x} = -x^2$. Thus, any representation of d as a sum of three squares gives us a square root of $-d$ in $\mathrm{B}^{(0)}(\mathbf{Z}) \subseteq \mathrm{B}(\mathbf{Q})$, hence another "copy" of the field $K = \mathbf{Q}(\sqrt{-d})$.

Let us take some time to ensure that the fact that $\mathrm{B}(\mathbf{Q})$ is not commutative does not lead to any issue. Let $x \in \mathscr{R}_3(d)$, that we see as an element in $\mathrm{B}^{(0)}(\mathbf{Z})$. We consider the map

$$\begin{array}{rccc} \mathrm{ev}_x & : & \mathbf{Q}[X] & \to & \mathbf{Q}[x] \\ & & P & \mapsto & P(x) \end{array}$$

This map makes sense because x is an element of the $\mathbf{Q}$-algebra $\mathrm{B}(\mathbf{Q})$, so we can evaluate polynomials at x. Moreover, it is a morphism of $\mathbf{Q}$-algebras, and what is important to notice is that we only use the fact that the mutiplication in $\mathrm{B}(\mathbf{Q})$ is $\mathbf{Q}$-bilinear, and we don't need commutativity. It follows that the kernel of ev_x is an ideal of $\mathbf{Q}[X]$. Since $\mathbf{Q}[X]$ is a PID, there exists a unique monic polynomial $\pi_x \in \mathbf{Q}[X]$ such that $\ker(\mathrm{ev}_x) = (\pi_x)$. Now since $x \in \mathscr{R}_3(d)$, we have $x^2+d = 0$ so that π_x divides X^2+d. But the latter is irreducible in $\mathbf{Q}[X]$, so we have $\pi_x = X^2+d$. Therefore, ev_x induces an isomorphism of $\mathbf{Q}$-algebras between $\mathbf{Q}[X]/(X^2+d)$ and $\mathbf{Q}[x]$. In particular, $\mathbf{Q}[x]$ is a field so we have $\mathbf{Q}[x] = \mathbf{Q}(x)$. Thus, we really get a field extension of $\mathbf{Q}$, obtained by adjoining a square root of $-d$, so this gives a natural identification with $\mathbf{Q}(\sqrt{-d})$.

More precisely, for all $x \in \mathscr{R}_3(d)$ (seen as a subset of $\mathrm{B}^{(0)}(\mathbf{Z})$), we denote by ι_x the $\mathbf{Q}$-linear map

$$\begin{array}{ccc} K & \to & \mathbf{Q}(x) \\ \sqrt{-d} & \mapsto & x \end{array}$$

Then this map is an isomorphism of $\mathbf{Q}$-algebras. This will allow us to transport ideals of $\mathcal{O}_K$ inside the quaternions, and it is the key idea to define an action of $\mathrm{Cl}(\mathcal{O}_K)$ on the representations of d as a sum of three squares. The isomorphism ι_x is integral in the sense that the rings of integers on both sides correspond via ι_x.

Lemma 4.2.1. *Assume that $x \in \mathscr{R}_3(d)$ for some admissible, square-free $d \equiv 1, 2 \bmod 4$. Let us denote by $\mathcal{O}_x$ the ring of integers of $\mathbf{Q}(x)$ (i.e. the set of elements in $\mathbf{Q}(x)$ that are integral over $\mathbf{Z}$). Then we have $\mathcal{O}_x = \mathbf{Z}[x] = \mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x)$. In particular $\iota_x(\mathcal{O}_K) = \mathcal{O}_x$.*

Proof. We prove that $\mathcal{O}_x \subseteq \mathbf{Z}[x] \subseteq \mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x) \subseteq \mathcal{O}_x$.

- If $y \in \mathcal{O}_x$ then $y \in \mathbf{Q}(x)$: we write it as $a + bx$ where $(a, b) \in \mathbf{Q}^2$. If $b = 0$, then y is in $\mathbf{Q}$, and is integral over $\mathbf{Z}$. This implies that $y \in \mathbf{Z}$ since $\mathbf{Z}$ is integrally closed. In particular, $y \in \mathbf{Z}[x]$. Otherwise, $b \neq 0$ and the minimal polynomial of y over $\mathbf{Q}$ is of degree at least 2. But by proposition 3.1.2, we know that the polynomial $X^2 - \mathrm{Tr}(y)X + \mathrm{N}(y)$ vanishes at y. Thus, this must be the minimal polynomial of y over $\mathbf{Q}$. Since $y \in \mathcal{O}_x$ it has coefficients in $\mathbf{Z}$ (see proposition 1.2.6). We deduce that :

$$\begin{cases} \mathrm{Tr}(y) = 2a \in \mathbf{Z} \\ \mathrm{N}(y) = a^2 + b^2 d \in \mathbf{Z} \end{cases} \tag{12}$$

  Here we used the fact that $x \in \mathscr{R}_3(d)$ to compute the trace and norm of $a + bx$. Multiplying the second line by 4 leads to $(2a)^2 + (2b)^2 d \in \mathbf{Z}$, hence $(2b)^2 d \in \mathbf{Z}$ since $2a \in \mathbf{Z}$. But this implies that $2b \in \mathbf{Z}$ because d is square-free, so it cannot balance eventual denominators of $2b$. Therefore, we can take $u, v \in \mathbf{Z}$ such that $a = \frac{u}{2}$ and $b = \frac{v}{2}$. Then the fact that $a^2 + b^2 d \in \mathbf{Z}$ implies that $u^2 + v^2 d \equiv 0 \bmod 4$.

  - If v is even, then $v^2 \equiv 0 \bmod 4$, hence $u^2 \equiv 0 \bmod 4$, so u is even too. In this case $a, b \in \mathbf{Z}$, so $y \in \mathbf{Z}[x]$.
  - If v is odd, then $v^2 \equiv 1 \bmod 4$, hence $u^2 + d \equiv 0 \bmod 4$. As 0 and 1 are the only squares modulo 4, and d is square-free, we must have $u^2 \equiv 1 \bmod 4$. But then $d \equiv -1 \bmod 4$, which is not the case by assumption. So this case cannot happen.

  So we proved the inclusion $\mathcal{O}_x \subseteq \mathbf{Z}[x]$.

- Now, if $y \in \mathbf{Z}[x]$, then we write $y = a + bx$ for some $a, b \in \mathbf{Z}$. Since $x \in \mathscr{R}_3(d)$, there are integers c, d, e such that $x = ci + dj + ek$. Thus, $y = a + bx = a1 + (bc)i + (bd)j + (be)k$ is a quaternion with all its coefficients in $\mathbf{Z}$, so it is in $\mathrm{B}(\mathbf{Z})$. This proves the inclusion $\mathbf{Z}[x] \subseteq \mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x)$.

- Finally, if $y \in \mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x)$, then since $y \in \mathrm{B}(\mathbf{Z})$, we have $\mathrm{N}(y), \mathrm{Tr}(y) \in \mathbf{Z}$. Thus, the polynomial $X^2 - \mathrm{Tr}(y)X + \mathrm{N}(y)$ is a polynomial with coefficients in $\mathbf{Z}$, that vanishes at y, showing that y is integral over $\mathbf{Z}$. This gives us the inclusion $\mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x) \subseteq \mathcal{O}_x$.

To get the "in particular" part of the statement : proposition 2.1.2 tells us that for our condition on d, we have $\mathcal{O}_K = \mathbf{Z}\left[\sqrt{-d}\right]$, hence $\iota_x(\mathcal{O}_K) = \mathbf{Z}[x] = \mathcal{O}_x$. We did not give the proof of proposition 2.1.2, but in fact it is exactly the same as what we have just done to show that $\mathcal{O}_x = \mathbf{Z}[x]$. □

Remark. *In the case $d \equiv 3 \bmod 8$, the statement is almost the same, we still have*

$$\mathcal{O}_x = \mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x) = \iota_x(\mathcal{O}_K),$$

and the only difference is that it is not equal to $\mathbf{Z}[x]$ (but this dichotomy is not so surprising given proposition 2.1.2).

Now, we define the action of $\mathrm{Cl}(\mathcal{O}_K)$ on the representations step by step. Let $x \in \mathscr{R}_3(d)$ and let I be a (possibly fractional) ideal of $\mathcal{O}_K$. It is finitely generated as a $\mathbf{Z}$-module, so $\iota_x(I)$ is also finitely generated as a $\mathbf{Z}$-module. Therefore, $\mathrm{B}(\mathbf{Z})\iota_x(I)$ is a finitely generated left $\mathrm{B}(\mathbf{Z})$-submodule of $\mathrm{B}(\mathbf{Q})$. By corollary 3.1.6, there exists $q \in \mathrm{B}^\times$ such that $\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})q^{-1}$. This way, we can think of our ideal I of $\mathcal{O}_K$ as an element $q \in \mathrm{B}^\times$. Of course, q is not uniquely determined, and we will explain how this issue is handled. Now, define $y := q^{-1}xq$. Let us prove that y is also an element in $\mathscr{R}_3(d)$.

- $y \in \mathrm{B}^{(0)}(\mathbf{Q})$ since $x \in \mathrm{B}^{(0)}(\mathbf{Q})$ and being trace-free is preserved under conjugation.

- $\mathrm{N}(y) = \mathrm{N}(x) = d$ by multiplicativity of the norm.
- To get the conclusion, it remains to show that $y \in \mathrm{B}^{(0)}(\mathbf{Z})$. As $y \in \mathrm{B}^{(0)}(\mathbf{Q})$, it just remains to show that $y \in \mathrm{B}(\mathbf{Z})$. But we have :

$$\begin{aligned} y = q^{-1}xq \in \mathrm{B}(\mathbf{Z})q^{-1}xq = \mathrm{B}(\mathbf{Z})\iota_x(I)xq = \mathrm{B}(\mathbf{Z})\iota_x(I)\iota_x(\sqrt{-d})q = \mathrm{B}(\mathbf{Z})\iota_x(I\sqrt{-d})q \\ \subseteq \mathrm{B}(\mathbf{Z})\iota_x(I)q \end{aligned} \tag{13}$$

  because $I\sqrt{-d} \subseteq I$ since I is an $\mathcal{O}_K$-submodule of K and $\sqrt{-d} \in \mathcal{O}_K$. As $\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})q^{-1}$, we obtain that $y \in \mathrm{B}(\mathbf{Z})$.

This seems to give us a way to associate to each pair (I, x) an element y which is a possibly new representation of x as a sum of three squares. The problem is that the element q is not uniquely determined, so the new element $y \in \mathscr{R}_3(d)$ that we define depends on some choices. Let us explain how to overcome this difficulty.

The element q is defined as a non-zero quaternion such that $\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})q^{-1}$. The other $r \in \mathrm{B}^\times$ such that $\mathrm{B}(\mathbf{Z})q^{-1} = \mathrm{B}(\mathbf{Z})r^{-1}$ are exactly the elements of the form $r = q\varepsilon$, where $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$. Now, if we take $r = q\varepsilon$ instead of q to define our new element in $\mathscr{R}_3(d)$, we obtain $y' = (q\varepsilon)^{-1}x(q\varepsilon) = \varepsilon^{-1}y\varepsilon$. In other words, different choices of the element q (which "represents" the ideal I inside $\mathrm{B}(\mathbf{Q})$) lead to elements of $\mathscr{R}_3(d)$ that only differ by conjugation by an element of $\mathrm{B}(\mathbf{Z})^\times$.

This is why the space on which $\mathrm{Cl}(\mathcal{O}_K)$ will act is not $\mathscr{R}_3(d)$, but the quotient space

$$\widetilde{\mathscr{R}_3}(d)^+ := \mathrm{B}(\mathbf{Z})^\times \backslash \mathscr{R}_3(d)$$

that is : the set of orbits of $\mathscr{R}_3(d)$ under the action of $\mathrm{B}(\mathbf{Z})^\times$ by conjugation. The orbit of an element $x \in \mathscr{R}_3(d)$ will be denoted by $[x]$. By definition, we have

$$[x] = \{\varepsilon x \varepsilon^{-1},\ \varepsilon \in \mathrm{B}(\mathbf{Z})^\times\}$$

and $\widetilde{\mathscr{R}_3}(d)^+ = \{[x],\ x \in \mathscr{R}_3(d)\}$. This is the "algebraic" point of view on $\widetilde{\mathscr{R}_3}(d)^+$, because we define it via conjugation in $\mathrm{B}^\times$. However, the previous section on the geometry behind these algebraic operations provides another interpretation of this quotient. Indeed, in view of proposition 4.1.10, if we see the elements of $\mathscr{R}_3(d)$ as points on the sphere of radius $\sqrt{d}$ in $\mathbf{Q}^3$, the set $\widetilde{\mathscr{R}_3}(d)^+$ is also the quotient $\mathrm{SO}_3(\mathbf{Z})^+ \backslash \mathscr{R}_3(d)$ (where the action of $\mathrm{SO}_3(\mathbf{Z})^+$ on $\mathscr{R}_3(d)$ is just the multiplication on the left)

We use the notations introduced in section 1.5 : $\mathrm{Fr}(\mathcal{O}_K)$ denotes the group of non-zero fractional ideals of $\mathcal{O}_K$. What we have done so far allows us to define a map

$$\begin{array}{ccc} \mathrm{Fr}(\mathcal{O}_K) \times \mathscr{R}_3(d) & \to & \widetilde{\mathscr{R}_3}(d)^+ \\ (I, x) & \mapsto & [y] \end{array} \tag{14}$$

where $y = q^{-1}xq$ for any $q \in \mathrm{B}^\times$ such that $\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})q^{-1}$. Now, let us prove that the image of (I, x) only depends on $[x]$. If $x' \in [x]$, let us write $x' = \varepsilon x \varepsilon^{-1}$ for some $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$. Our aim is to prove that the image of (I, x') by the map in (14) is the same as the image of (I, x).
We have $\iota_{x'}(I) = \varepsilon\iota_x(I)\varepsilon^{-1}$, hence

$$\mathrm{B}(\mathbf{Z})\iota_{x'}(I) = \mathrm{B}(\mathbf{Z})\varepsilon\iota_x(I)\varepsilon^{-1} = \mathrm{B}(\mathbf{Z})\iota_x(I)\varepsilon^{-1}$$

(using the fact that $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$, so that $\mathrm{B}(\mathbf{Z})\varepsilon = \mathrm{B}(\mathbf{Z})$). Thus, if $q \in \mathrm{B}^\times$ is such that $\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})q^{-1}$, then $r := \varepsilon q$ is such that $\mathrm{B}(\mathbf{Z})\iota_{x'}(I) = \mathrm{B}(\mathbf{Z})r^{-1}$.
Therefore, the image of (I, x) is $\left[q^{-1}xq\right]$ while the image of (I, x') is $\left[r^{-1}x'r\right]$. But

$$r^{-1}x'r = (\varepsilon q)^{-1}\varepsilon x \varepsilon^{-1}(\varepsilon q) = q^{-1}xq$$

hence the conclusion. So we have a well defined map

$$\begin{array}{ccc} \mathrm{Fr}(\mathcal{O}_K) \times \widetilde{\mathscr{R}_3}(d)^+ & \to & \widetilde{\mathscr{R}_3}(d)^+ \\ (I, [x]) & \mapsto & [y] =: I.[x] \end{array}$$

Proposition 4.2.2. *The map above is an action of the group* $\mathrm{Fr}(\mathcal{O}_K)$ *on* $\widetilde{\mathscr{R}_3}(d)^+$. *In other words,*

- *for all* $[x] \in \widetilde{\mathscr{R}_3}(d)^+$, $\mathcal{O}_K.[x] = [x]$
- *for all* $I, J \in \mathrm{Fr}(\mathcal{O}_K)$ *and for all* $[x] \in \widetilde{\mathscr{R}_3}(d)^+$, $I.(J.[x]) = (IJ).[x]$

Proof. For the first point : we have $\iota_x(\mathcal{O}_K) = \mathcal{O}_x$ by lemma 4.2.1, hence $\mathrm{B}(\mathbf{Z})\iota_x(\mathcal{O}_K) = \mathrm{B}(\mathbf{Z})\mathcal{O}_x = \mathrm{B}(\mathbf{Z})(\mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x))$. But since $1 \in \mathcal{O}_x$, we have $\mathrm{B}(\mathbf{Z}) \subseteq \mathrm{B}(\mathbf{Z})\mathcal{O}_x$, and conversely, we have

$$\mathrm{B}(\mathbf{Z})(\mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x)) \subseteq \mathrm{B}(\mathbf{Z})$$

because $\mathrm{B}(\mathbf{Z})$ is a subring of $\mathrm{B}(\mathbf{Q})$. Thus, we have $\mathrm{B}(\mathbf{Z})\iota_x(\mathcal{O}_K) = \mathrm{B}(\mathbf{Z})1$, so $\mathcal{O}_K.[x]$ is defined as $\left[1^{-1}x1\right] = [x]$.

Now let us prove the second point. Let $I, J \in \mathrm{Fr}(\mathcal{O}_K)$, and let $q, s \in \mathrm{B}^\times$ be such that

$$\begin{cases} \mathrm{B}(\mathbf{Z})\iota_x(J) = \mathrm{B}(\mathbf{Z})q^{-1} \\ \mathrm{B}(\mathbf{Z})\iota_x(IJ) = \mathrm{B}(\mathbf{Z})s^{-1} \end{cases}$$

Then $(IJ).[x] = \left[s^{-1}xs\right]$ and $J.[x] = \left[q^{-1}xq\right]$. Let us set $y := q^{-1}xq$. We want to compute $I.[y]$. For this we need to find a generator of the left $\mathrm{B}(\mathbf{Z})$-module $\mathrm{B}(\mathbf{Z})\iota_y(I)$. Since $y = q^{-1}xq$, we have $\iota_y(I) = q^{-1}\iota_x(I)q$, hence

$$\begin{aligned} \mathrm{B}(\mathbf{Z})\iota_y(I) &= \mathrm{B}(\mathbf{Z})q^{-1}\iota_x(I)q = \mathrm{B}(\mathbf{Z})\iota_x(J)\iota_x(I)q \\ &= \mathrm{B}(\mathbf{Z})\iota_x(IJ)q = \mathrm{B}(\mathbf{Z})s^{-1}q \end{aligned}$$

Thus, in order to define $I.[y]$, we can take $r := q^{-1}s \in \mathrm{B}^\times$ as an element such that

$$\mathrm{B}(\mathbf{Z})\iota_y(I) = \mathrm{B}(\mathbf{Z})r^{-1}$$

Then $I.[y] = \left[r^{-1}yr\right] = \left[\left(q^{-1}s\right)^{-1} q^{-1}xq \left(q^{-1}s\right)\right] = \left[s^{-1}xs\right] = (IJ).[x]$. This gives the conclusion : $I.(J.[x]) = (IJ).[x]$. □

Finally, what we want to show now is that this action induces an action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\widetilde{\mathscr{R}_3}(d)^+$. In order to do this, we prove that for any I in $\mathrm{Fr}(\mathcal{O}_K)$, for any $\lambda \in K^\times$, the "action" of λI on $\widetilde{\mathscr{R}_3}(d)^+$ is the same as the action of I.

Let $I \in \mathrm{Fr}(\mathcal{O}_K)$, $\lambda \in K^\times$, and $x \in \mathscr{R}_3(d)$. We have

$$\mathrm{B}(\mathbf{Z})\iota_x(\lambda I) = \mathrm{B}(\mathbf{Z})\iota_x(I)\iota_x(\lambda)$$

because $I\lambda = \lambda I$ (in K everything commutes). So if $q \in \mathrm{B}^\times$ is such that $\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})q^{-1}$, then it suffices to take $r := \iota_x\left(\lambda^{-1}\right) q$ to have

$$\mathrm{B}(\mathbf{Z})\iota_x(\lambda I) = \mathrm{B}(\mathbf{Z})r^{-1}$$

Then $(\lambda I).[x] = \left[r^{-1}xr\right] = \left[q^{-1}\iota_x(\lambda)x\iota_x\left(\lambda^{-1}\right) q\right] = \left[q^{-1}\iota_x\left(\lambda\sqrt{-d}\lambda^{-1}\right) q\right]$. As K is commutative, $\lambda\sqrt{-d}\lambda^{-1} = \sqrt{-d}$, hence

$$(\lambda I).[x] = \left[q^{-1}\iota_x\left(\sqrt{-d}\right) q\right] = \left[q^{-1}xq\right] = I.[x]$$

Summary : All these verifications can be a bit long to read, and there is a risk of forgetting what we are doing, so let us summarize here.

We have an action of $\mathrm{Fr}(\mathcal{O}_K)$ on $\widetilde{\mathscr{R}_3}(d)^+$ working as follows : given a (possibly fractional) ideal I of $\mathcal{O}_K$ and $x \in \mathscr{R}_3(d)$ (that we think as a pure quaternion of norm d with coefficients in $\mathbf{Z}$), we consider

the left $\mathrm{B}(\mathbf{Z})$-module $\mathrm{B}(\mathbf{Z})\iota_x(I)$. By previous results on quaternions, we can find $q \in \mathrm{B}^\times$ such that $\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})q^{-1}$. This way, we can think of our ideal I as an element q in $\mathrm{B}^\times$. Then the action of I on x is just the conjugation by q. So we define $I.x$ as $y := q^{-1}xq$. The only issue is that q is not uniquely determined, it is determined up to multiplication by an element in $\mathrm{B}(\mathbf{Z})^\times$. Thus, y is only determined up to conjugation by an element of $\mathrm{B}(\mathbf{Z})^\times$. This is the reason why we cannot really define directly an action of $\mathrm{Fr}(\mathcal{O}_K)$ on $\mathscr{R}_3(d)$, but only on a quotient of $\mathscr{R}_3(d)$:

$$\widetilde{\mathscr{R}_3}(d)^+ := \mathrm{B}(\mathbf{Z})^\times \backslash \mathscr{R}_3(d)$$

Finally, we checked that for all $I \in \mathrm{Fr}(\mathcal{O}_K)$, and for all $\lambda \in K^\times$, the ideals I and λI have exactly the same action on $\widetilde{\mathscr{R}_3}(d)^+$. Therefore, we have in fact a group action of $\mathrm{Cl}(\mathcal{O}_K)$:

$$\begin{array}{ccc} \mathrm{Cl}(\mathcal{O}_K) \times \widetilde{\mathscr{R}_3}(d)^+ & \to & \widetilde{\mathscr{R}_3}(d)^+ \\ [I]\,, [x] & \mapsto & I.[x] \end{array}$$

where we denoted between brackets the class of I in the class group of K. The aim of the next section is to prove that this action is in fact free and transitive.

4.3 Conclusion on the number of representations

In this section we prove that when $d \equiv 1, 2 \bmod 4$, the action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\widetilde{\mathscr{R}_3}(d)^+$ is free and transitive. We say that $\widetilde{\mathscr{R}_3}(d)^+$ is a $\mathrm{Cl}(\mathcal{O}_K)$-torsor. This fact will give us almost immediately the size of $\mathscr{R}_3(d)$ in terms of the class number of $\mathbf{Q}(\sqrt{-d})$. The proofs presented here follow the article [Reh82], which gives a modernized version of some of the results in Venkov's original papers [Ven22] and [Ven29]. We start by three technical lemmas.

Recall that if $x \in \mathscr{R}_3(d)$, we can see it as an element in $\mathrm{B}^{(0)}(\mathbf{Z})$ such that $\mathrm{N}(x) = d$, or equivalently $x^2 = -d$. We proved that there is an isomorphism of $\mathbf{Q}$-algebras between $\mathbf{Q}(\sqrt{-d})$ and $\mathbf{Q}(x)$ (just given by $\sqrt{-d} \mapsto x$). So $\mathbf{Q}(x)$ is in fact an imaginary quadratic field, it's just that we did not embed it inside $\mathbf{C}$ by choosing a square root of $-d$ in $\mathbf{C}$. Instead, we took a square root x in $\mathrm{B}^{(0)}(\mathbf{Z})$. But as it is a number field, all the facts we recalled in section 1.6 apply to $\mathbf{Q}(x)$. In particular, its ring of integers $\mathcal{O}_x$ is a Dedekind ring, so it makes sense to talk about fractional ideals of $\mathcal{O}_x$ and their inverse.

Lemma 4.3.1. *If $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_x$ then $\mathrm{B}(\mathbf{Z})\mathfrak{a} \cap \mathbf{Q}(x) = \mathfrak{a}$.*

Proof. First, since $1 \in \mathrm{B}(\mathbf{Z})$, we have $\mathfrak{a} \subseteq \mathrm{B}(\mathbf{Z})\mathfrak{a}$, so

$$\mathfrak{a} \subseteq \mathrm{B}(\mathbf{Z})\mathfrak{a} \cap \mathbf{Q}(x).$$

Now, to prove the other inclusion we first remark that $(\mathrm{B}(\mathbf{Z})\mathfrak{a} \cap \mathbf{Q}(x))\mathcal{O}_x = \mathrm{B}(\mathbf{Z})\mathfrak{a} \cap \mathbf{Q}(x)$. Indeed, the inclusion "$\supseteq$" is clear because $1 \in \mathcal{O}_x$, and the inclusion "$\subseteq$" just follows from the fact that $\mathfrak{a}\mathcal{O}_x \subseteq \mathfrak{a}$ (because $\mathfrak{a}$ is a sub-$\mathcal{O}_x$-module of $\mathbf{Q}(x)$). Now since $\mathcal{O}_x$ is a Dedekind ring, every non-zero fractional ideal is invertible : so we can consider $\mathfrak{a}^{-1}$ (i.e. the fractional ideal of $\mathcal{O}_x$ such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}_x$). Then we have :

$$\begin{aligned} \mathrm{B}(\mathbf{Z})\mathfrak{a} \cap \mathbf{Q}(x) &= (\mathrm{B}(\mathbf{Z})\mathfrak{a} \cap \mathbf{Q}(x))\mathcal{O}_x \\ &= (\mathrm{B}(\mathbf{Z})\mathfrak{a} \cap \mathbf{Q}(x))\mathfrak{a}^{-1}\mathfrak{a} \\ &\subseteq (\mathrm{B}(\mathbf{Z})\mathfrak{a}\mathfrak{a}^{-1} \cap \mathbf{Q}(x)\mathfrak{a}^{-1})\mathfrak{a} \\ &= (\underbrace{\mathrm{B}(\mathbf{Z})\mathcal{O}_x}_{=\mathrm{B}(\mathbf{Z})} \cap \underbrace{\mathbf{Q}(x)\mathfrak{a}^{-1}}_{=\mathbf{Q}(x)})\mathfrak{a} \\ &= \mathcal{O}_x\mathfrak{a} \subseteq \mathfrak{a} \end{aligned}$$

This finishes the proof. □

Lemma 4.3.2. *If $x \in \mathscr{R}_3(d)$ then $\{\alpha \in \mathrm{B}(\mathbf{Q}),\ \alpha x = x\alpha\} = \mathbf{Q}(x)$.*

Proof. Let us consider the conjugation map

$$\begin{array}{rccc} \gamma_x & : & \mathrm{B}(\mathbf{Q}) & \to & \mathrm{B}(\mathbf{Q}) \\ & & z & \mapsto & xzx^{-1} \end{array}$$

It is a $\mathbf{Q}$-linear map i.e. an endomorphism of $\mathrm{B}(\mathbf{Q})$ which is a $\mathbf{Q}$-vector space of dimension 4. Since $x^2 = -d$, we have $(\gamma_x)^2 = \gamma_{-d} = \mathrm{id}$ because $-d \in \mathbf{Q}^\times = \mathcal{Z}(\mathrm{B}^\times)$. Thus, the polynomial $P := X^2 - 1$ satisfies $P(\gamma_x) = 0$, so the eigenvalues of γ_x are in $\{\pm 1\}$. Let us prove that -1 is indeed an eigenvalue for γ_x. If 1 were the only eigenvalue of γ_x, then its minimal polynomial would be $X - 1$ (since it must divide P). So γ_x would be the identity, which is equivalent to $x \in \mathbf{Q}^\times$. But this is not the case since $x^2 = -d < 0$. Therefore, -1 is an eigenvalue of γ_x. Let us take $t \in \mathrm{B}(\mathbf{Q})^\times$ such that $\gamma_x(t) = -t$. Then it is easy to prove that $(1, x, t, xt)$ is a basis of $\mathrm{B}(\mathbf{Q})$, and in this basis, the matrix of γ_x is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

This shows that $\{\alpha \in \mathrm{B}(\mathbf{Q}) \mid \gamma_x(\alpha) = \alpha\} = \mathbf{Q} + \mathbf{Q}x = \mathbf{Q}(x)$, and this gives the lemma. □

Lemma 4.3.3. *If $x, y \in \mathscr{R}_3(d)$, then $\{\alpha \in \mathrm{B}(\mathbf{Q}), x\alpha = \alpha y\}$ is a left-$\mathbf{Q}(x)$-vector space space of rank 1 (hence of rank 2 over $\mathbf{Q}$).*

Proof. Let $x, y \in \mathscr{R}_3(d)$. In particular, they are two elements in $\mathrm{B}^{(0)}(\mathbf{Q})$ with the same norm, so corollary 4.1.6 tells us that we can find $q \in \mathrm{B}^\times$ such that $y = q^{-1}xq$. Then for all $\alpha \in \mathrm{B}(\mathbf{Q})$,

$$\begin{aligned} x\alpha = \alpha y &\iff x\alpha = \alpha q^{-1}xq \iff x(\alpha q^{-1}) = (\alpha q^{-1})x \\ &\iff \alpha q^{-1} \in \mathbf{Q}(x) \quad \text{(by lemma 4.3.2)} \\ &\iff \alpha \in \mathbf{Q}(x)q \end{aligned}$$

□

We are now ready to prove the $\mathrm{Cl}(\mathcal{O}_K)$-torsor structure.

Proposition 4.3.4. *The action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\widetilde{\mathscr{R}_3}(d)^+$ is free, that is : for any $[I] \in \mathrm{Cl}(\mathcal{O}_K)$ and any $[x] \in \widetilde{\mathscr{R}_3}(d)^+$, we have*

$$[I].[x] = [x] \implies I \text{ is a principal fractional ideal.}$$

Proof. If $[I].[x] = [x]$, we can find $q \in \mathrm{B}^\times$ such that $\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})q^{-1}$ and $q^{-1}xq = x$. By lemma 4.3.2, this implies that $q^{-1} \in \mathbf{Q}(x)$, so that $\mathcal{O}_x q^{-1}$ is a (principal) fractional ideal of $\mathbf{Q}(x)$. Besides,

$$\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})q^{-1} = \mathrm{B}(\mathbf{Z})\mathcal{O}_x q^{-1}$$

because $\mathrm{B}(\mathbf{Z})\mathcal{O}_x = \mathrm{B}(\mathbf{Z})$. Now, if we intersect the equality above with $\mathbf{Q}(x)$, and use lemma 4.3.1, we get that $\iota_x(I) = \mathcal{O}_x q^{-1}$ (since $\iota_x(I)$ and $\mathcal{O}_x q^{-1}$ are two fractional ideals in $\mathbf{Q}(x)$). Therefore, $\iota_x(I)$ is a principal fractional ideal (generated by q^{-1}), and we deduce that I is principal because

$$I = \iota_x^{-1}\iota_x(I) = \iota_x^{-1}(\mathcal{O}_x q^{-1}) = \mathcal{O}_K \iota_x^{-1}(q^{-1})$$

□

Remark. *Note that so far, we did not need the assumption "$d \equiv 1, 2 \bmod 4$". The fact that there is a free action of the class group of $\mathbf{Q}(\sqrt{-d})$ on $\widetilde{\mathscr{R}_3}(d)^+$ holds true for any d admissible, square-free. It is only for the transitivity statement that we need to assume $d \equiv 1, 2 \bmod 4$.*

In order to prove the transitivity of the action, we introduce the following notation : for all $x, y \in \mathscr{R}_3(d)$,

$$\Lambda_{x \to y} := \{\lambda \in \mathrm{B}(\mathbf{Z}) \mid x\lambda = \lambda y\}$$

Let us collect some easy properties of this set in a lemma :

Lemma 4.3.5.
- *For all $x, y \in \mathscr{R}_3(d)$, $\Lambda_{x\to y}$ is a free-$\mathbf{Z}$-submodule of $\mathrm{B}(\mathbf{Z})$ of rank 2.*
- *For all $\alpha \in \mathrm{B}(\mathbf{Z})$, $x\alpha + \alpha y \in \Lambda_{x\to y}$*

Proof. For the first assertion, we remark that $\Lambda_{x\to y}$ is a sub-$\mathbf{Z}$-module of $\mathrm{B}(\mathbf{Z})$. Since $\mathrm{B}(\mathbf{Z})$ is free of rank 4, we deduce that $\Lambda_{x\to y}$ is a free $\mathbf{Z}$-module of rank less than or equal to 4 (by the adapted basis theorem for modules over a PID). In fact, lemma 4.3.3 tells us that $\{\alpha \in \mathrm{B}(\mathbf{Q}), x\alpha = \alpha y\}$ is a $\mathbf{Q}$-vector space of dimension 2, and from this fact, one can easily prove that the rank of $\Lambda_{x\to y}$ as a $\mathbf{Z}$-module is equal to 2.
The second point is just a verification, using the fact that since x and y belong to $\mathscr{R}_3(d)$, they satisfy $x^2 = y^2 = -d$. □

The transitivity rests on the following lemma, that we will only prove at the end of the section because it is quite technical.

Lemma 4.3.6. *When $d \equiv 1, 2 \bmod 4$, we have : for all $x, y \in \mathscr{R}_3(d)$, we have $\mathrm{B}(\mathbf{Z})\Lambda_{x\to y} = \mathrm{B}(\mathbf{Z})$.*

Proof. See the end of the section. It is this lemma that fails when $d \equiv 3 \bmod 8$, in fact the alternative $\mathrm{B}(\mathbf{Z})\Lambda_{x\to y} = \mathrm{B}(\mathbf{Z})(1+i)$ can also happen in this case, as it is stressed by [Reh82] (but not proved). □

Using this lemma, we are now able to prove the following proposition.

Proposition 4.3.7. *When $d \equiv 1, 2 \bmod 4$, the action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\widetilde{\mathscr{R}_3}(d)^+$ is transitive, that is : for all $[x], [y] \in \widetilde{\mathscr{R}_3}(d)^+$, there exists $[I] \in \mathrm{Cl}(\mathcal{O}_K)$ such that $[I].[x] = [y]$*

Proof. Let $x, y \in \mathscr{R}_3(d)$. The aim is to find a fractional ideal I of $\mathcal{O}_K$ such that $I.[x] = [y]$. It is easy to see that $\Lambda_{x\to y}$ is a left $\mathcal{O}_x$-module. Indeed, we know that $\mathcal{O}_x = \mathbf{Z}[x]$ (see lemma 4.2.1), so it suffices to show that if $\lambda \in \Lambda_{x\to y}$, then $x\lambda \in \Lambda_{x\to y}$, and it is a straightforward verification.
The only issue for us is that we would like to see $\Lambda_{x\to y}$ as a fractional ideal of $\mathcal{O}_x$, so that it corresponds via ι_x to an ideal of $\mathcal{O}_K$. But $\Lambda_{x\to y}$ may not be contained in $\mathbf{Q}(x)$. In fact, corollary 4.1.6 tells us that there exists $q \in \mathrm{B}^\times$ such that $y = q^{-1}xq$, and then by lemma 4.3.3, we have $\Lambda_{x\to y} \subseteq \mathbf{Q}(x)q$. Thus, if we consider $\Lambda_{x\to y}q^{-1}$ instead of $\Lambda_{x\to y}$, it will work. Indeed, $\Lambda_{x\to y}q^{-1}$ is still a left $\mathcal{O}_x$-module, and it is contained in $\mathbf{Q}(x)$. As $\mathbf{Q}(x)$ is commutative, $\Lambda_{x\to y}q^{-1}$ is also a right $\mathcal{O}_x$-module i.e. an $\mathcal{O}_x$-submodule of the quadratic field $\mathbf{Q}(x)$.
To show that it is a fractional ideal, it just remains to find $r \in \mathcal{O}_x \backslash \{0\}$ such that $r\left(\Lambda_{x\to y}q^{-1}\right) \subseteq \mathcal{O}_x$. For this, it suffices to remark that if we denote by m the lowest common multiple of the denominators that appear in the coefficients of q^{-1} (when we write q^{-1} in the basis $(1, i, j, k)$ of $\mathrm{B}(\mathbf{Q})$), then we can take $r = 2m$. Indeed, $\Lambda_{x\to y} \subseteq \mathrm{B}(\mathbf{Z})$, so any $\lambda \in \Lambda_{x\to y}$ has its coefficients in $\frac{1}{2}\mathbf{Z}$, so $r\lambda q^{-1}$ has coefficients in $\mathbf{Z}$. In particular $r\lambda q^{-1} \in \mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x) = \mathcal{O}_x$. Thus $\Lambda_{x\to y}q^{-1}$ is indeed a non-zero fractional ideal of $\mathcal{O}_x$.

Now, let us prove that if we take the fractional ideal of $\mathcal{O}_K$

$$I := \iota_x^{-1}\left(\Lambda_{x\to y}q^{-1}\right)$$

it satisfies $I.[x] = [y]$. We have $\mathrm{B}(\mathbf{Z})\iota_x(I) = \mathrm{B}(\mathbf{Z})\Lambda_{x\to y}q^{-1} = \mathrm{B}(\mathbf{Z})q^{-1}$ by the key lemma 4.3.6. Thus,

$$I.[x] = \left[q^{-1}xq\right] = [y]$$

so $[I]$ is an element of $\mathrm{Cl}(\mathcal{O}_K)$ mapping $[x]$ to $[y]$: this finishes the proof. □

Remark. *As we just proved, the fact that the action of $\mathrm{Cl}(\mathcal{O}_K)$ is transitive tells us that for each $[x], [y] \in \widetilde{\mathscr{R}_3}(d)^+$, there exists an element $[I]$ of $\mathrm{Cl}(\mathcal{O}_K)$ such that $[I].[x] = [y]$. But since we also know that the action is free, this element $[I]$ is unique ! This is why we introduce a notation for this unique element of the class group : let us denote by $[\Lambda_{x\to y}]$ the unique $[I]$ in $\mathrm{Cl}(\mathcal{O}_K)$ such that $[I].[x] = [y]$. With the notations of the proof above, $[\Lambda_{x\to y}]$ denotes $\iota_x^{-1}\left(\Lambda_{x\to y}q^{-1}\right)$. Let us insist that there is an abuse of notation, because $\Lambda_{x\to y}$ is not a fractional ideal in $\mathcal{O}_K$, so it does not really make sense to consider its equivalence class in the ideal class group of $\mathcal{O}_K$.*

Let us now conclude on the question of the number of representations of an integer as a sum of three squares.

Theorem 4.3.8. *Let $d \geqslant 2$ be a square-free admissible integer. As above, we denote by K the imaginary quadratic field $\mathbf{Q}(\sqrt{-d})$. Let us denote by h_K its class number i.e. $h_K := |\mathrm{Cl}(\mathcal{O}_K)|$. Then the number of representations of d as a sum of three squares of integers is given by the following relations :*

- $|\mathscr{R}_3(d)| = 12h_K$ *when* $d \equiv 1, 2 \bmod 4$
- $|\mathscr{R}_3(d)| = 24h_K$ *when* $d \equiv 3 \bmod 8$

Proof. As we said at the beginning of this section, we will only prove the result in the case where $d \equiv 1, 2 \bmod 4$. In this case, we just proved that there is a free and transitive action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\widetilde{\mathscr{R}_3}(d)^+$. Thus, if we fix any point $[x] \in \widetilde{\mathscr{R}_3}(d)^+$, the orbit map

$$\begin{array}{ccc} \mathrm{Cl}(\mathcal{O}_K) & \to & \widetilde{\mathscr{R}_3}(d)^+ \\ [I] & \mapsto & [I].[x] \end{array}$$

is a bijection, so $|\widetilde{\mathscr{R}_3}(d)^+| = |\mathrm{Cl}(\mathcal{O}_K)| = h_K$.
To conclude, we need to show that $|\mathscr{R}_3(d)| = 12|\widetilde{\mathscr{R}_3}(d)^+|$.

One geometric approach is the following : recall that $\widetilde{\mathscr{R}_3}(d)^+ = \mathrm{SO}_3(\mathbf{Z})^+ \backslash \mathscr{R}_3(d)$: the set of orbits for the natural action of $\mathrm{SO}_3(\mathbf{Z})^+$ on $\mathscr{R}_3(d)$ (seen as a subset of $\mathbf{Z}^3$). If we prove that this action is free, we will have that each orbit is made of exactly $12 = |\mathrm{SO}_3(\mathbf{Z})^+|$ points, and this gives the result. So we just need to prove that for all $M \in \mathrm{SO}_3(\mathbf{Z})^+$, if $Mx = x$ for some $x \in \mathscr{R}_3(d)$, then $M = \mathrm{id}$. I did not investigate this approach further, but it should be possible given the explicit description of the elements of $\mathrm{SO}_3(\mathbf{Z})^+$.

Another approach is to view $\widetilde{\mathscr{R}_3}(d)^+$ as $\mathrm{B}(\mathbf{Z})^\times \backslash \mathscr{R}_3(d)$: the set of orbits for the action of $\mathrm{B}(\mathbf{Z})^\times$ by conjugation (when we view $\mathscr{R}_3(d)$ as a subset of $\mathrm{B}^{(0)}(\mathbf{Z})$). Then we want to show that for all $x \in \mathscr{R}_3(d)$, its orbit

$$[x] = \{\varepsilon x \varepsilon^{-1} \mid \varepsilon \in \mathrm{B}(\mathbf{Z})^\times\}$$

is made of 12 elements. In order to do this, it is sufficient to show that the stabilizer of x is $\{\pm 1\}$, because then we will have a bijection

$$\mathrm{B}(\mathbf{Z})^\times / \{\pm 1\} \to [x]$$

and since $\mathrm{B}(\mathbf{Z})^\times$ is made of 24 elements, this will give the conclusion. So let us consider $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$ such that $\varepsilon x \varepsilon^{-1} = x$. Then $\varepsilon \in \mathbf{Q}(x)$ by lemma 4.3.2, so $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times \cap \mathbf{Q}(x) = \mathcal{O}_x^\times$. But $\mathcal{O}_x = \mathbf{Z}[x]$, so we can write $\varepsilon = a + bx$, and the fact that $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$ tells us that $\mathrm{N}(\varepsilon) = 1$, so $a^2 + b^2 d = 1$, which implies that $b = 0$ and $a \in \{\pm 1\}$ (because $d \geqslant 2$).

Thus, we have $|\mathscr{R}_3(d)| = 12|\widetilde{\mathscr{R}_3}(d)^+| = 12h_K$. □

Finally, let us go back to the proof we left earlier, of an important but technical lemma.

Proof of lemma 4.3.6 : Let $x, y \in \mathscr{R}_3(d)$ for some $d \geqslant 2$, square-free, $d \equiv 1 \bmod 4$ (the case $d \equiv 2 \bmod 4$ is similar). The aim is to show that

$$\mathrm{B}(\mathbf{Z})\Lambda_{x \to y} = \mathrm{B}(\mathbf{Z}).$$

First, we remark that $\mathrm{B}(\mathbf{Z})\Lambda_{x \to y}$ is a left ideal of $\mathrm{B}(\mathbf{Z})$, so we can use corollary 3.1.5 to find an element $\rho \in \mathrm{B}(\mathbf{Z})$ such that :

$$\mathrm{B}(\mathbf{Z})\Lambda_{x \to y} = \mathrm{B}(\mathbf{Z})\rho.$$

Then $\mathrm{B}(\mathbf{Z})\Lambda_{x \to y} = \mathrm{B}(\mathbf{Z})$ if and only if $\rho \in \mathrm{B}(\mathbf{Z})^\times$, if and only if $\mathrm{N}(\rho) = 1$ (see proposition 3.1.8). We will do it in two steps :

- *Step 1 : we prove that* $2 \nmid \mathrm{N}(\rho)$.

  Since $\Lambda_{x\to y} \subseteq \mathrm{B}(\mathbf{Z})\rho$ and the norm is multiplicative, we have $\mathrm{N}(\rho) \mid \mathrm{N}(\lambda)$ for all $\lambda \in \Lambda_{x\to y}$. Therefore, it suffices to find an element $\lambda \in \Lambda_{x\to y}$ such that $2 \nmid \mathrm{N}(\lambda)$ to get the conclusion of this step 1.
  Recall the following general fact (stated in lemma 4.3.5) : since $x^2 = y^2 = -d$, a straighforward verification shows that for all $\alpha \in \mathrm{B}(\mathbf{Z})$, $x\alpha + \alpha y \in \Lambda_{x\to y}$ (this will be used below).
  Now, let us write $x = x_1 i + x_2 j + x_3 k$ and $y = y_1 i + y_2 j + y_3 k$. Since $x_1^2 + x_2^2 + x_3^2 = \mathrm{N}(x) = d \equiv 1 \bmod 4$, two of the x_i's must be even, and one of them has to be odd. Let us assume, for instance, that

  $$x_1 \equiv x_2 \equiv 0 \bmod 2 \quad \text{and} \quad x_3 \equiv 1 \bmod 2$$

  It is the same for y : one of the y_i's is odd while the two others are even.

  (i) If $y_1 \equiv y_2 \equiv 0 \bmod 2$ and $y_3 \equiv 1 \bmod 2$: denote by

  $$\omega_0 := x + y = (x_1 + y_1)i + (x_2 + y_2)j + (x_3 + y_3)k$$
  $$\omega_1 := xi + iy = -(x_1 + y_1) + (x_3 - y_3)j + (y_2 - x_2)k$$

  Then w_0 and ω_1 are in $\Lambda_{x\to y}$ since they are of the form $x\alpha + \alpha y$ for some $\alpha \in \mathrm{B}(\mathbf{Z})$. Moreover, we remark that their coefficients in the basis $(1, i, j, k)$ are all even, so $\frac{\omega_0}{2}$ and $\frac{\omega_1}{2}$ are in $\mathrm{B}(\mathbf{Z})$, hence in $\Lambda_{x\to y}$. Now, let us prove that one of them has a norm which is not divisible by 2. We have

  $$\mathrm{N}(\omega_0) - \mathrm{N}(\omega_1) = 4x_2y_2 + 4x_3y_3 \equiv 4 \bmod 8$$

  so there exists $\varepsilon \in \{0, 1\}$ such that $\mathrm{N}(\omega_\varepsilon) \not\equiv 0 \bmod 8$. Then $2 \nmid \mathrm{N}\left(\frac{\omega_\varepsilon}{2}\right)$ so we can take λ to be $\frac{\omega_\varepsilon}{2}$. This gives an element in $\Lambda_{x\to y}$ such that $2 \nmid \mathrm{N}(\lambda)$.

  (ii) If $y_1 \equiv y_3 \equiv 0 \bmod 2$ and $y_2 \equiv 1 \bmod 2$: we consider $\omega := x(1 + j) + (1 + j)y$. As it is of the form $x\alpha + \alpha y$ for some $\alpha \in \mathrm{B}(\mathbf{Z})$, it belongs to $\Lambda_{x\to y}$. Besides, we have

  $$\omega = -(x_2 + y_2) + (x_1 - x_3 + y_1 + y_3)i + (x_2 + y_2)j + (x_1 + x_3 - y_1 + y_3)k$$

  and we remark that all the coefficients of ω are odd, so $\frac{\omega}{2} \in \mathrm{B}(\mathbf{Z})$. Thus $\lambda := \frac{\omega}{2}$ belongs to $\Lambda_{x\to y}$. Moreover, if we go back to the definition of the norm, expand everything, and take into account the parity conditions on the x_i's and y_i's, we see that :

  $$\mathrm{N}(\omega) \equiv 4 \bmod 8$$

  hence $2 \nmid \mathrm{N}(\lambda)$.

  (iii) It works as in case (ii), starting from $\omega := x(1 + k) + (1 + k)y$.

  Thus, we covered all the possibilities for y when x is such that x_1 and x_2 are odd and x_3 is even. The other cases for the parity of the coefficients of x can be done by similar arguments. The case $d \equiv 2 \bmod 4$ is also similar. This step 1 is the one that fails when $d \equiv 3 \bmod 8$: in this case we cannot exclude the possibility that $2 \mid \mathrm{N}(\rho)$.

- *Step 2 : we prove that for all p odd prime,* $p \nmid \mathrm{N}(\rho)$.

  Assume for a contradiction that there exists an odd prime number p such that $p \mid \mathrm{N}(\rho)$. With the notations of the case (i) in step 1, we have $\omega_0, \omega_1 \in \Lambda_{x\to y}$. In particular, they belong to $\mathrm{B}(\mathbf{Z})\Lambda_{x\to y} = \mathrm{B}(\mathbf{Z})\rho$ i.e. ρ is a right divisor of ω_0 and ω_1 in $\mathrm{B}(\mathbf{Z})$. Therefore, it is also a right divisor of $i(\omega_0 + i\omega_1) = ix - xi$. This implies that $\mathrm{N}(\rho) \mid \mathrm{N}(ix - xi) = 4(x_2^2 + x_3^2)$, hence $p \mid 4(x_2^2 + x_3^2)$. As p is an odd prime, we conclude that $p \mid x_2^2 + x_3^2$.
  Then, we do the same thing with ω_1 replaced by $\omega_1' := xj + jy$ (resp. $\omega_1'' := xk + ky$), we

have $j(\omega_0 + j\omega_1') = jx - xj$ (resp. $k(\omega_0 + k\omega_1'') = kx - xk$), and $\mathrm{N}(\rho) \mid \mathrm{N}(jx - xj)$ (resp. $\mathrm{N}(\rho) \mid \mathrm{N}(kx - xk)$). We conclude as above that $p \mid x_1^2 + x_3^2$ (resp. $p \mid x_1^2 + x_2^2$). Thus,

$$\begin{cases} x_2^2 + x_3^2 \equiv 0 \bmod p \\ x_1^2 + x_3^2 \equiv 0 \bmod p \\ x_1^2 + x_2^2 \equiv 0 \bmod p \end{cases}$$

which implies $x_1 \equiv x_2 \equiv x_3 \equiv 0 \bmod p$, because the matrix

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

is in $\mathrm{GL}_3(\mathbf{F}_p)$ (its determinant is 2, which is invertible modulo our odd prime p). But then $d = x_1^2 + x_2^2 + x_3^2 \equiv 0 \bmod p^2$, contradicting the fact that d is square-free. This finishes the proof. □

4.4 Siegel's theorem and estimate of the size of $\mathscr{R}_3(d)$

In this section, we discuss the following theorem on the size of $\mathscr{R}_3(d)$.

Theorem 4.4.1. *For any $\varepsilon > 0$, we have*

$$d^{\frac{1}{2}-\varepsilon} \ll_\varepsilon |\mathscr{R}_3(d)| \ll_\varepsilon d^{\frac{1}{2}+\varepsilon}$$

for all $d \geqslant 2$ admissible and square-free.

The notation $\ll_\varepsilon$ is introduced more precisely later in this thesis (see here), since it becomes more convenient only towards the end of the proof of the main equidistribution theorem. But we can already explain what it means in this particular statement. Theorem 4.4.1 states that for any $\varepsilon > 0$, there exist two constants $c(\varepsilon), C(\varepsilon)$, depending only on ε, such that for all $d \geqslant 2$ admissible and square-free :

$$C(\varepsilon) d^{\frac{1}{2}-\varepsilon} \leqslant |\mathscr{R}_3(d)| \leqslant c(\varepsilon) d^{\frac{1}{2}+\varepsilon}$$

The most difficult estimate is the lower bound, which comes from a famous theorem by Siegel, that we will quote without proof. This theorem gives a lower bound for the value at 1 of some L-functions attached to real Dirichlet characters. By Dirichlet class number formula, this gives an estimate of the behaviour of the class number of $\mathbf{Q}(\sqrt{-d})$ with respect to d. Finally, since we proved an exact formula connecting this class number and the size of $\mathscr{R}_3(d)$, Siegel's theorem provides in fact an estimate of the size of $\mathscr{R}_3(d)$.

Theorem 4.4.2 (Siegel, 1935)**.** *For any $\varepsilon > 0$, there exists an ineffective constant $C_1(\varepsilon) > 0$ (depending only on ε) such that for any $q \geqslant 2$, and for every real primitive Dirichlet character modulo q, we have*

$$L(1, \chi) \geqslant \frac{C_1(\varepsilon)}{q^\varepsilon}.$$

Proof. We refer to [Dav80] (and the extended proofs given in [Str08]), or [Kow04]. □

Remark. *The constant implied in the lower bound given in this theorem is ineffective since it depends on the existence or not of a real zero close to 1 of Dirichlet L-functions attached to real characters: the so-called Siegel zero.*

Now, let $d \geqslant 2$ be a square-free integer. Dirichlet class number formula (see theorem 2.4.1) applied to the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-d})$, tells us that :

$$|\mathrm{Cl}(\mathcal{O}_K)| = \frac{w}{2\pi} \sqrt{|D|} L(1, \chi_D)$$

where w is the number of units in $\mathcal{O}_K$, D is the discriminant of K, and χ_D is the Kronecker symbol. By the facts gathered in appendix B, χ_D is a real primitive Dirichlet character modulo $|D|$, so the estimate from Siegel's theorem for the value of $L(1, \chi_D)$ applies. Taking into account that $D = -d$ or $-4d$ (see the beginning of our section 2.1 on imaginary quadratic fields), we obtain that there exists a constant $C_2(\varepsilon)$, depending only on ε, such that for every $d \geqslant 2$, square-free,

$$|\mathrm{Cl}(\mathcal{O}_K)| \geqslant C_2(\varepsilon) d^{\frac{1}{2}-\varepsilon}$$

(where K still denotes $\mathbf{Q}(\sqrt{-d})$).

Finally, we use theorem 4.3.8, which gives us a connection between the class number of $\mathbf{Q}(\sqrt{-d})$ and $|\mathscr{R}_3(d)|$. We find that for any $\varepsilon > 0$, there exists a constant $C(\varepsilon)$, depending only on ε, such that for all $d \geqslant 2$ admissible and square-free,

$$|\mathscr{R}_3(d)| \geqslant C(\varepsilon) d^{\frac{1}{2}-\varepsilon} \tag{15}$$

In particular, $|\mathscr{R}_3(d)|$ tends to infinity as d goes to infinity among the admissible, square-free integers. But once we know that we have more and more integers points as the radius grows (among the admissible integers, of course), we may ask the question of the distribution of these integers points on the sphere. Are they evenly distributed ? Or do certain regions of the sphere "attract" more integer points ? This is the type of questions we are going to discuss in the next section.

One may also ask if we have an interesting upper bound for $|\mathscr{R}_3(d)|$, in order to know if the previous lower bound is the best we can hope for. In fact, the question of the upper bound is more elementary. In the appendix on L-functions, and more precisely : in proposition A.9, we prove an elementary upper bound for $L(1, \chi)$ when χ is a non-trivial Dirichlet character. It implies that there exists a constant c such that for all $q \geqslant 2$ and for any non-trivial Dirichlet character modulo q :

$$L(1, \chi) \leqslant c \ln(q)$$

In particular, for any $\varepsilon > 0$, there exists a constant $c(\varepsilon)$, depending only on ε, such that for any $q \geqslant 2$, and for every real primitive Dirichlet character modulo q, we have :

$$L(1, \chi) \leqslant c_1(\varepsilon) q^{\varepsilon}$$

Now by the same arguments as above, we can deduce that for any $\varepsilon > 0$, there exists a constant $c(\varepsilon)$, depending only on ε, such that for all $d \geqslant 2$ admissible and square-free,

$$|\mathscr{R}_3(d)| \leqslant c(\varepsilon) d^{\frac{1}{2}+\varepsilon} \tag{16}$$

Combining (15) and (16), we obtain that the growth of $|\mathscr{R}_3(d)|$ (among the admissible, square-free values of d) is approximately the same as $\sqrt{d}$.

5. Equidistribution of the integer points on the discrete sphere

The first equidistribution result regarding the integer points on spheres was proved by Linnik in the late 50's, using dynamical ideals.

Theorem 5.0.1 (Linnik). *As $d \to +\infty$ among the admissible, square-free, integers satisfying $d \equiv \pm 1 \bmod 5$, the set*

$$\left\{ \frac{\mathbf{x}}{\sqrt{d}},\ \mathbf{x} \in \mathscr{R}_3(d) \right\} \subseteq S_2$$

becomes equiditributed on the unit sphere S_2 with respect to the Lebesgue probability measure.

This means that if we denote by red_∞ the scaling map

$$\begin{array}{rccc} \mathrm{red}_\infty & : & \mathscr{R}_3(d) & \to & S_2 \\ & & \mathbf{x} & \mapsto & \frac{1}{\sqrt{d}}\mathbf{x} \end{array}$$

then the number of elements of $\mathscr{R}_3(d)$ falling inside some subset $\Omega \subseteq S_2$, divided by the total number of points in $\mathscr{R}_3(d)$, converges as d goes to $+\infty$, to the area of Ω (with the notion of area given by the renormalized Lebesgue measure on S_2, so that $\mathrm{area}(S_2) = 1$). In other words

$$\frac{|\mathrm{red}_\infty^{-1}(\Omega)|}{|\mathscr{R}_3(d)|} \underset{d \to +\infty}{\longrightarrow} \mathrm{area}(\Omega)$$

where the limit is taken among the integers d satisfying the conditions in the theorem. In fact, the condition $d \equiv \pm 1 \bmod 5$ is the Linnik condition at the prime 5, it is equivalent to the statement "the prime 5 is split in $\mathbf{Q}(\sqrt{-d})$" (thanks to proposition 2.1.8). This condition can be replaced by Linnik's condition at any arbitrary prime $p > 3$: then the limit must be taken among the d's such that p is split in $\mathbf{Q}(\sqrt{-d})$. This condition will ensure that the trajectories we define on $\mathscr{R}_3(d)$ are "interesting", in the sense that they will visit many $\mathrm{SO}_3(\mathbf{Z})$-orbits of $\mathscr{R}_3(d)$. Indeed, we are going to define trajectories on $\mathscr{R}_3(d)$ in a way that lifts the action of the subgroup $[\mathfrak{p}]^{\mathbf{Z}}$ of $\mathrm{Cl}\left(\mathcal{O}_{\mathbf{Q}(\sqrt{-d})}\right)$ on $\widetilde{\mathscr{R}_3(d)}^+$, where $\mathfrak{p}$ is a prime ideal above p. But if p is inert, then $[\mathfrak{p}]$ is the trivial element of $\mathrm{Cl}\left(\mathcal{O}_{\mathbf{Q}(\sqrt{-d})}\right)$, and if p is totally ramified, then $[\mathfrak{p}]$ is an element of order 2 in the class group. In both cases, the action of $[\mathfrak{p}]^{\mathbf{Z}}$ is rather simple at the level of $\mathrm{SO}_3(\mathbf{Z})^+$-orbits. We want the trajectories to reach more orbits, and this is why there is this Linnik's condition.

In the article [EMV10], the authors mention the fact that removing this condition was considered a very difficult problem. It is only thirty years after the work of Linnik that this question was solved, by a totally different approach, by Duke (see [Duk88]), and independently by Fomenko and Golubeva (see [FG90]). I did not have time to read about their proofs, since the aim of this master thesis was to understand Linnik's original method, but let me give a few keywords for readers interested in learning more about this. In Duke's approach, the idea is to use a Weyl criterion adapted to the equidistribution problem. The Weyl sums that appear are Fourier coefficients of half-integral weight modular forms. Then, proving the equidistribution result is equivalent to proving non-trivial bounds for these Fourier coefficients.

To illustrate the ideas of the ergodic method with less technicalities, we will focus on a discrete analogue of theorem 5.0.1. Namely, we will look at the distribution of the congruences of the points in $\mathscr{R}_3(d)$. For q an integer coprime with d, let us denote by $\mathscr{R}_3(d,q)$ the sphere modulo q :

$$\mathscr{R}_3(d,q) := \left\{ (\overline{x},\overline{y},\overline{z}) \in (\mathbf{Z}/q\mathbf{Z})^3\ ,\ \overline{x}^2 + \overline{y}^2 + \overline{z}^2 = \overline{d} \right\}$$

We will discuss the proof of the following theorem.

Theorem 5.0.2 (Linnik). *Let q be a fixed integer, coprime with 30. As $d \to +\infty$ among the admissible, square-free integers satisfying $d \equiv \pm 1 \bmod 5$ and $\gcd(d,q) = 1$, the set*

$$\{\mathbf{x} \bmod q,\ \mathbf{x} \in \mathscr{R}_3(d)\} \subseteq \mathscr{R}_3(d,q)$$

becomes equidistributed on $\mathscr{R}_3(d,q)$, with respect to the uniform measure.

In other words, if we denote by $\mathrm{red}_q : \mathscr{R}_3(d) \to \mathscr{R}_3(d,q)$ the reduction modulo q of the three coordinates, the theorem asserts that for all $\overline{\mathbf{x}} \in \mathscr{R}_3(d,q)$,

$$\frac{|\mathrm{red}_q^{-1}(\overline{\mathbf{x}})|}{|\mathscr{R}_3(d)|} \underset{d\to+\infty}{\sim} \frac{1}{|\mathscr{R}_3(d,q)|}$$

Once again, the condition $d \equiv \pm 1 \bmod 5$ is Linnik's condition at 5, but the same theorem holds for any prime $p > 3$, replacing the condition "q coprime with 30" by "q coprime with $6p$", and "$d \equiv \pm 1 \bmod 5$" by "d such that p splits in $\mathbf{Q}(\sqrt{-d})$". In fact, we will explain the proof of a refinement of this theorem, which asserts that this equidistribution is "almost uniform" in $\overline{\mathbf{x}}$.

More precisely, for any $\overline{\mathbf{x}} \in \mathscr{R}_3(d,q)$, denote by $\mathrm{dev}_d(\overline{\mathbf{x}})$ the *deviation at* $\overline{\mathbf{x}}$:

$$\mathrm{dev}_d(\overline{\mathbf{x}}) := \frac{|\mathrm{red}_q^{-1}(\overline{\mathbf{x}})|}{|\mathscr{R}_3(d)|}|\mathscr{R}_3(d,q)| - 1$$

Theorem 5.0.2 is then equivalent to : for all $\overline{\mathbf{x}} \in \mathscr{R}_3(d,q)$, $\mathrm{dev}_d(\overline{\mathbf{x}}) \underset{d\to+\infty}{\longrightarrow} 0$. We will discuss the following refinement :

Theorem 5.0.3 ([EMV10], Theorem 1.8)**.** *Fix $\nu, \delta > 0$ and suppose that $q \leqslant d^{\frac{1}{2}-\nu}$ and $\gcd(q,30) = 1$. Then the fraction of $\overline{\mathbf{x}} \in \mathscr{R}_3(d,q)$ for which $|\mathrm{dev}_d(\overline{\mathbf{x}})| > \delta$:*

$$\frac{|\{\overline{\mathbf{x}} \in \mathscr{R}_3(d,q), |\mathrm{dev}_d(\overline{\mathbf{x}})| > \delta\}|}{|\mathscr{R}_3(d,q)|}$$

tends to zero as $d \to +\infty$ (with $d \equiv \pm 1 \bmod 5$, admissible, square-free).

In this theorem, one can also replace Linnik's condition at 5 by the condition at any fixed prime $p > 3$ (this is what we will do).

Let us sketch the main ideas of the proof :

- Let us denote by $\mathfrak{p}$ and $\mathfrak{p}'$ the ideals above p in the ring of integers of $K = \mathbf{Q}(\sqrt{-d})$. Consider the subgroup $[\mathfrak{p}]^{\mathbf{Z}}$ of $\mathrm{Cl}(\mathcal{O}_K)$. This subgroup acts on $\widetilde{\mathscr{R}_3(d)^+}$. The first step consists in lifting this action to an action of $[\mathfrak{p}]^{\mathbf{Z}}$ on $\mathscr{R}_3(d)$. This is the aim of section 5.1.
- Once we have an action of $[\mathfrak{p}]^{\mathbf{Z}}$ on $\mathscr{R}_3(d)$, we attach to each point $\mathbf{x} \in \mathscr{R}_3(d)$ a *trajectory* on $\mathscr{R}_3(d)$: it is roughly defined as the sequence of points $([\mathfrak{p}]^i\mathbf{x})_{i\in\mathbf{Z}}$ (but in fact, we need to keep track of the transition matrices which allow us to go from one point of the trajectory to the next one, so a trajectory consists of a little bit more data than just the sequence of its points).
- Then, we endow $\mathscr{R}_3(d,q)$ with a graph structure, and we define trajectories on $\mathscr{R}_3(d,q)$ by reducing modulo q the trajectories on $\mathscr{R}_3(d)$, while keeping track of the transition matrices.
- Finally, we prove theorem 5.0.3 by contradiction. If we assume that the result does not hold, then many points of $\mathscr{R}_3(d)$ (essentially all of them) will give rise to trajectories on $\mathscr{R}_3(d,q)$ which will be exceptional, in the sense that they will satisfy a large deviation inequality. Then, we prove that this implies that many non-backtracking walks on the graph $\mathscr{R}_3(d,q)$ will be exceptional. But the fact that $\mathscr{R}_3(d,q)$ is an expander will ensure that the number of exceptional walks must actually be rather small. Thus, we will get a contradiction because we will find that too many walks satisfy the large deviation inequality.

5.1 Lifting the action of $[\mathfrak{p}]^{\mathbf{Z}}$ to $\mathscr{R}_3(d)$

In section 4.2, we defined an action of the class group of $\mathbf{Q}(\sqrt{-d})$ on $\widetilde{\mathscr{R}_3}(d)^+$ when d is square-free and admissible. We considered this quotient $\widetilde{\mathscr{R}_3}(d)^+$ of $\mathscr{R}_3(d)$ merely because for any $q \in \mathrm{B}(\mathbf{Z})$, the left-ideal $\mathrm{B}(\mathbf{Z})q$ is the same as $\mathrm{B}(\mathbf{Z})\varepsilon q$ for any $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$. Taking a quotient of $\mathscr{R}_3(d)$ was a way to get an action which does not depend on the choice of a generator of an ideal in $\mathrm{B}(\mathbf{Z})$. However, if we allow ourselves to choose arbitrarily a generator, we will be able to lift the action to $\mathscr{R}_3(d)$. Although it is less canonical to work with $\mathscr{R}_3(d)$ instead of $\widetilde{\mathscr{R}_3}(d)^+$ (arbitrary choices are made), this will give rise to trajectories on $\mathscr{R}_3(d)$, and the study of these trajectories is the core of the ergodic method we aim to present here.

Let d be an admissible square-free integer, and let K be $\mathbf{Q}(\sqrt{-d})$. Let $p > 3$ be a rational prime which is split in K. Write

$$p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$$

Then we have the following proposition :

Proposition 5.1.1. *For any $x \in \mathscr{R}_3(d)$ (viewed as a trace-free quaternion), there exists $z \in \mathrm{B}(\mathbf{Z})$, unique modulo multiplication on the left by an element of $\mathrm{B}(\mathbf{Z})^\times$ such that $\mathrm{B}(\mathbf{Z})\iota_x(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})z$. Besides, $\mathrm{N}(z) = p$.*

Proof. As $\mathfrak{p} \subseteq \mathcal{O}_K$, we have $\iota_x(\mathfrak{p}) \subseteq \iota_x(\mathcal{O}_K) = \mathcal{O}_x = \mathrm{B}(\mathbf{Z}) \cap \mathbf{Q}(x)$ (see lemma 4.2.1). In particular $\mathrm{B}(\mathbf{Z})\iota_x(\mathfrak{p}) \subseteq \mathrm{B}(\mathbf{Z})$, so it is a left-ideal of $\mathrm{B}(\mathbf{Z})$. By corollary 3.1.5, There exists $z \in \mathrm{B}(\mathbf{Z})$ such that $\mathrm{B}(\mathbf{Z})\iota_x(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})z$. Moreover if $z' \in \mathrm{B}(\mathbf{Z})$ is such that $\mathrm{B}(\mathbf{Z})z = \mathrm{B}(\mathbf{Z})z'$, then $\mathrm{N}(z) \mid \mathrm{N}(z')$ and $\mathrm{N}(z') \mid \mathrm{N}(z)$, hence $\mathrm{N}(z) = \mathrm{N}(z')$. Now, $z' \in \mathrm{B}(\mathbf{Z})z' = \mathrm{B}(\mathbf{Z})z$, so we can write $z' = \varepsilon z$ for some $\varepsilon \in \mathrm{B}(\mathbf{Z})$. Taking the norms in this equality gives us $\mathrm{N}(\varepsilon) = 1$ i.e. $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$. This shows the first part of the statement.

Let us prove that $\mathrm{N}(z) = p$. We have :

$$\mathrm{B}(\mathbf{Z})\iota_x(p\mathcal{O}_K) = \mathrm{B}(\mathbf{Z})\iota_x(p)\iota_x(\mathcal{O}_K) = (\mathrm{B}(\mathbf{Z})\mathcal{O}_x)p = \mathrm{B}(\mathbf{Z})p$$

Since $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}' \subset \mathfrak{p}$, $\mathrm{B}(\mathbf{Z})\iota_x(p\mathcal{O}_K) \subseteq \mathrm{B}(\mathbf{Z})\iota_x(\mathfrak{p})$, hence $\mathrm{B}(\mathbf{Z})p \subseteq \mathrm{B}(\mathbf{Z})z$. This implies that $\mathrm{N}(z)$ divides $\mathrm{N}(p) = p^2$, so $\mathrm{N}(z) \in \{1, p, p^2\}$.

- If $\mathrm{N}(z) = 1$, then $\mathrm{B}(\mathbf{Z})z = \mathrm{B}(\mathbf{Z}) = \mathrm{B}(\mathbf{Z})\iota_x(\mathcal{O}_K)$. Thus $\mathrm{B}(\mathbf{Z})\iota_x(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})\iota_x(\mathcal{O}_K)$. By lemma 4.3.1 we would get that $\mathfrak{p} = \mathcal{O}_K$, which is a contradiction.
- If $\mathrm{N}(z) = p^2$, then we use the inclusion $\mathrm{B}(\mathbf{Z})p \subseteq \mathrm{B}(\mathbf{Z})z$ to find $u \in \mathrm{B}(\mathbf{Z})$ such that $p = uz$. Taking the norms leads to $\mathrm{N}(u) = 1$ i.e. $u \in \mathrm{B}(\mathbf{Z})^\times$. Then $\mathrm{B}(\mathbf{Z})p = \mathrm{B}(\mathbf{Z})z$, wich implies $\mathfrak{p} = p\mathcal{O}_K$ (again by lemma 4.3.1) : contradiction.

This proves that $\mathrm{N}(z) = p$. □

Let us denote by $\mathcal{H}_p$ the set $\{z \in \mathrm{B}(\mathbf{Z}),\ \mathrm{N}(z) = p\}$ and by $\widetilde{\mathcal{H}_p}$ the quotient $\mathrm{B}(\mathbf{Z})^\times\backslash\mathcal{H}_p$ (the set of orbits for the action of $\mathrm{B}(\mathbf{Z})^\times$ on $\mathcal{H}_p$ by left multiplication). We denote by $[z]$ the orbit of z, so in other words we have

$$[z] = \left\{\varepsilon z,\ \varepsilon \in \mathrm{B}(\mathbf{Z})^\times\right\}$$

and $\widetilde{\mathcal{H}_p} = \{[z], z \in \mathcal{H}_p\}$.

The above proposition tells us that for all $x \in \mathscr{R}_3(d)$, there exists a unique $[z] \in \widetilde{\mathcal{H}_p}$ such that $\mathrm{B}(\mathbf{Z})\iota_x(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})z'$ for any $z' \in [z]$. At this point, what we did in the previous section was to define the image of $[x] \in \widetilde{\mathscr{R}_3}(d)^+$ under the action of $[\mathfrak{p}] \in \mathrm{Cl}(\mathcal{O}_K)$ as $[y] = [zxz^{-1}]$. The advantage is that this image $[y]$ does not depend on the choice of a representative for the orbit $[z] \in \widetilde{\mathcal{H}_p}$. But a drawback is that it does not give a unique point in $\mathscr{R}_3(d)$ as the image of x, but rather a set of points. However, if we choose an arbitrary representative set of the quotient $\widetilde{\mathcal{H}_p}$, say $\{z_1, \ldots, z_{p+1}\}$ (we will explain

why $|\widetilde{\mathcal{H}_p}| = p+1$), this will allow us to define a real image of x in $\mathscr{R}_3(d)$. Indeed, it suffices to take the unique i such that $\mathrm{B}(\mathbf{Z})\iota_x(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})z_i$, and then define $y := z_i x z_i^{-1}$. Then by definition, the equivalence class of y in $\widetilde{\mathscr{R}_3(d)^+}$ corresponds to the action of $[\mathfrak{p}]$ on $[x]$, so in this sense, we can say that we lift the previous action of $[\mathfrak{p}]^{\mathbf{Z}}$ on $\widetilde{\mathscr{R}_3(d)^+}$ to an "action" on $\mathscr{R}_3(d)$.

Remark. *We put the word action between quotes because we think of $y = z_i x z_i^{-1}$ as the point of $\mathscr{R}_3(d)$ obtained by the action of $[\mathfrak{p}]$ on x, but we do not claim that this defines a real group action of $[\mathfrak{p}]^{\mathbf{Z}}$ on $\mathscr{R}_3(d)$. For instance, if the representative set $\{z_1, \dots, z_{p+1}\}$ is not stable under taking the inverse, the equality $[\mathfrak{p}].[\mathfrak{p}'].x = x$ may not hold for some x in $\mathscr{R}_3(d)$.*

Now our aim is to explain how we choose a set of representatives for $\widetilde{\mathcal{H}_p}$. This set is easier to describe in terms of matrices, so that is why we try to interpret the elements $z \in \mathcal{H}_p$ in terms of their matrix $\gamma_z \in \mathrm{SO}_3(\mathbf{Q})$ (the matrix of the conjugation by z).

Definition 5.1.2. *Let us denote by $\mathcal{M}_p$ the set of rotations "with denominator p" :*

$$\mathcal{M}_p := \{M \in \mathrm{SO}_3(\mathbf{Q}) \mid pM \in \mathcal{M}_3(\mathbf{Z}) \text{ but } M \notin \mathcal{M}_3(\mathbf{Z})\}$$

Since $\mathrm{SO}_3(\mathbf{Z}) = \mathrm{SO}_3(\mathbf{Q}) \cap \mathcal{M}_3(\mathbf{Z})$, we have

$$\mathcal{M}_p = \{M \in \mathrm{SO}_3(\mathbf{Q}) \mid pM \in \mathcal{M}_3(\mathbf{Z})\} \setminus \mathrm{SO}_3(\mathbf{Z})$$

Lemma 5.1.3. *The map $z \mapsto \gamma_z$ (see the section 4.1 on geometric aspects of quaternions) induces a map from $\mathcal{H}_p$ to $\mathcal{M}_p$. In other words, the rotation corresponding to the conjugation by a Hurwitz quaternion of norm p is a matrix with denominator p.*

Proof. This can be seen as a consequence of the following fact on Hurwitz quaternions :
if z is a Hurwitz quaternion such that all its coefficients in the basis $(1, i, j, k)$ are in $\mathbf{Z} + \frac{1}{2}$, we can always find a unit ε in $\mathrm{B}(\mathbf{Z})^\times$ such that εz has coefficients in $\mathbf{Z}$.
This is proved in [Hin08], chapter III for instance.

Indeed, let us take $z \in \mathcal{H}_p$ (a Hurwitz quaternion of norm p), and let $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$ be such that εz has coefficients in $\mathbf{Z}$. Then $\gamma_{\varepsilon z} = \gamma_\varepsilon \gamma_z$, and we know from proposition 4.1.10 that γ_ε is an element of $\mathrm{SO}_3(\mathbf{Z})^+$. Therefore, if we prove that $\gamma_{\varepsilon z} \in \mathcal{M}_p$, we will get that $\gamma_z = \gamma_\varepsilon^{-1}\gamma_{\varepsilon z} \in \mathcal{M}_p$. Indeed, γ_ε is just a permutation matrix with eventual signs, so it will not create denominators. Thus, we are reduced to the case where z is a quaternion of norm p with coefficients in $\mathbf{Z}$. In this case, as $z^{-1} = \frac{\overline{z}}{\mathrm{N}(z)} = \frac{\overline{z}}{p}$, it is clear from the formula

$$\gamma_z(x) = zx\frac{\overline{z}}{p}$$

that the matrix γ_z satisfies the condition $p\gamma_z \in \mathcal{M}_3(\mathbf{Z})$. It remains to check that $\gamma_z \notin \mathrm{SO}_3(\mathbf{Z})$. But if $\gamma_z \in \mathrm{SO}_3(\mathbf{Z})$, then since $\mathrm{SO}_3(\mathbf{Z}) = \mathrm{SO}_3(\mathbf{Z})^+ \sqcup \gamma_{1+i}\mathrm{SO}_3(\mathbf{Z})^+$ and $\mathrm{SO}_3(\mathbf{Z})^+$ is the image of $\mathrm{B}(\mathbf{Z})^\times$, we would find an element $v \in \mathrm{B}(\mathbf{Z})^\times \sqcup (1+i)\mathrm{B}(\mathbf{Z})^\times$ such that $\gamma_z = \gamma_v$ (see proposition 4.1.10 and corollary 4.1.11). Then there exists $\lambda \in \mathbf{Q}^\times$ such that $z = \lambda v$. Let us write $\lambda = a/b$ with a, b two coprime integers. Then if we take the norm in the equality $z = \lambda v$ we obtain $b^2\mathrm{N}(z) = a^2\mathrm{N}(v)$, hence $b^2 \mid \mathrm{N}(v)$. As $v \in \mathrm{B}(\mathbf{Z})^\times \sqcup (1+i)\mathrm{B}(\mathbf{Z})^\times$, its norm is either 1 or 2, which implies that $b^2 = 1$. We deduce that $\mathrm{N}(z) = p = a^2\mathrm{N}(v)$. As p is square-free, this implies that $a^2 = 1$, but then $p = \mathrm{N}(v)$: this is a contradiction since $\mathrm{N}(v) \in \{1, 2\}$, and p is an odd prime. This finishes to prove that $\gamma_z \in \mathcal{M}_p$.
Thus, $z \mapsto \gamma_z$ induces a map from $\mathcal{H}_p$ to $\mathcal{M}_p$: the rotation corresponding to a Hurwitz quaternion of norm p is a matrix with denominator p. □

Now, $\mathrm{SO}_3(\mathbf{Z})$ acts on $\mathcal{M}_p$ by left multiplication, and we denote by $\widetilde{\mathcal{M}_p}$ the quotient $\mathrm{SO}_3(\mathbf{Z})\backslash\mathcal{M}_p$.

Proposition 5.1.4. *The map $z \mapsto \gamma_z$ induces a bijection between $\widetilde{\mathcal{H}_p}$ and $\widetilde{\mathcal{M}_p}$.*

Proof. • The previous lemma tells us that $z \mapsto \gamma_z$ defines a map from $\mathcal{H}_p$ to $\mathcal{M}_p$. Now, we compose this map with the surjection mapping a matrix to its class modulo the action of $\mathrm{SO}_3(\mathbf{Z})$. We obtain

$$\begin{array}{rccc} \varphi & : & \mathcal{H}_p & \to & \widetilde{\mathcal{M}_p} \\ & & z & \mapsto & \mathrm{SO}_3(\mathbf{Z})\gamma_z \end{array}$$

The aim is to prove that this map is surjective, and that $\varphi(z) = \varphi(z')$ if and only if there exists $\varepsilon \in \mathrm{B}(\mathbf{Z})^\times$ such that $z' = \varepsilon z$.

- If $z, z' \in \mathcal{H}_p$ are such that $\varphi(z) = \varphi(z')$ then there exists $\delta \in \mathrm{SO}_3(\mathbf{Z}) = \mathrm{SO}_3(\mathbf{Z})^+ \sqcup \gamma_{1+i}\mathrm{SO}_3(\mathbf{Z})^+$ such that $\gamma_{z'} = \delta\gamma_z$. In other words, there exists $v \in \mathrm{B}(\mathbf{Z})^\times \sqcup (1+i)\mathrm{B}(\mathbf{Z})^\times$ such that $\gamma_{z'} = \gamma_v\gamma_z$. This implies that there exists $\lambda \in \mathbf{Q}^\times$ such that $z' = \lambda vz$.
  - If we assume that $v \in (1+i)\mathrm{B}(\mathbf{Z})^\times$, then $\mathrm{N}(v) = 2$, so when we take the norms we obtain $p = 2\lambda^2 p$, hence $\lambda = \pm\frac{1}{\sqrt{2}}$: this is a contradiction since $\sqrt{2} \notin \mathbf{Q}$.
  - Thus, we are necessarily in the case where $v \in \mathrm{B}(\mathbf{Z})^\times$. Then if we take the norms we obtain $\lambda^2 = 1$, so $\lambda \in \{\pm 1\}$ and this gives the conclusion : $z' = \pm vz$ with v (and also $-v$) in $\mathrm{B}(\mathbf{Z})^\times$.

  Conversely, if $z' = vz$ for some $v \in \mathrm{B}(\mathbf{Z})^\times$, then $\gamma_{z'} = \gamma_v\gamma_z$ and $\gamma_v \in \mathrm{SO}_3(\mathbf{Z})$ by proposition 4.1.10. Thus, $\mathrm{SO}_3(\mathbf{Z})\gamma_{z'} = \mathrm{SO}_3(\mathbf{Z})\gamma_z$.

- Let us prove the surjectivity. We want to prove that for any $M \in \mathcal{M}_p$, the orbit $\mathrm{SO}_3(\mathbf{Z})M$ contains a matrix γ_x for some $x \in \mathcal{H}_p$.
  Let $M \in \mathcal{M}_p$. In particular, $M \in \mathrm{SO}_3(\mathbf{Q})$, so proposition 4.1.5 tells us that we can find $x \in \mathrm{B}^\times$ (a non-zero element of $\mathrm{B}(\mathbf{Q})$) such that $M = \gamma_x$. Moreover, for all $\lambda \in \mathbf{Q}^\times$, $\gamma_{\lambda x} = \gamma_x$, so we can kill all the eventual denominators in the coefficients of x, and assume that x has coefficients in $\mathbf{Z}$. For the same reason, we can divide by the greatest common divisors of all the coefficients of x, and still get that the corresponding rotation is the same. Thus, we can write $M = \gamma_x$ where $x = a + bi + cj + dk$ is a quaternion with $a, b, c, d \in \mathbf{Z}$ and $\gcd(a, b, c, d) = 1$.

  Then we can compute the matrix of γ_x : it suffices to write $xix^{-1}, xjx^{-1}, xkx^{-1}$ in the basis i, j, k (recall that $x^{-1} = \frac{\overline{x}}{\mathrm{N}(x)}$). We obtain

$$\gamma_x = \frac{1}{\mathrm{N}(x)} \begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2+c^2-b^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2+d^2-c^2-b^2 \end{pmatrix}$$

  Since $\gamma_x = M \in \mathcal{M}_p$, the matrix $p\gamma_x$ has coefficients in $\mathbf{Z}$. Therefore :

$$\mathrm{Tr}(p\gamma_x) = p\frac{3a^2-b^2-c^2-d^2}{\mathrm{N}(x)} = \frac{4pa^2}{\mathrm{N}(x)} - p \in \mathbf{Z}$$

  hence :

$$\frac{4pa^2}{\mathrm{N}(x)} \in \mathbf{Z}. \tag{17}$$

  Now, looking at the coefficient $(1,1)$ of the matrix, we also have that

$$p\frac{a^2+b^2-c^2-d^2}{\mathrm{N}(x)}$$

  must be an integer. But it is equal to

$$\frac{2p(a^2+b^2)}{\mathrm{N}(x)} - p$$

  so if we multiply by 2 we get that

$$\frac{4pa^2}{\mathrm{N}(x)} + \frac{4pb^2}{\mathrm{N}(x)} - 2p \in \mathbf{Z}.$$

  As we already know from the computation of the trace, the first term is an integer, hence :

$$\frac{4pb^2}{\mathrm{N}(x)} \in \mathbf{Z}. \tag{18}$$

Similar computations with the other diagonal coefficients of the matrix lead to

$$\frac{4pc^2}{\mathrm{N}(x)} \in \mathbf{Z} \text{ and } \frac{4pd^2}{\mathrm{N}(x)} \in \mathbf{Z}. \tag{19}$$

We deduce from (17), (18) and (19) that $\mathrm{N}(x) \mid 4p\gcd(a^2, b^2, c^2, d^2) = 4p$. Thus,

$$\mathrm{N}(x) \in \{1, 2, 4, p, 2p, 4p\}$$

- If $\mathrm{N}(x) = 1$: then x is a Hurwitz quaternion of norm 1, so it is in $\mathrm{B}(\mathbf{Z})^\times$, and we know that in this case the matrix γ_x is in $\mathrm{SO}_3(\mathbf{Z})^+$. But this contradicts the fact that $\gamma_x = M \in \mathcal{M}_p$ since we excluded $\mathrm{SO}_3(\mathbf{Z})$ from the matrices of $\mathcal{M}_p$.
- If $\mathrm{N}(x) = 2$: then $x' := (1+i)x$ still has coefficients in $\mathbf{Z}$. Let us write it as

  $$x' = a' + b'i + c'j + d'k.$$

  Then we have $\mathrm{N}(x') = (a')^2 + (b')^2 + (c')^2 + (d')^2 = \mathrm{N}(1+i)\mathrm{N}(x) = 4$. But is is easy to see that the only way that a sum of four squares can be congruent to zero modulo 4 is that the four integers have the same parity. Thus, a', b', c' and d' have the same parity, so that $\frac{x'}{2}$ is a Hurwitz quaternion. Besides, it has norm 1, so $\frac{x'}{2} \in \mathrm{B}(\mathbf{Z})^\times$. We deduce that $\gamma_{\frac{x'}{2}} \in \mathrm{SO}_3(\mathbf{Z})^+$. But since $2 \in \mathbf{Q}^\times = \mathcal{Z}(\mathrm{B}^\times)$, $\gamma_{\frac{x'}{2}} = \gamma_{x'} = \gamma_{1+i}\gamma_x$. Thus,

  $$\gamma_x = \gamma_{1+i}^{-1}\gamma_{x'} \in \mathrm{SO}_3(\mathbf{Z})$$

  since both γ_{1+i} and $\gamma_{x'}$ belong to $\mathrm{SO}_3(\mathbf{Z})$. This contradicts the fact that $\gamma_x = M \in \mathcal{M}_p$.
- If $\mathrm{N}(x) = 4$: then $a^2 + b^2 + c^2 + d^2 = 4$, and a, b, c, d are all integers. So we don't have many possibilities. Either one coefficient equals ± 2 and all the others are zero, or all the coefficients equal ± 1. In any case, $\frac{x}{2}$ is a Hurwitz quaternion, and its norm is one, so $\frac{x}{2} \in \mathrm{B}(\mathbf{Z})^\times$, hence $\gamma_x = \gamma_{\frac{x}{2}} \in \mathrm{SO}_3(\mathbf{Z})$. This contradicts the fact that $\gamma_x \in \mathcal{M}_p$.

Thus, $\mathrm{N}(x) \in \{p, 2p, 4p\}$. Now,

- if $\mathrm{N}(x) = 4p$: then $a^2 + b^2 + c^2 + d^2 \equiv 0 \bmod 4$, and it is easy to see that this implies that all the coefficients have the same parity. Therefore, $\frac{x}{2}$ is a Hurwitz quaternion, and it has norm p. Since $\gamma_x = \gamma_{\frac{x}{2}}$ we obtain the conclusion because we wrote M as the conjugation by a Hurwitz quaternion of norm p.
- if $\mathrm{N}(x) = 2p$: In this case, we cannot write M as a γ_z for some $z \in \mathcal{H}_p$, but we are going to prove that in the orbit $\mathrm{SO}_3(\mathbf{Z})M$, there is such a γ_z. In fact it is the same trick as in the case $\mathrm{N}(x) = 2$: we consider $x' := (1+i)x$. This is a quaternion with coefficients in $\mathbf{Z}$, and norm $4p$ ($\equiv 0 \bmod 4$). Hence all the coefficients of x' have the same parity. So $\frac{x'}{2}$ is a Hurwitz quaternion of norm p, and

  $$\gamma_{\frac{x'}{2}} = \gamma_{x'} = \gamma_{1+i}\gamma_x \in \mathrm{SO}_3(\mathbf{Z})M$$

- if $\mathrm{N}(x) = p$: then there is nothing to do, $M = \gamma_x$ is the rotation associated with a Hurwitz quaternion of norm p.

□

Remark. *This proof sheds light on an important point : the map $z \mapsto \gamma_z$ is not surjective from $\mathcal{H}_p \to \mathcal{M}_p$. We really need to take the $\mathrm{SO}_3(\mathbf{Z})$-orbits to be able to "reach" any element of $\mathcal{M}_p$ (up to multiplication by an element of $\mathrm{SO}_3(\mathbf{Z})$). Indeed, the case $\mathrm{N}(x) = 2p$ in the proof shows that sometimes, $M \in \mathcal{M}_p$ cannot be written as γ_z for some $z \in \mathcal{H}_p$, but one needs to take a Hurwitz quaternion of norm $2p$ instead. However, the orbit $\mathrm{SO}_3(\mathbf{Z})M$ contains some γ_z where $z \in \mathcal{H}_p$.*

This proposition makes a connection between some subset of matrices with denominator p that we introduce below and Hurwitz quaternions of norm p. It is very important in order to understand why this strange set of matrices has a something to do with the action of $[\mathfrak{p}]$ and $[\mathfrak{p}']$ on $\widetilde{\mathscr{R}_3(d)^+}$.

Definition 5.1.5. *Let us denote by $\mathcal{A}_p$ the set of matrices $M \in \mathcal{M}_p$ such that their reduction modulo 3 is equal to the identity matrix.*

Let us stress that since $p > 3$, it is invertible modulo 3, so it makes sense to look at the reduction modulo 3 of a matrice with denominator p. For instance, when $p = 5$, the matrices

$$A := \frac{1}{5}\begin{pmatrix} 5 & 0 & 0 \\ 0 & -4 & 3 \\ 0 & -3 & -4 \end{pmatrix} \text{ and } D := \frac{1}{5}\begin{pmatrix} 5 & 0 & 0 \\ 0 & 4 & 3 \\ 0 & -3 & 4 \end{pmatrix}$$

are both in $\mathcal{M}_5$ (they are easily seen to be in $\mathrm{SO}_3(\mathbf{Q})$ and to have denominator 5). However, $A \in \mathcal{A}_5$ whereas $D \notin \mathcal{A}_5$. Indeed, $5 \equiv -1 \bmod 3$, so when we reduce A and D modulo 3, the factor $\frac{1}{5}$ becomes -1. Hence

$$A \equiv -\begin{pmatrix} 5 & 0 & 0 \\ 0 & -4 & 3 \\ 0 & -3 & -4 \end{pmatrix} \equiv -\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \equiv I_3 \bmod 3$$

whereas

$$D \equiv -\begin{pmatrix} 5 & 0 & 0 \\ 0 & 4 & 3 \\ 0 & -3 & 4 \end{pmatrix} \equiv -\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \not\equiv I_3 \bmod 3$$

In fact, it is not hard to find the list of all the elements of $\mathcal{A}_5$: they are matrices of denominator 5, so we look for matrices of the form

$$\frac{1}{5}\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

where the entries $a_{i,j}$ are all integers. Moreover, we look for elements that are in $\mathrm{SO}_3(\mathbf{Q})$, so each column must be of norm 1, so if we take into account that we factored by $\frac{1}{5}$, this means that for all $1 \leqslant j \leqslant 3$,

$$a_{1,j}^2 + a_{2,j}^2 + a_{3,j}^2 = 25$$

But this does not have many solutions in integers ! Up to permutation, we are either in the case $0^2 + 0^2 + (\pm 5)^2 = 25$ or in the case $0^2 + (\pm 3)^2 + (\pm 4)^2 = 25$. Moreover, we cannot have all the columns with only one non-zero coefficient equal to ± 5 because in this case the matrix obtained is in $\mathrm{SO}_3(\mathbf{Z})$, and we excluded these from the definition of matrices with denominator 5. Taking into account the orthogonality conditions between the columns, and the condition modulo 3, we end up with

$$\mathcal{A}_5 = \left\{A, B, C, A^{-1}, B^{-1}, C^{-1}\right\}$$

where $A = \frac{1}{5}\begin{pmatrix} 5 & 0 & 0 \\ 0 & -4 & 3 \\ 0 & -3 & -4 \end{pmatrix}$, $B = \frac{1}{5}\begin{pmatrix} -4 & 0 & 3 \\ 0 & 5 & 0 \\ -3 & 0 & -4 \end{pmatrix}$ and $C = \frac{1}{5}\begin{pmatrix} -4 & -3 & 0 \\ 3 & -4 & 0 \\ 0 & 0 & 5 \end{pmatrix}$.

Note that $\mathcal{A}_p$ is symmetric : if $A \in \mathcal{A}_p$ then $A^{-1} = {}^tA \in \mathcal{A}_p$.

Lemma 5.1.6. *$\mathcal{A}_p$ is a set of representatives for $\widetilde{\mathcal{M}_p}$.*

Proof. As we already mentioned, $\frac{1}{p}$ makes sense modulo 3 since p is a prime number strictly larger than 3. Therefore, we are allowed to consider the reductions modulo 3 of the elements of $\mathcal{M}_p$ (because they are matrices of denominator p). Given a matrix $\gamma \in \mathcal{M}_p$, we denote by $\overline{\gamma}$ its reduction modulo 3.

Since $\gamma \in \mathrm{SO}_3(\mathbf{Q})$, it is easy to prove that $\overline{\gamma} \in \mathrm{SO}_3(\mathbf{F}_3)$: the group of isometries with determinant 1 of the quadratic space $(\mathbf{F}_3^3, q)$ where q denotes the "sum of three squares" quadratic form :

$$\begin{array}{rccc} q & : & \mathbf{F}_3^3 & \to & \mathbf{F}_3 \\ & & \begin{pmatrix} \overline{x} \\ \overline{y} \\ \overline{z} \end{pmatrix} & \mapsto & \overline{x}^2 + \overline{y}^2 + \overline{z}^2 \end{array}$$

The multiplication on the right by $\overline{\gamma}$ is a bijection of $\mathrm{SO}_3(\mathbf{F}_3)$, so there exists a unique matrix M (depending on $\overline{\gamma}$) such that $M\overline{\gamma} = I_3$ (the identity element of $\mathrm{SO}_3(\mathbf{F}_3)$).
Now, we remark that the reduction modulo 3

$$\mathrm{SO}_3(\mathbf{Z}) \to \mathrm{SO}_3(\mathbf{F}_3)$$

is an isomorphism, because the matrices of $\mathrm{SO}_3(\mathbf{Z})$ have coefficients in $\{0, 1, -1\}$. Therefore, the unique M that we found before corresponds to a unique element of $\mathrm{SO}_3(\mathbf{Z})$, that we still denote by M (it is exactly the same matrix, except that we do not think of the coefficients $-1, 0$ and 1 as elements of $\mathbf{Z}/3\mathbf{Z}$ but as elements of $\mathbf{Z}$). Then $M\gamma \in \mathrm{SO}_3(\mathbf{Z})\gamma$ and reduces to the identity modulo 3 : it belongs to $\mathcal{A}_p$. This proves that for all $\gamma \in \mathcal{M}_p$, there exists a unique element of $\mathcal{A}_p$ in the orbit $\mathrm{SO}_3(\mathbf{Z})\gamma$. Hence $\mathcal{A}_p$ is a set of representatives for $\widetilde{\mathcal{M}_p}$. □

It is in terms of these matrices that we are going to define trajectories on $\mathscr{R}_3(d)$.

5.2 Definition of the trajectories on $\mathscr{R}_3(d)$

Given a point $\mathbf{x} \in \mathscr{R}_3(d)$, we are going to define in two different ways a *trajectory* on $\mathscr{R}_3(d)$ attached to $\mathbf{x}$. The first definition relies on a proposition of [EMV10] that we were not able to prove completely. However, this first approach gives rise to trajectories which are *non-backtracking* by definition, and this property is needed in the proof of our main theorem. On the other hand, we will give another way to define trajectories, which relies more explicitly on the "action" of $[\mathfrak{p}]^{\mathbf{Z}}$ on $\mathscr{R}_3(d)$. These two definitions coincide, but this fact seems very difficult to prove without going through the "adelization" part of the article we are studying. Understanding this point will be our aim in the following weeks or months.

§5.2.1 A first definition

The following proposition will allow us to define trajectories in a very elementary way. Indeed, one only needs to know the definition of the matrices in $\mathcal{A}_p$ (see definition 5.1.5), so if we take the statement as a blackbox, it really seems like a magical set of rotation matrices, which happen to have nice properties with respect to the integer points on the sphere.

Proposition 5.2.1 ([EMV10], proposition 2.5)**.** *Suppose that $p > 3$ is a prime number which is split in $\mathbf{Q}(\sqrt{-d})$. Then for all $\mathbf{x} \in \mathscr{R}_3(d)$, there are exactly two matrices $w \in \mathcal{A}_p$ such that $w\mathbf{x} \in \mathscr{R}_3(d)$.*

In the next paragraph on the alternative definition of the trajectories, we prove that for all $\mathbf{x} \in \mathcal{A}_p$, there are *at least* two matrices as in this proposition. But we were not able to prove that there are *at most* two.

Now, let $\mathbf{x} \in \mathscr{R}_3(d)$. Thanks to this proposition, there are exactly two matrices in $\mathcal{A}_p$, say w_0, w_1, such that $w_1\mathbf{x} \in \mathscr{R}_3(d)$ and $w_0^{-1}\mathbf{x} \in \mathscr{R}_3(d)$. We define

$$\mathbf{x}_1 := w_1\mathbf{x} \text{ and } \mathbf{x}_{-1} := w_0^{-1}\mathbf{x}$$

Then starting from $\mathbf{x}_1$, the same proposition tells us that there are two matrices mapping $\mathbf{x}_1$ to a point which is still in $\mathscr{R}_3(d)$. But we already know that w_1^{-1} is one of these two matrices, since $w_1^{-1}\mathbf{x}_1 = \mathbf{x}$. So we denote by w_2 the other one, and define

$$\mathbf{x}_2 := w_2\mathbf{x}_1$$

In other words, we take the unique matrix in $\mathcal{A}_p$ which maps $\mathbf{x}_1$ to an integer point and which does not make us backtrack.

In this way, we can apply proposition 5.2.1 at each step, and define a sequence of integer points $(\mathbf{x}_i)_{i\in\mathbf{Z}}$. This sequence can be represented by the starting point $\mathbf{x} =: \mathbf{x}_0$, and a sequence $(w_i)_{i\in\mathbf{Z}}$ of matrices in $\mathcal{A}_p$ such that $w_{i+1} \neq w_i^{-1}$. The i-th point of the trajectory is defined inductively by the rule

$$\mathbf{x}_{i+1} = w_{i+1}\mathbf{x}_i$$

Since $(w_i)_{i\in\mathbf{Z}}$ satisfies the property $w_{i+1} \neq w_i^{-1}$, we say that it is a reduced word in the alphabet $\mathcal{A}_p$. In terms of the trajectory, this means that it is not backtracking. Let us stress that with this definition of the trajectories, the fact that we obtain non-backtracking trajectories is immediate, it just comes from the way we choose the element of $\mathcal{A}_p$ to define the next point.

§5.2.2 A second way to define trajectories

Let $\mathbf{x} = (x, y, z) \in \mathscr{R}_3(d)$. As before, we identify $\mathbf{x}$ with the quaternion $xi + yj + zk \in \mathrm{B}^{(0)}(\mathbf{Z})$. We know from proposition 5.1.1 that there exists a unique class $[\alpha] \in \widetilde{\mathcal{H}_p}$ such that $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})\tilde{\alpha}$ for any $\tilde{\alpha}$ in $[\alpha]$. Under the bijection of proposition 5.1.4, this class $[\alpha]$ corresponds to a unique class $[M] \in \widetilde{\mathcal{M}_p}$. Since $\mathcal{A}_p$ is a set of representatives for $\widetilde{\mathcal{M}_p}$ by lemma 5.1.6, the class $[M]$ is represented by a unique matrix in $\mathcal{A}_p$, say $w_{\mathbf{x},1}$. Then we define $\mathbf{x}_1$ as $w_{\mathbf{x},1}\mathbf{x}$.

Since $w_{\mathbf{x},1}$ is in the same $\mathrm{SO}_3(\mathbf{Z})$-orbit as γ_α, our new point $\mathbf{x}_1$ is in the same $\mathrm{SO}_3(\mathbf{Z})$-orbit as $\gamma_\alpha(\mathbf{x})$. But because α is such that $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})\alpha$, we know from section 4.2 (more precisely : the argument is given at equation (13)) that $\gamma_\alpha(\mathbf{x}) \in \mathscr{R}_3(d)$. Thus, $\mathbf{x}_1 \in \mathscr{R}_3(d)$.

This is great because at first sight it is not obvious that we can find a matrix $w \in \mathcal{A}_p$ such that $w\mathbf{x} \in \mathscr{R}_3(d)$. Indeed, the elements of $\mathcal{A}_p$ are in $\mathrm{SO}_3(\mathbf{Q})$, so we know that $w\mathbf{x}$ will still be on the sphere of radius $\sqrt{d}$, but the fact that the coordinates will remain integers for at least one w did not seem clear to me without this interpretation in terms of quaternions.

Besides, recall that we defined (in a neighbourhood of proposition 4.2.2) $[\mathfrak{p}].[\mathbf{x}]$ as $[\gamma_\alpha(\mathbf{x})]$ (here the brackets around $\mathbf{x}$ and $\gamma_\alpha(\mathbf{x})$ denote $\mathrm{SO}_3(\mathbf{Z})^+$-orbits, i.e. elements of $\widetilde{\mathscr{R}_3(d)^+}$). Thus, $\mathbf{x}_1$ is in the same $\mathrm{SO}_3(\mathbf{Z})$-orbit as (any element of) $[\mathfrak{p}].[\mathbf{x}]$. We think of it as the point obtained from $\mathbf{x}$ after the "action" of $[\mathfrak{p}]$.

Similarly, starting from $\mathbf{x}_1$, we look for $\beta \in \mathcal{H}_p$ such that $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}_1}(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})\beta$, then we define $w_{\mathbf{x},2}$ as the unique element of $\mathcal{A}_p$ which is in the same $\mathrm{SO}_3(\mathbf{Z})$-orbit as γ_β, and set $\mathbf{x}_2 := w_{\mathbf{x},2}\mathbf{x}_1$. We can continue this process to define a sequence $(\mathbf{x}_i)_{i\geqslant 0}$ of integer points on the sphere of radius $\sqrt{d}$ (where $\mathbf{x}_0 = \mathbf{x}$ is our starting point).

But we can also go in the other direction, that is : instead of looking at a lift of the action of $[\mathfrak{p}]$ at each step, we can look at the effect of a lift of the action of $[\mathfrak{p}'] = [\mathfrak{p}]^{-1}$. So, starting from $\mathbf{x}$, we look for $\alpha' \in \mathcal{H}_p$ such that $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}') = \mathrm{B}(\mathbf{Z})\alpha'$, and then denote by $w_{\mathbf{x},0}^{-1}$ the unique matrix in $\mathcal{A}_p$ which is in the $\mathrm{SO}_3(\mathbf{Z})$-orbit of $\gamma_{\alpha'}$. Then we define $\mathbf{x}_{-1}$ as $w_{\mathbf{x},0}^{-1}\mathbf{x}$. For the same reasons as we evoqued for the definition of $\mathbf{x}_1$, this point $\mathbf{x}_{-1}$ is also in $\mathscr{R}_3(d)$. Note that $w_{\mathbf{x},0}^{-1} \neq w_{\mathbf{x},1}$ because $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}) \neq \mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}')$ (this follows from lemma 4.3.1 and the fact that $\mathfrak{p} \neq \mathfrak{p}'$). Indeed, since the left $\mathrm{B}(\mathbf{Z})$ ideals are not equal, their generators are in two different classes of $\widetilde{\mathcal{H}_p}$, so they correspond to two different classes in $\widetilde{\mathcal{M}_p}$: this implies that they are represented by distinct elements of $\mathcal{A}_p$.

Then we can go on, look for $\beta' \in \mathcal{H}_p$ such that $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}_{-1}}(\mathfrak{p}') = \mathrm{B}(\mathbf{Z})\beta'$, then find $w_{\mathbf{x},-1}^{-1} \in \mathcal{A}_p$ (unique) such that $\gamma_{\beta'}$ is $\mathrm{SO}_3(\mathbf{Z})$-equivalent to $w_{\mathbf{x},-1}^{-1}$, and define $\mathbf{x}_{-2} \in \mathscr{R}_3(d)$ as $w_{\mathbf{x},-1}^{-1}\mathbf{x}_{-1}$, and so on ...

Note that we proved a part of proposition 5.2.1 :

Proposition 5.2.2. *For all $\mathbf{x} \in \mathscr{R}_3(d)$, there are at least two matrices $w \in \mathcal{A}_p$ such that $w\mathbf{x} \in \mathscr{R}_3(d)$.*

Proof. When defining the trajectory $(\mathbf{x}_i)_{i\in\mathbf{Z}}$ in the paragraph above, we proved that the matrices $w_{\mathbf{x},1}$ and $w_{\mathbf{x},0}^{-1}$ are distinct and satisfy the property. □

Remark. *For $i \geqslant 0$, $\mathbf{x}_{i+1}$ is obtained from $\mathbf{x}_i$ via the "action" of $[\mathfrak{p}]$ (because we consider $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}_i}(\mathfrak{p})$ to define it), and $\mathbf{x}_{-(i+1)}$ is defined from $\mathbf{x}_{-i}$ via the "action" of $[\mathfrak{p}']$. However, it does not seem so clear that this defines a real group action of $[\mathfrak{p}]^{\mathbf{Z}}$ on $\mathscr{R}_3(d)$. For instance, we should have $[\mathfrak{p}'].[\mathfrak{p}].\mathbf{x} = \mathbf{x}$, but the way we defined the actions of $[\mathfrak{p}]$ and $[\mathfrak{p}']$ on the points of $\mathscr{R}_3(d)$ does not seem to allow us to prove this easily.*

Another issue that we have at the moment is that with this definition, it does not seem obvious at all that the trajectories are non-backtracking. Here, we present an attempt to prove this fact, but we could not conclude. In this attempt, we see that this question is in fact related to the remark above. We hope that leaving this attempt in this thesis will clarify why there is something not obvious to prove to see that we really defined an action of $[\mathfrak{p}]^{\mathbf{Z}}$.

Proposition 5.2.3 (The trajectories are non-backtracking)**.** *For all $i \in \mathbf{Z}$,*

$$w_{\mathbf{x},i+1} \neq w_{\mathbf{x},i}^{-1}$$

Attempt. We already proved it for $i = 0$, but the the way we defined the trajectory does not allow us to repeat exactly the same argument for other values of i. Indeed, for $i = 0$, we defined $w_{\mathbf{x},1}$ and $w_{\mathbf{x},0}^{-1}$ using the actions of $[\mathfrak{p}]$ and $[\mathfrak{p}']$ on the point $\mathbf{x}$, so the fact that they are distinct essentially came from the fact that $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}) \neq \mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}')$. Now, the issue we have when considering $i \neq 0$, for instance $i > 0$, is that $\mathbf{x}_{i-1}$ is not a priori defined from $\mathbf{x}_i$ via the action of $[\mathfrak{p}']$: it is $\mathbf{x}_i$ which is defined from $\mathbf{x}_{i-1}$ via the action of $[\mathfrak{p}]$. It is not clear that $[\mathfrak{p}']$ acts on $\mathbf{x}_i$ via the inverse of the matrix of $\mathcal{A}_p$ corresponding to the action of $[\mathfrak{p}]$ on $\mathbf{x}_{i-1}$. More explicitly :

- We construct $\mathbf{x}_i$ starting from $\mathbf{x}_{i-1}$ by considering the left ideal $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}_{i-1}}(\mathfrak{p})$, writing it in the form $\mathrm{B}(\mathbf{Z})\gamma_{\alpha_i}$ for some Hurwitz quaternion α_i of norm p, and then we denote by $w_{\mathbf{x},i}$ the unique matrix in $\mathcal{A}_p$ which is left $\mathrm{SO}_3(\mathbf{Z})$-equivalent to γ_{α_i}. The point $\mathbf{x}_i$ is then defined as $w_{\mathbf{x},i}\mathbf{x}_{i-1}$.
- On the other hand, if we want to define the point obtained from $\mathbf{x}_i$ via the action of $[\mathfrak{p}']$, we follow the same steps : write $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}_i}(\mathfrak{p}') = \mathrm{B}(\mathbf{Z})\gamma_{\alpha_i'}$, and $(w'_{\mathbf{x},i})^{-1}$ the unique element of $\mathcal{A}_p$ which is left $\mathrm{SO}_3(\mathbf{Z})$-equivalent to $\gamma_{\alpha_i'}$. We obtain a new point

  $$\mathbf{x}'_{i-1} := (w'_{\mathbf{x},i})^{-1}\mathbf{x}_i$$

  which belongs to $\mathscr{R}_3(d)$.

At this point, we would like to prove that $w'_{\mathbf{x},i} = w_{\mathbf{x},i}$, but for the moment, we have not found an elementary argument. However, as we will discuss in the next paragraph, our two definitions of trajectories coincide, and with the first definition, there is nothing to prove, the trajectories are non-backtracking by definition. □

Admitting this proposition, this means that we can represent the trajectory $(\mathbf{x}_i)_{i\in\mathbf{Z}}$ as follows : it is the data of a starting point $\mathbf{x} = \mathbf{x}_0$, and a word $W_{\mathbf{x}} = (w_{\mathbf{x},i})_{i\in\mathbf{Z}}$ in the alphabet $\mathcal{A}_p$, satisfying :

$$w_{\mathbf{x},i}\mathbf{x}_{i-1} = \mathbf{x}_i \text{ and } w_{\mathbf{x},i+1} \neq w_{\mathbf{x},i}^{-1}$$

Definition 5.2.4. *A word $(w_i)_{i\in\mathbf{Z}}$ in the alphabet $\mathcal{A}_p$ satisfying the property $w_{i+1} \neq w_i^{-1}$ is said to be reduced.*

Example : Let us take $d := 29$, and $K = \mathbf{Q}(\sqrt{-d})$. The integer d is admissible and square-free. This follows from theorem 3.4.2, but since 29 is not very large, we can just try a little bit to find several ways

of writing it as a sum of three squares. For instance we have $29 = 5^2 + 2^2 + 0^2$, or $29 = 4^2 + 3^2 + 2^2$. The two prime ideals above 5 in $\mathcal{O}_K$ are

$$\mathfrak{p} := \langle 5, 1 + \sqrt{-d} \rangle \text{ and } \mathfrak{p}' = \langle 5, 1 - \sqrt{-d} \rangle$$

(where the brackets mean that we are taking the ideal of $\mathcal{O}_K$ generated by the two elements inside the brackets). Now, let us start from some $\mathbf{x}_0 \in \mathscr{R}_3(d)$, for instance

$$\mathbf{x}_0 := \begin{pmatrix} 5 \\ 2 \\ 0 \end{pmatrix}$$

To define $\mathbf{x}_1$, we first need to find $\alpha \in \mathrm{B}(\mathbf{Z})$ such that $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}_0}(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})\alpha$. But

$$\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}_0}(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})5 + \mathrm{B}(\mathbf{Z})(1 + \mathbf{x}_0),$$

hence such a quaternion α must be a right divisor (inside $\mathrm{B}(\mathbf{Z})$) of both 5 and $1 + \mathbf{x}_0$. Besides, we know that we can look for α in the list

$$L := \{1 \pm 2i, 1 \pm 2j, 1 \pm 2j\}$$

as the latter is a set of representatives for Hurwitz quaternions of norm 5, modulo the action of units. For all $z \in L$, z is a right divisor of $1 + \mathbf{x}_0$ inside $\mathrm{B}(\mathbf{Z})$ if and only if $(1 + \mathbf{x}_0)z^{-1} \in \mathrm{B}(\mathbf{Z})$. So we just have to compute $(1 + \mathbf{x}_0)z^{-1}$ for all $z \in L$, and see which one still belongs to $\mathrm{B}(\mathbf{Z})$. After a few attemps, we obtain :

$$\begin{aligned}(1 + \mathbf{x}_0)(1 - 2j) &= (1 + 5i + 2j)(1 - 2j) \\ &= 1 + 5i + 2j - 2j - 10ij - 4j^2 \\ &= 1 + 5i - 10k + 4 \\ &= 5 + 5i - 10k\end{aligned}$$

hence

$$(1 + \mathbf{x}_0)(1 + 2j)^{-1} = (1 + \mathbf{x}_0)\left(\frac{1 - 2j}{5}\right) \in \mathrm{B}(\mathbf{Z}).$$

Thus, $\alpha := 1 + 2j$ satisfies $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}_0}(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})\alpha$. Now, let us see which element of $\mathcal{A}_5$ is in the same $\mathrm{SO}_3(\mathbf{Z})$-orbit as γ_α. We have

$$\gamma_\alpha = \frac{1}{5}\begin{pmatrix} -3 & 0 & 4 \\ 0 & 5 & 0 \\ -4 & 0 & -3 \end{pmatrix}$$

let us mention that there is a possibility to use WolframAlpha to find the rotation corresponding to a given quaternion :
https://www.wolframalpha.com/input/?i=draw+1+%2B0i+%2B2j+%2B0k+as+a+rotation+operator

This matrix γ_α is easily seen to be in the same $\mathrm{SO}_3(\mathbf{Z})$-orbit as the matrix $B^{-1} \in \mathcal{A}_5$. Indeed,

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}\begin{pmatrix} -3 & 0 & 4 \\ 0 & 5 & 0 \\ -4 & 0 & -3 \end{pmatrix} = \begin{pmatrix} -4 & 0 & -3 \\ 0 & 5 & 0 \\ 3 & 0 & -4 \end{pmatrix}$$

Then we define

$$\mathbf{x}_1 := B^{-1}\mathbf{x}_0 = \frac{1}{5}\begin{pmatrix} -4 & 0 & -3 \\ 0 & 5 & 0 \\ 3 & 0 & -4 \end{pmatrix}\begin{pmatrix} 5 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} -4 \\ 2 \\ 3 \end{pmatrix}$$

Similarly, one can check that $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}_1}(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})(1-2k)$, and that γ_{1-2k} is $\mathrm{SO}_3(\mathbf{Z})$-equivalent to the matrix $C \in \mathcal{A}_5$. Hence :

$$\mathbf{x}_2 := C\mathbf{x}_1 = \frac{1}{5}\begin{pmatrix} -4 & -3 & 0 \\ 3 & -4 & 0 \\ 0 & 0 & 5 \end{pmatrix}\begin{pmatrix} -4 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ -4 \\ 3 \end{pmatrix}$$

Similarly, in the other direction, we have $\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}') = \mathrm{B}(\mathbf{Z})(1-2j)$ and γ_{1-2j} is in the same $\mathrm{SO}_3(\mathbf{Z})$-orbit as $B \in \mathcal{A}_5$. Thus, we define

$$\mathbf{x}_{-1} := B\mathbf{x} = \frac{1}{5}\begin{pmatrix} -4 & 0 & 3 \\ 0 & 5 & 0 \\ -3 & 0 & -4 \end{pmatrix}\begin{pmatrix} 5 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} -4 \\ 2 \\ -3 \end{pmatrix}$$

This way, we obtain the following truncated trajectory :

$$\cdots \underset{\mathbf{x}_{-3}}{\begin{pmatrix} 2 \\ 5 \\ 0 \end{pmatrix}} \overset{A}{\longmapsto} \underset{\mathbf{x}_{-2}}{\begin{pmatrix} 2 \\ -4 \\ -3 \end{pmatrix}} \overset{C^{-1}}{\longmapsto} \underset{\mathbf{x}_{-1}}{\begin{pmatrix} -4 \\ 2 \\ -3 \end{pmatrix}} \overset{B^{-1}}{\longmapsto} \underset{\mathbf{x}_0}{\begin{pmatrix} 5 \\ 2 \\ 0 \end{pmatrix}} \overset{B^{-1}}{\longmapsto} \underset{\mathbf{x}_1}{\begin{pmatrix} -4 \\ 2 \\ 3 \end{pmatrix}} \overset{C}{\longmapsto} \underset{\mathbf{x}_2}{\begin{pmatrix} 2 \\ -4 \\ 3 \end{pmatrix}} \overset{A}{\longmapsto} \underset{\mathbf{x}_3}{\begin{pmatrix} 2 \\ 5 \\ 0 \end{pmatrix}} \cdots$$

Remark. *We will see that the properties of these trajectories lead to a proof of an equidistribution result. But one can also find another interest to the process described above : finding new representations as a sum of three squares. Indeed, when $d = 29$, it is not difficult to find all the possible representations, but if d is very large, it can be very long. However, the matrices of $\mathcal{A}_p$ can help us to find new representations starting from an initial one. For instance let us consider*

$$d := 32591826 = 5689^2 + 23^2 + 476^2$$

Let us denote by $\mathbf{x}_0 := \begin{pmatrix} 5689 \\ 23 \\ 476 \end{pmatrix} \in \mathscr{R}_3(d)$. *As $d \equiv 1 \bmod 5$, the prime 5 is split in $\mathbf{Q}(\sqrt{-d})$, so we know that there are at least two matrices in $\mathcal{A}_5$, say w and w', such that $w\mathbf{x}_0 \in \mathscr{R}_3(d)$ and $w'\mathbf{x}_0 \in \mathscr{R}_3(d)$. Since $|\mathcal{A}_5| = 6$, we just have to do six products of a (3×3)-matrix by a column vector, so it is really economic. We find that*

$$A^{-1}\mathbf{x}_0 = \begin{pmatrix} 5689 \\ -304 \\ 367 \end{pmatrix} \text{ and } C\mathbf{x}_0 = \begin{pmatrix} -4565 \\ 3395 \\ 476 \end{pmatrix}$$

hence two new representations of d as a sum of three squares :

$$d = 5689^2 + (-304)^2 + 367^2 \text{ and } d = (-4565)^2 + 3395^2 + 476^2$$

In fact, in the article [EMV10], they prove that exactly two elements $w \in \mathcal{A}_5$ are such that $w\mathbf{x}_0 \in \mathscr{R}_3(d)$. What we proved here just explains that there are at least two, corresponding to the actions of $[\mathfrak{p}]$ and $[\mathfrak{p}']$ (the elements of $\mathrm{Cl}(\mathcal{O}_K)$ corresponding to the two prime ideals above 5), and this is sufficient for us. If $d \not\equiv \pm 1 \bmod 5$, we can replace the prime 5 by another prime p which is split in $\mathbf{Q}(\sqrt{-d})$, and work with $\mathcal{A}_p$ instead of $\mathcal{A}_5$.

This remark raises an interesting question : can we use these trajectories to find all the representations of d as a sum of three squares ? In other words, will the trajectory reach all the $\mathrm{SO}_3(\mathbf{Z})$-orbits of $\mathscr{R}_3(d)$? This would be great because, as we said, this would be a very efficient way to find representations as a sum of three squares, since at each step, we just have to do six matrix multiplications, and we know that two of them will give us a possibly different representation. This question is related to the question : is the subgroup $[\mathfrak{p}]^{\mathbf{Z}}$ all or almost all of the group $\mathrm{Cl}(\mathcal{O}_K)$? This is a "seemingly difficult question" according to [EMV10], but apparently, people believe that this happens for infinitely many d. So let us just say that it is reasonable to hope that our trajectories will reach all the $\mathrm{SO}_3(\mathbf{Z})$-orbits of $\mathscr{R}_3(d)$.

§5.2.3 The two definitions of the trajectories coincide

As we will need to combine the properties of our two definitions of the trajectories, we admit the following fact :

It can be shown that the two previous definitions of the trajectories on $\mathscr{R}_3(d)$ coincide. In particular, the "action" of $[\mathfrak{p}]^{\mathbf{Z}}$ on $\mathscr{R}_3(d)$ as defined in the previous paragraph is a real group action, and the trajectory defined with this point of view is non-backtracking.

This highly non-trivial statement comes from the fact that a finite version of the graph $\mathscr{R}_3(d)$ can be identified with a finite quotient of the Bruhat-Tits tree of $\mathrm{PGL}_2(\mathbf{Q}_p)$ (an explicit $(p+1)$-valent tree).

5.3 The graph structure on $\mathscr{R}_3(d,q)$

Let $p>3$ be a prime number, et q be an integer coprime with $6p$ (this condition is used in theorem 5.6.1, but will remain a bit obscure because we do not prove this theorem). Then in particular, q is coprime with p, so p is invertible modulo q. Thus, we can reduce the elements of $\mathcal{A}_p$ modulo q, since they are matrices of denominator p. Let us denote by $\overline{\gamma}$ these reductions modulo q. It is easy to see that since $\mathcal{A}_p \subseteq \mathrm{SO}_3(\mathbf{Q})$, they act on $\mathscr{R}_3(d,q)$: for all $\overline{\mathbf{x}} \in \mathscr{R}_3(d,q)$, for all $\gamma \in \mathcal{A}_p$, $\overline{\gamma}\ \overline{\mathbf{x}} \in \mathscr{R}_3(d,q)$. This endows $\mathscr{R}_3(d,q)$ with a structure of a $|\mathcal{A}_p|$-regular undirected graph by joining each vertex $\overline{\mathbf{x}} \in \mathscr{R}_3(d,q)$ to the vertices $\overline{\gamma}\ \overline{\mathbf{x}}$, $\gamma \in \mathcal{A}_p$. In fact, it is a *multigraph* : we allow multiple edges between two vertices and edges connecting a vertex to itself. Indeed, there might exist two matrices $\gamma_1, \gamma_2 \in \mathcal{A}_p$ such that $\overline{\gamma}_1\ \overline{\mathbf{x}} = \overline{\gamma}_2\ \overline{\mathbf{x}} =: \overline{\mathbf{y}}$. In this case, we will draw one edge corresponding to γ_1, and one different edge, corresponding to γ_2, to connect $\overline{\mathbf{x}}$ and $\overline{\mathbf{y}}$. By an abuse of notation, we will also denote by $\mathscr{R}_3(d,q)$ this graph. Since $|\mathcal{A}_p|$ is the degree of this graph (that is : the number of edges meeting at each vertex), it is crucial to know this cardinality in order to have a better understanding of this graph.

Proposition 5.3.1. *We have* $|\mathcal{A}_p| = p+1$.

Proof. David E Speyer's answer on mathoverflow : https://mathoverflow.net/questions/84897/proofs-of-jacobis-four-square-theorem, and Claude Quitté's answer on Les-Mathématiques.net : http://www.les-mathematiques.net/phorum/read.php?5,1821586 helped me a lot.

As $\mathcal{A}_p$ is a set of representatives for $\widetilde{\mathcal{M}_p}$ and $|\widetilde{\mathcal{M}_p}| = |\widetilde{\mathcal{H}_p}|$ by proposition 5.1.4, we have $|\mathcal{A}_p| = |\widetilde{\mathcal{H}_p}|$. Moreover, any orbit $[z] \in \widetilde{\mathcal{H}_p}$ is made of 24 elements of $\mathcal{H}_p$ because $|\mathrm{B}(\mathbf{Z})^\times| = 24$. Thus,

$$\mathcal{H}_p = 24|\widetilde{\mathcal{H}_p}|.$$

So $|\mathcal{A}_p| = p+1$ if and only if $|\mathcal{H}_p| = 24(p+1)$. This reduces the question to counting the Hurwitz quaternions of norm p.

- *Step 1 : for any* $x \in \mathrm{B}(\mathbf{Z})$*, the index of the principal ideal* $x\mathrm{B}(\mathbf{Z})$ *inside* $\mathrm{B}(\mathbf{Z})$ *equals* $\mathrm{N}(x)^2$.

  $\mathrm{B}(\mathbf{Z})$ is a free $\mathbf{Z}$-module of rank 4, with basis $\mathcal{B} := (i,j,k,\delta)$ (for example), where δ denotes $\frac{1}{2}(1+i+j+k)$. Therefore, we can repeat the arguments of the proof of proposition 1.6.5, and conclude that the index of $x\mathrm{B}(\mathbf{Z})$ inside $\mathrm{B}(\mathbf{Z})$ is equal to the absolute value of the determinant of the multiplication by x (as a $\mathbf{Z}$-linear map from $\mathrm{B}(\mathbf{Z})$ to itself). Now, if $x = a+bi+cj+dk$, one can check that :

$$\begin{aligned}
xi &= (a+b)i + (b+d)j + (b-c)k - 2b\delta \\
xj &= (c-d)i + (a+c)j + (b+c)k - 2c\delta \\
xk &= (c+d)i + (d-b)j + (a+d)k - 2d\delta \\
x\delta &= (b+c)i + (c+d)j + (b+d)k + (a-b-c-d)\delta
\end{aligned}$$

  So the matrix of the multiplication by x in the basis $\mathcal{B}$ of $\mathrm{B}(\mathbf{Z})$ is the following :

$$\mathrm{Mat}_{\mathcal{B},\mathcal{B}}(m_x) = \begin{pmatrix} a+b & c-d & c+d & b+c \\ b+d & a+c & d-b & c+d \\ b-c & b+c & a+d & b+d \\ -2b & -2c & -2d & a-b-c-d \end{pmatrix}$$

The determinant of this matrix is $(a^2+b^2+c^2+d^2)^2$, that is : $\mathrm{N}(x)^2$. In fact, the computation is easier if we proceed as follows : $\mathcal{B}$ is a $\mathbf{Z}$-basis of $\mathrm{B}(\mathbf{Z})$, but it is also a $\mathbf{Q}$-basis of $\mathrm{B}(\mathbf{Q})$, so we can see $\mathrm{Mat}_{\mathcal{B},\mathcal{B}}(m_x)$ as the matrix of the multiplication by x (on the left) as an endomorphism of $\mathrm{B}(\mathbf{Q})$. Thus, the determinant of this matrix is the same as the determinant of $\mathrm{Mat}_{\mathcal{C},\mathcal{C}}(m_x)$ where $\mathcal{C} = (1, i, j, k)$ is the usual basis of $\mathrm{B}(\mathbf{Q})$.

Thanks to this first step, we deduce that if $z \in \mathcal{H}_p$, then the index of $z\mathrm{B}(\mathbf{Z})$ inside $\mathrm{B}(\mathbf{Z})$ is equal to p^2. But conversely, if I is a right ideal of $\mathrm{B}(\mathbf{Z})$ of index p^2, then by corollary 3.1.5 it is of the form $z\mathrm{B}(\mathbf{Z})$ for some $z \in \mathrm{B}(\mathbf{Z})$, and the latter must have norm p in order to have the correct index. Therefore, the map $z \mapsto z\mathrm{B}(\mathbf{Z})$, from $\mathcal{H}_p$ to the set of right ideals of $\mathrm{B}(\mathbf{Z})$ of index p^2, is well defined and surjective. Besides, for a given right ideal $z\mathrm{B}(\mathbf{Z})$, there are exactly 24 elements of $\mathcal{H}_p$ mapping to this ideal (they are exactly the elements $z\varepsilon$ where ε runs over $\mathrm{B}(\mathbf{Z})^\times$). Hence $|\mathcal{H}_p|$ equals 24 times the number of right ideals of $\mathrm{B}(\mathbf{Z})$ of index p^2. So $|\mathcal{A}_p| = p+1$ if and only if there are exactly $p+1$ such ideals.

- *Step 2 : we reduce to the question of counting ideals in* $\mathrm{B}(\mathbf{Z})/p\mathrm{B}(\mathbf{Z})$.

  If $z \in \mathcal{H}_p$, then $\mathrm{N}(z) = z\overline{z} = p \in z\mathrm{B}(\mathbf{Z})$, so $p\mathrm{B}(\mathbf{Z}) \subseteq z\mathrm{B}(\mathbf{Z})$. Hence all the right ideals of $\mathrm{B}(\mathbf{Z})$ of index p^2 contain $p\mathrm{B}(\mathbf{Z})$. It is well known that the natural surjection map $\pi\colon \mathrm{B}(\mathbf{Z}) \to \mathrm{B}(\mathbf{Z})/p\mathrm{B}(\mathbf{Z})$ induces a bijection between right ideals of $\mathrm{B}(\mathbf{Z})$ containing $p\mathrm{B}(\mathbf{Z})$ and right ideals of $\mathrm{B}(\mathbf{Z})/p\mathrm{B}(\mathbf{Z})$. Moreover, this correspondence of ideals preserves the index. Thus, the number of right ideals of $\mathrm{B}(\mathbf{Z})$ of index p^2 equals the number of right ideals of $\mathrm{B}(\mathbf{Z})/p\mathrm{B}(\mathbf{Z})$ of index p^2.

- *Step 3 :* $\mathrm{B}(\mathbf{Z})/p\mathrm{B}(\mathbf{Z}) \simeq \mathcal{M}_2(\mathbf{F}_p)$.

  By the same counting argument as in the proof of proposition 3.2.2, we can find $u, v \in \mathbf{Z}$ such that $u^2 + v^2 \equiv -1 \bmod p$. Let us define the following four elements of $\mathcal{M}_2(\mathbf{F}_p)$:

$$\mathbf{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ J := \begin{pmatrix} u & v \\ v & -u \end{pmatrix} \text{ and } K := \begin{pmatrix} v & -u \\ -u & -v \end{pmatrix}$$

  Then $I^2 = J^2 = K^2 = -\mathbf{1}$ and $IJ = -JI = K$, $JK = -KJ = I$ and $KI = -IK = J$. Thanks to these relations, we can define a ring homomorphism

$$\phi\colon \mathrm{B}(\mathbf{Z}) \to \mathcal{M}_2(\mathbf{F}_p)$$

  as follows : first, we set $\phi(1) = \mathbf{1}$, $\phi(i) = I$, $\phi(j) = J$ and $\phi(k) = K$. Then we extend it to all the elements of $\mathrm{B}(\mathbf{Z})$ by linearity : if $x = a + bi + cj + dk$ is a Hurwitz quaternion with coefficients in $\mathbf{Z}$, there is no issue, we map it to $a\mathbf{1} + bI + cJ + dK$, but how do we do if x has coefficients in $\mathbf{Z} + \frac{1}{2}$? In this case, we just remark that since p is an odd prime, 2 is invertible modulo p, so we can find $m \in \mathbf{Z}$ whose reduction modulo p is the inverse of the class of 2 mod p. Then, if $x = \frac{a}{2} + \frac{b}{2}i + \frac{c}{2}j + \frac{d}{2}k$ where a, b, c, d are odd integers, we define $\phi(x)$ as $ma\mathbf{1} + mbI + mcJ + mdK$. Note that since we are looking at matrices with coefficients in $\mathbf{F}_p$, this does not depend on the choice of the integer m satisfying $2m \equiv 1 \bmod p$.

  Let us prove that this ring homomorphism is surjective. It suffices to prove that ϕ reaches the four matrices $E_{i,j}$ of the canonical basis of $\mathcal{M}_2(\mathbf{F}_p)$. It is even sufficient to prove that ϕ reaches the matrices $2E_{i,j}$. Indeed, if $z \in \mathrm{B}(\mathbf{Z})$ is such that $\phi(z) = 2E_{i,j}$ then it suffices to take an

integer m whose reduction modulo p is the inverse of 2 (it exists), and then mz is still in $\mathrm{B}(\mathbf{Z})$ and $\phi(mz) = m\phi(z) = E_{i,j}$. Now we have the following relations :

$$\begin{cases} \mathbf{1} - uJ - vK = 2E_{1,1} \\ I - vJ + uK = 2E_{1,2} \\ -I - vJ + uK = 2E_{2,1} \\ \mathbf{1} + uJ + vK = 2E_{2,2} \end{cases}$$

hence $\phi(1 - uj - vk) = 2E_{1,1}$, $\phi(i - vj + uk) = 2E_{1,2}$ ... This proves that ϕ is surjective.

Finally, it remains to show that $\ker(\phi) = p\mathrm{B}(\mathbf{Z})$. We have that $(\mathbf{1}, I, J, K)$ is a basis of the $\mathbf{F}_p$-vector space $\mathcal{M}_2(\mathbf{F}_p)$ (because it is made of 4 elements, and generates $\mathcal{M}_2(\mathbf{F}_p)$, as we have just seen while proving the surjectivity). Therefore, $\phi(a + bi + cj + dk) = 0$ if and only if $a, b, c, d \equiv 0 \bmod p$ (with the convention that we replace $\frac{1}{2}$ by the class of m modulo p when we have a Hurwitz quaternion with coefficients in $\mathbf{Z}+\frac{1}{2}$). This is equivalent to $a+bi+cj+dk \in p\mathrm{B}(\mathbf{Z})$. Thus, ϕ induces a ring isomorphism

$$\mathrm{B}(\mathbf{Z})/p\mathrm{B}(\mathbf{Z}) \simeq \mathcal{M}_2(\mathbf{F}_p)$$

- *Step 4 : counting right ideals of $\mathcal{M}_2(\mathbf{F}_p)$.*

  By the preceding step, we are reduced to the question of counting the right ideals of index p^2 inside $\mathcal{M}_2(\mathbf{F}_p)$. By the correspondence explained in the appendix C, these ideals are in one to one correspondence with the vector subspaces of $\mathbf{F}_p$ of index p, that is : the lines in $\mathbf{F}_p$. There are $p + 1$ such lines, hence the conclusion.

□

Remark. *We proved that the number of Hurwitz quaternions of norm p (for p odd prime) is $24(p+1)$. This means that the number of solutions to the equation*

$$a^2 + b^2 + c^2 + d^2 = p$$

where a, b, c, d are either all in $\mathbf{Z}$ or all in $\mathbf{Z} + \frac{1}{2}$ is equal to $24(p + 1)$. So we are not far from proving the formula given in theorem 3.0.2 for the number of representations of p as a sum of four squares.

This proposition tells us that $\mathscr{R}_3(d, q)$ is a $(p + 1)$-regular undirected graph : each vertex $\overline{\mathbf{x}} \in \mathscr{R}_3(d, q)$ has $(p + 1)$ edges that are incident to it. We say that each vertex has valency (or degree) $p + 1$.

Example : Let us take $d = 29$, $p = 5$ and $q = 7$. Since $5 \times 3 = 15 \equiv 1 \bmod 7$, we can replace the coefficient $\frac{1}{5}$ in front of the matrices in $\mathcal{A}_5$ by a multiplication by 3 when we compute the reduction modulo 7. We obtain that the reductions modulo 7 of the matrices in $\mathcal{A}_5$ are :

$$\overline{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & -2 & 2 \end{pmatrix}, \ \overline{B} = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 1 & 0 \\ -2 & 0 & 2 \end{pmatrix} \text{ and } \overline{C} = \begin{pmatrix} 2 & -2 & 0 \\ 2 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and their transpose. The points of $\mathscr{R}_3(d, q)$ are the $(x, y, z) \in (\mathbf{Z}/q\mathbf{Z})^3$ such that :

$$x^2 + y^2 + z^2 \equiv d \equiv 29 \equiv 1 \bmod 7$$

Up to permutation of the coordinates, the points of $\mathscr{R}_3(d, q)$ are :

$$(5,2,0)\ (4,3,2)\ (1,0,0)\ (6,0,0)\ (2,2,0)\ (5,5,0)\ (3,3,2)\ (4,4,2)\ (5,3,3)\ (5,4,3)\ (5,4,4)$$

(here we identify the elements of $\mathbf{Z}/7\mathbf{Z}$ with their unique representative in $\{0, \ldots, 6\}$). With the help of a computer, we find that there are 42 points in $\mathscr{R}_3(d, q)$.

Starting from the point $\overline{\mathbf{x}} = (5, 2, 0)$, let us draw the edges joining it to other vertices of $\mathscr{R}_3(d, q)$. These are the points $\overline{\mathbf{y}} = \overline{\gamma}\ \overline{\mathbf{x}}$ for $\gamma \in \mathcal{A}_5$. On the figure below, we put arrows with the matrices that made us go from $\overline{\mathbf{x}}$ to $\overline{\mathbf{y}}$, but it is just to clarify. In the end, we forget about these arrows, and view $\mathscr{R}_3(d, q)$ as an undirected graph.

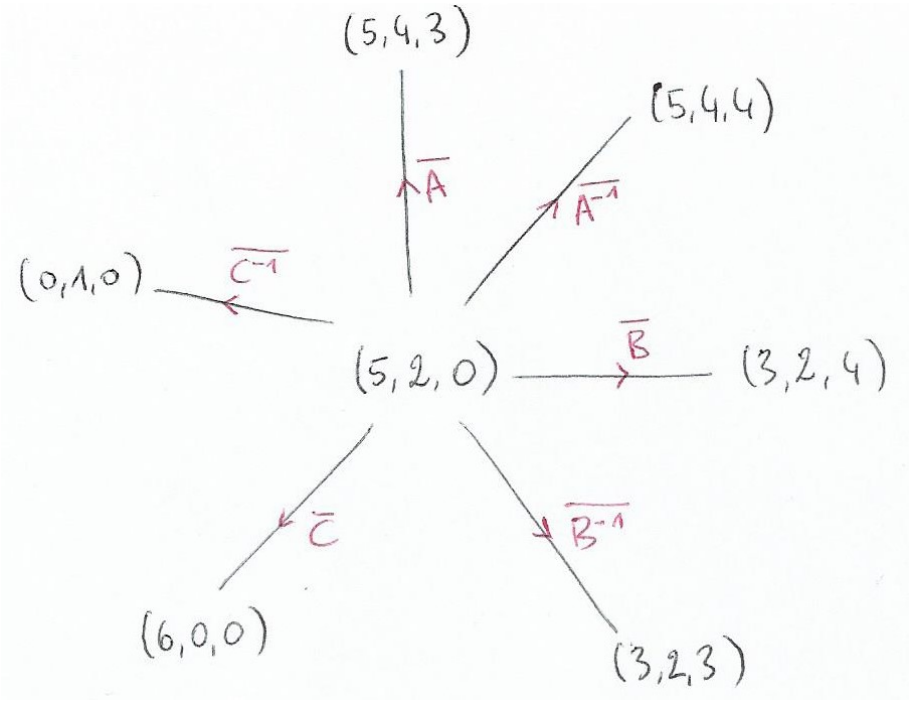


FIGURE 1. The edges joining $\overline{\mathbf{x}} = (5, 2, 0)$ to the $\overline{\gamma}\ \overline{\mathbf{x}}$, $\gamma \in \mathcal{A}_5$.

Then, starting from each of our 6 new vertices, we can draw edges joining them to their images under the action of the matrices of $\mathcal{A}_5$. If we do several extra steps we obtain the following part of the graph $\mathscr{R}_3(d, q)$ (but it is hard to represent the whole graph, since it has 42 vertices, each of them with 6 incident edges...)

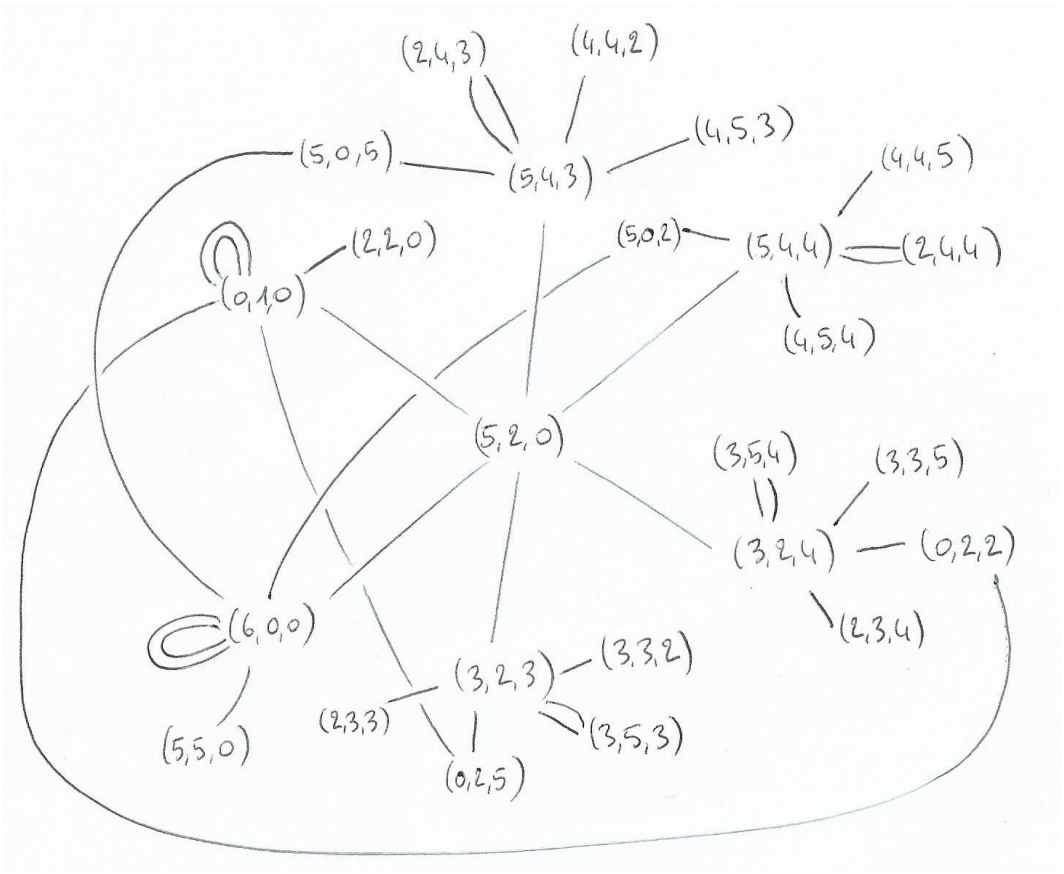


FIGURE 2. A part of the graph $\mathscr{R}_3(29,7)$.

We just saw that the structure of the graph $\mathscr{R}_3(d,q)$ depends a lot on the arithmetic properties of the integers involved. The number of edges meeting at a fixed vertex essentially depends on the number of ways to write p as a sum of four squares. One may also ask : how many vertices are there ? This is also an arithmetic question, since we need to understand the number of solutions to the equation

$$x^2+y^2+z^2=d$$

in $\mathbf{Z}/q\mathbf{Z}$. Heuristically, we can guess that the answer will be roughly q^2, because once x and y are fixed (q^2 choices for their values), then either $d-x^2-y^2$ is a square modulo q, and in this case there are two solutions z to the equation above, or $d-x^2-y^2$ is not a square modulo q, and in this case there is no solution. Since there are roughly as many squares as non-squares modulo q, this gives us the conclusion of this heuristic. However, this argument can be made more rigorous : using the chinese remainder theorem, we reduce to the case whre q is a power of a prime number, and in this case estimates follow from classical computations on Gauss sums. This leads to the following result.

Proposition 5.3.2. *For any $\varepsilon>0$, one has*

$$q^{2-\varepsilon} \ll_\varepsilon |\mathscr{R}_3(d,q)| \ll_\varepsilon q^{2+\varepsilon}$$

for all $q\geqslant 2$ and for all d coprime with q.

5.4 Trajectories on $\mathscr{R}_3(d,q)$

To each point $\mathbf{x}\in\mathscr{R}_3(d)$, we want to attach a trajectory on the graph $\mathscr{R}_3(d,q)$: a first idea could be to reduce modulo q the coordinates of the points of the trajectory of $\mathbf{x}$ on $\mathscr{R}_3(d)$, as defined in section 5.2. So the trajectory associated with $\mathbf{x}\in\mathscr{R}_3(d)$ would be the sequence $(\overline{\mathbf{x}}_i)_{i\in\mathbf{Z}}$, where $\overline{\mathbf{x}}_i$ denotes $\mathrm{red}_q(\mathbf{x}_i)$, and $(\mathbf{x}_i)_{i\in\mathbf{Z}}$ is the trajectory of $\mathbf{x}=\mathbf{x}_0$ on $\mathscr{R}_3(d)$. However, if we do that, there is the risk that "too many" distinct points on $\mathscr{R}_3(d)$ give rise to the same trajectory, because the congruence

properties of the $\mathbf{x}_i$'s will be the same, despite the fact that we started from different trajectories on $\mathscr{R}_3(d)$. So in order to get many different trajectories, we also take into account the edge connecting $\overline{\mathbf{x}}_i$ and $\overline{\mathbf{x}}_{i+1}$. Thus, to each $\mathbf{x} \in \mathscr{R}_3(d)$, we attach a *marked walk* on $\mathscr{R}_3(d,q)$ consisting of a marked base point $\overline{\mathbf{x}}_0$ and the choice, for each i, of an edge joining $\overline{\mathbf{x}}_i$ to $\overline{\mathbf{x}}_{i+1}$.

Definition 5.4.1. *With the notations of section 5.2 for the transition matrices, the trajectory of the point $\mathbf{x} \in \mathscr{R}_3(d)$ is*

$$\Gamma_{\mathbf{x}} := \{\overline{\mathbf{x}}, (w_{\mathbf{x},i})_{i\in\mathbf{Z}}\}$$

By the previous section, we know that the elements of $\mathcal{A}_p$ label the edges of our graph $\mathscr{R}_3(d,q)$. Therefore, $\Gamma_{\mathbf{x}}$ defines a walk on $\mathscr{R}_3(d,q)$: starting from $\overline{\mathbf{x}}_0 := \overline{\mathbf{x}}$, we go to $\overline{\mathbf{x}}_1 = \overline{w}_{\mathbf{x},1}\overline{\mathbf{x}}_0$ via the edge labeled $w_{\mathbf{x},1}$, then we go from $\overline{\mathbf{x}}_1$ to $\overline{\mathbf{x}}_2 = \overline{w}_{\mathbf{x},2}\overline{\mathbf{x}}_1$ via the edge labeled $w_{\mathbf{x},2}$, and so on. In the other direction, we define $\overline{\mathbf{x}}_{-1}$ as $\overline{w}_{\mathbf{x},0}^{-1}\mathbf{x}_0$, and we draw the walk going from $\overline{\mathbf{x}}_{-1}$ to $\overline{\mathbf{x}}_0$ via the edge labeled $w_{\mathbf{x},0}$, and so on.

Finally, for any integer $\ell \geqslant 1$, we define $W_{\mathbf{x}}^{(\ell)}$ (resp. $\Gamma_{\mathbf{x}}^{(\ell)}$) to be the truncated word (resp. truncated walk) of length 2ℓ. Explicitly :

$$W_{\mathbf{x}}^{(\ell)} = (w_{\mathbf{x},-\ell+1}, w_{\mathbf{x},-\ell+2}, \ldots, w_{\mathbf{x},\ell})$$

and

$$\Gamma_{\mathbf{x}}^{(\ell)} = (\overline{\mathbf{x}}, w_{\mathbf{x},-\ell+1}, w_{\mathbf{x},-\ell+2} \ldots, w_{\mathbf{x},\ell})$$

Example : We continue in the setting of the previous examples : $p = 5$, $d = 29$ and $q = 7$. Consider the truncated trajectory on $\mathscr{R}_3(d)$ from the example in section 5.2 :

$$\cdots \underset{\mathbf{x}_{-2}}{\begin{pmatrix}2\\-4\\-3\end{pmatrix}} \overset{C^{-1}}{\longmapsto} \underset{\mathbf{x}_{-1}}{\begin{pmatrix}-4\\2\\-3\end{pmatrix}} \overset{B^{-1}}{\longmapsto} \underset{\mathbf{x}_0}{\begin{pmatrix}5\\2\\0\end{pmatrix}} \overset{B^{-1}}{\longmapsto} \underset{\mathbf{x}_1}{\begin{pmatrix}-4\\2\\3\end{pmatrix}} \overset{C}{\longmapsto} \underset{\mathbf{x}_2}{\begin{pmatrix}2\\-4\\3\end{pmatrix}} \cdots$$

We reduce this trajectory modulo 7 :

$$\cdots \underset{\overline{\mathbf{x}}_{-2}}{\begin{pmatrix}2\\3\\4\end{pmatrix}} \overset{\overline{C^{-1}}}{\longmapsto} \underset{\overline{\mathbf{x}}_{-1}}{\begin{pmatrix}3\\2\\4\end{pmatrix}} \overset{\overline{B^{-1}}}{\longmapsto} \underset{\overline{\mathbf{x}}_0}{\begin{pmatrix}5\\2\\0\end{pmatrix}} \overset{\overline{B^{-1}}}{\longmapsto} \underset{\overline{\mathbf{x}}_1}{\begin{pmatrix}3\\2\\3\end{pmatrix}} \overset{\overline{C}}{\longmapsto} \underset{\overline{\mathbf{x}}_2}{\begin{pmatrix}2\\3\\3\end{pmatrix}} \cdots$$

This gives the following truncated walk $\Gamma_{\mathbf{x}}^{(2)}$:

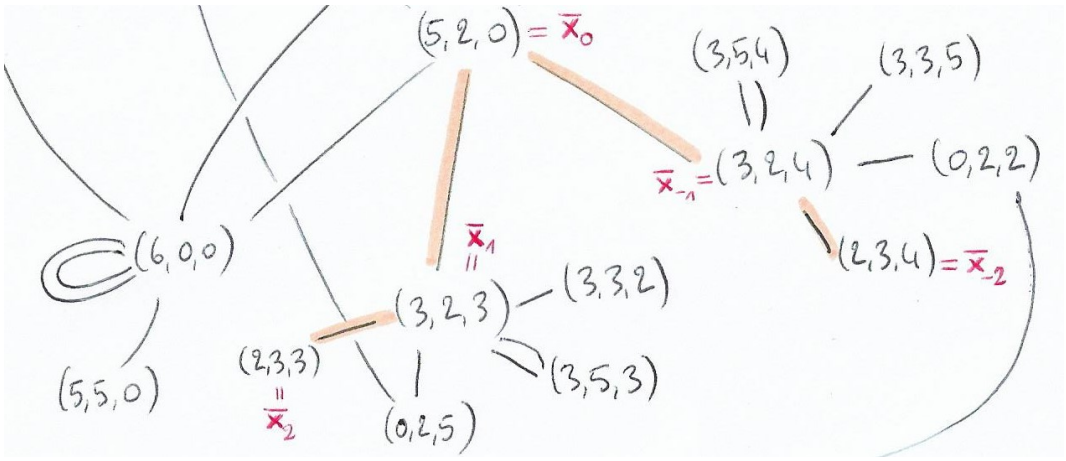


FIGURE 3. The truncated walk $\Gamma_{\mathbf{x}}^{(2)}$ on the graph $\mathscr{R}_3(29,7)$, for $\mathbf{x} = (5,2,0)$.

Let us stress that the trajectories arising as $\Gamma_{\mathbf{x}}$ cannot be arbitrary walks on the graph $\mathscr{R}_3(d,q)$. Indeed, by proposition 5.2.3, the word $W_{\mathbf{x}}$ satisfies the condition $w_{\mathbf{x},i+1} \neq w_{\mathbf{x},i}^{-1}$ for all $i \in \mathbf{Z}$. Thus, the walk cannot traverse the same edge twice in succession. However, this does not prevent $\Gamma_{\mathbf{x}}$ from going from $\overline{\mathbf{x}}$ to $\overline{\mathbf{y}}$ and then right after from $\overline{\mathbf{y}}$ to $\overline{\mathbf{x}}$. But it has to use different edges. More informally, a walker following the trajectory $\Gamma_{\mathbf{x}}$ is allowed to go back to a vertex she has already visited, but is not allowed to backtrack.

Definition 5.4.2. *A non-backtracking marked walk on the graph $\mathscr{R}_3(d,q)$ is the data $(\overline{\mathbf{x}}, (w_i)_{i\in\mathbf{Z}})$ of a base point $\overline{\mathbf{x}}$, and a reduced word $(w_i)_{i\in\mathbf{Z}}$ in the alphabet $\mathcal{A}_p$ (see definition 5.2.4). The sequence of vertices visited by the walk can be determined inductively by the rule that $\overline{\mathbf{x}}_{i+1}$ is the vertex arrived at by following the edge labeled w_{i+1} starting from $\overline{\mathbf{x}}_i$.*

Example : we make this example mostly to stress an important point : this definition includes all the possible non-backtracking walks on $\mathscr{R}_3(d,q)$, not only the ones arising as the reduction modulo q of a trajectory on $\mathscr{R}_3(d)$. For instance, if we keep the same values as in the previous examples ($d = 29, p = 5$ and $q = 7$), the point $(6,0,0)$ belongs to $\mathscr{R}_3(d,q)$, but it is easy to see that no point of $\mathscr{R}_3(d)$ reduces to this point modulo q. However, we can define a non-backtracking marked walk with marked point $\overline{\mathbf{x}} = (6,0,0)$. Consider the (truncated) word (A, B, C, B^{-1}, A, B). It gives rise to the following truncated walk on $\mathscr{R}_3(d,q)$:

$$\underset{\overline{\mathbf{x}}_{-3}}{\begin{pmatrix}3\\-2\\-4\end{pmatrix}} \xmapsto{A} \underset{\overline{\mathbf{x}}_{-2}}{\begin{pmatrix}3\\-5\\3\end{pmatrix}} \xmapsto{B} \underset{\overline{\mathbf{x}}_{-1}}{\begin{pmatrix}5\\-5\\0\end{pmatrix}} \xmapsto{C} \underset{\overline{\mathbf{x}}_{0}}{\begin{pmatrix}6\\0\\0\end{pmatrix}} \xmapsto{B^{-1}} \underset{\overline{\mathbf{x}}_{1}}{\begin{pmatrix}5\\0\\5\end{pmatrix}} \xmapsto{A} \underset{\overline{\mathbf{x}}_{2}}{\begin{pmatrix}5\\3\\3\end{pmatrix}} \xmapsto{B} \underset{\overline{\mathbf{x}}_{3}}{\begin{pmatrix}2\\3\\-4\end{pmatrix}}$$

5.5 Spacing properties of trajectories

As we already mentioned, it is possible that distinct trajectories on $\mathscr{R}_3(d)$ give rise to the same trajectories on $\mathscr{R}_3(d,q)$, at least for a certain time. Indeed, even if we start from two different points $\mathbf{x}$ and $\mathbf{x}'$ in $\mathscr{R}_3(d)$, they may have the same reduction modulo q, and the truncated words $W_{\mathbf{x}}^{(\ell)}$ and $W_{\mathbf{x}'}^{(\ell)}$ may coincide. In this section, we try to develop criteria to measure the closeness of trajectories.

Proposition 5.5.1 (Shadowing Lemma, [EMV10], proposition 2.11). *Let $\mathbf{x}, \mathbf{x}' \in \mathscr{R}_3(d)$. Let $\ell \geqslant 1$.*

- *The truncated words $W_{\mathbf{x}}^{(\ell)}$ and $W_{\mathbf{x}'}^{(\ell)}$ coincide if and only if $\mathbf{x} \equiv \pm\mathbf{x}' \bmod p^\ell$.*
- *The truncated walks $\Gamma_{\mathbf{x}}^{(\ell)}$ and $\Gamma_{\mathbf{x}'}^{(\ell)}$ coincide if and only if, in addition, $\mathbf{x} \equiv \mathbf{x}' \bmod q$.*

Let us denote by $\mathbf{x}.\mathbf{x}'$ the usual scalar product of these two vectors in $\mathbf{Q}^3$. If $\Gamma_{\mathbf{x}}^{(\ell)}$ and $\Gamma_{\mathbf{x}'}^{(\ell)}$ coincide, then :

$$\mathbf{x}.\mathbf{x}' \equiv d \bmod q^2 \quad \text{and} \quad \mathbf{x}.\mathbf{x}' \equiv \pm d \bmod p^{2\ell}$$

Proof. We admit the first point. It is proved in the article, but in a part entitled "adelization" which introduces a lot of notions that are new to me, I would need a lot more time to understand this part. However, let us give a reformulation of the statement, in order to understand what it means, and why it is difficult. Let us denote $W_{\mathbf{x}} = (w_i)_{i\in\mathbf{Z}}$ and $W_{\mathbf{x}'} = (w'_i)_{i\in\mathbf{Z}}$.
For $\ell = 1$, the condition $W_{\mathbf{x}}^{(\ell)} = W_{\mathbf{x}'}^{(\ell)}$ means that $(w_0, w_1) = (w'_0, w'_1)$. Equivalently, this means that when we define the trajectories of $\mathbf{x}$ and $\mathbf{x}'$ on $\mathscr{R}_3(d)$, we take the same matrix $w_0 \in \mathcal{A}_p$ to define $\mathbf{x}_{-1}$ (as $w_0^{-1}\mathbf{x}$) and $\mathbf{x}'_{-1}$ (as $w_0^{-1}\mathbf{x}'$) and the same matrix $w_1 \in \mathcal{A}_p$ to define $\mathbf{x}_1$ (as $w_1\mathbf{x}$) and $\mathbf{x}'_1$ (as $w_1\mathbf{x}'$). Therefore, the meaning of the first point is that the fact that $\mathbf{x}$ and $\mathbf{x}'$ are p-adically close forces us to choose the same matrices in $\mathcal{A}_p$ for a long time, when defining the trajectories of these two points on $\mathscr{R}_3(d)$. Since matrices in $\mathcal{A}_p$ are rotations of $\mathbf{Q}^3$, we can also reformulate it as a condition for the trajectories of $\mathbf{x}$ and $\mathbf{x}'$ to be parallel for a long time.
Now, if we go back to section 5.2 to remember how these matrices of $\mathcal{A}_p$ are chosen, we see that the condition $W_{\mathbf{x}}^{(1)} = W_{\mathbf{x}'}^{(1)}$ is equivalent to the following equalities of ideals of $\mathrm{B}(\mathbf{Z})$:

$$\mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}) = \mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}'}(\mathfrak{p}) \text{ and } \mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}}(\mathfrak{p}') = \mathrm{B}(\mathbf{Z})\iota_{\mathbf{x}'}(\mathfrak{p}')$$

(where $\mathfrak{p}$ and $\mathfrak{p}'$ still denote the two ideals above p in $\mathbf{Q}(\sqrt{-d})$). But it does not seem easy to make a connection between the p-adic closeness of $\mathbf{x}$ and $\mathbf{x}'$ and the fact that the ideals of $\mathrm{B}(\mathbf{Z})$ associated with the action of $\mathfrak{p}$ and $\mathfrak{p}'$ on $\mathbf{x}$ and $\mathbf{x}'$ are the same.

The second point is clear, since the walks coincide if and only if they have the same marked point and the same transition matrices. The condition "$\mathbf{x} \equiv \mathbf{x}'$ mod q" is exactly the condition "having the same marked point".

Finally, if the two truncated trajectories are equal, then $\mathbf{x} \equiv \pm\mathbf{x}'$ mod p^ℓ and $\mathbf{x} \equiv \mathbf{x}'$ mod q. This implies that $(\mathbf{x} - \pm\mathbf{x}').(\mathbf{x} - \pm\mathbf{x}') \equiv 0$ mod $p^{2\ell}$ and $(\mathbf{x} - \mathbf{x}').(\mathbf{x} - \mathbf{x}') \equiv 0$ mod q^2. If we develop the first congruence, and take into account that $\mathbf{x}.\mathbf{x} = d = \mathbf{x}'.\mathbf{x}'$, we obtain $\pm 2\mathbf{x}.\mathbf{x}' \equiv 2d$ mod $p^{2\ell}$. Since p is an odd prime, we can multiply by the inverse of 2 modulo p, and this gives $\mathbf{x}.\mathbf{x}' \equiv \pm d$ mod $p^{2\ell}$. Similarly, the second congruence leads to $\mathbf{x}.\mathbf{x}' \equiv d$ mod q^2. Note that q is also odd because we assumed q coprime with $6p$.

□

Notation : In order to avoid carrying too many constants we will use the notations "$f \ll g$" and "$f \gg g$" in the sequel. These notations are used a lot in analytic number theory, and differ a little bit from the notation $f = O(g)$, so let us take some time to make some precisions. We follow the introduction of [Kow04].

- *The notation $f = O(g)$:* we consider a topological space X, and a point $x_0 \in X$. Let f and g be two real valued functions defined on a neighbourhood of x_0 in X, not necessarily defined at x_0. We say that
$$f = O(g) \text{ when } x \to x_0$$
if there exists a neighbourhood V of x_0 in X and a constant C (depending a priori on x_0 and V) such that $|f(x)| \leqslant Cg(x)$ for all $x \in V \setminus \{x_0\}$.

- *The notation $f \ll g$:* we consider two functions f, g defined on a set X (not necessarily a topological space), and with real values. Then we say that :
$$f \ll g \text{ on } Y \subseteq X$$
if there exists a constant C such that for all $x \in Y$, $|f(x)| \leqslant Cg(x)$. We will refer to such a constant C as an implicit constant (because is does not appear when writing $f \ll g$). Besides, C can depend on other parameters (ε, δ for instance), and in this case if we want to stress on which parameters it depends, we will write $f \ll_{\varepsilon,\delta} g$.

The difference is that in the second case, the subset Y must be written explicitly, whereas in the first case, the neighbourhood V is implicit, and could be replaced by a smaller neighbourhood of x_0. The notation O refers to an asymptotic behaviour, whereas the notation $f \ll g$ can be used for an equality that holds everywhere where f and g are defined. Very often, the subset Y is clear from the context. For instance when we gave an estimate of $|\mathscr{R}_3(d)|$ in section 4.4, we could have replaced the long sentence "for all $\varepsilon > 0$, there exists a constant $C(\varepsilon)$, depending only on ε, such that for all $d \geqslant 2$ admissible and square-free, $|\mathscr{R}_3(d)| \geqslant C(\varepsilon) d^{\frac{1}{2}-\varepsilon}$" (and the analogue statement for the upper bound) by the more compact notation :

$$\text{for any } \varepsilon > 0,\ d^{\frac{1}{2}-\varepsilon} \ll_\varepsilon |\mathscr{R}_3(d)| \ll_\varepsilon d^{\frac{1}{2}+\varepsilon} \text{ for all } d \geqslant 2 \text{ admissible and square-free.}$$

But in the sequel, we will sometimes omit the set in which d ranges, since in the whole study of our equidistribution problem, d is assumed to be admissible and square-free.

Proposition 5.5.2 (Linnik's basic Lemma, [EMV10], proposition 2.12)**.** *Let $e \in \mathbf{Z}$ be such that $|e| \neq d$. The number of pairs $(\mathbf{x}, \mathbf{x}') \in \mathscr{R}_3(d)^2$ with scalar product $\mathbf{x}.\mathbf{x}' = e$ is $\ll_\varepsilon d^\varepsilon$.*

Proof. We admit this proposition. It is proved in [EMV10], pages 24 and 25, using a construction called the orthogonal complement construction, which is not hard to understand once one knows about the action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\widetilde{\mathscr{R}_3(d)}^+$. The reason why we admit this lemma is that the second part of the proof relies on the notion of a quadratic form represented by another quadratic form, and we did not have time to read more about this vocabulary. □

Observe that since $\mathbf{x}.\mathbf{x} = \mathbf{x}'.\mathbf{x}' = d$, we have $|\mathbf{x}.\mathbf{x}'| \leqslant d$ by Cauchy-Schwarz inequality. Hence if $|e| > d$, there is no pair $(\mathbf{x}, \mathbf{x}') \in \mathscr{R}_3(d)^2$ with scalar product equal to e. Besides, if $|e| = d$, a pair $(\mathbf{x}, \mathbf{x}')$ such that $\mathbf{x}.\mathbf{x}' = e$ satisfies the case of equality in Cauchy-Schwarz inequality, so $\mathbf{x}'$ must be proportional to $\mathbf{x}$. As they have the same norm, this implies that $\mathbf{x} = \pm\mathbf{x}'$, and the sign is determined by the sign of e. This shows that there are $|\mathscr{R}_3(d)|$ pairs with scalar product equal to d : namely the pairs $(\mathbf{x}, \mathbf{x})$, for $\mathbf{x} \in \mathscr{R}_3(d)$, and $|\mathscr{R}_3(d)|$ pairs with scalar product equal to $-d$, namely the pairs $(\mathbf{x}, -\mathbf{x})$ for $\mathbf{x} \in \mathscr{R}_3(d)$.

Corollary 5.5.3. *For any $\varepsilon > 0$, one has :*

$$\left|\left\{(\mathbf{x}, \mathbf{x}') \in \mathscr{R}_3(d)^2,\ \Gamma_{\mathbf{x}}^{(\ell)} = \Gamma_{\mathbf{x}'}^{(\ell)}\right\}\right| \ll_\varepsilon |\mathscr{R}_3(d)| + d^\varepsilon \left(1 + \frac{d}{q^2 p^{2\ell}}\right)$$

Proof. We decompose the set with respect to the value of $\mathbf{x}.\mathbf{x}'$:

$$\underbrace{\left\{(\mathbf{x}, \mathbf{x}') \in \mathscr{R}_3(d)^2,\ \Gamma_{\mathbf{x}}^{(\ell)} = \Gamma_{\mathbf{x}'}^{(\ell)}\right\}}_{=:A} = \bigsqcup_{e \in \mathbf{Z}} \underbrace{\left\{(\mathbf{x}, \mathbf{x}') \in \mathscr{R}_3(d)^2,\ \Gamma_{\mathbf{x}}^{(\ell)} = \Gamma_{\mathbf{x}'}^{(\ell)} \text{ and } \mathbf{x}.\mathbf{x}' = e\right\}}_{=:A_e}$$

By the previous observation, the sets on the right hand side are empty if $|e| > d$, hence :

$$|A| = \sum_{|e| \leqslant d} |A_e|$$

Now, we bound the terms where $|e| = d$ by the number of pairs such that $\mathbf{x}.\mathbf{x}' = e$, that is : $|\mathscr{R}_3(d)|$. This gives :

$$|A| \leqslant 2|\mathscr{R}_3(d)| + \sum_{|e| < d} |A_e|$$

Besides, by proposition 5.5.1, if $\mathbf{x}$ and $\mathbf{x}'$ are such that $\Gamma_{\mathbf{x}'}^{(\ell)} = \Gamma_{\mathbf{x}}^{(\ell)}$, then

$$\begin{cases} \mathbf{x}.\mathbf{x}' \equiv d \bmod q^2 \\ \mathbf{x}.\mathbf{x}' \equiv \pm d \bmod p^{(2\ell)} \end{cases} \tag{20}$$

So if e does not verify the congruences (20), the set A_e is empty. Thus,

$$|A| \leqslant 2|\mathscr{R}_3(d)| + \sum_{\substack{|e| < d \\ e \equiv d \bmod q^2 \\ e \equiv \pm d \bmod p^{2\ell}}} |A_e|$$

By Linnik's basic lemma (proposition 5.5.2), we have the following estimate : for any $\varepsilon > 0$, $|A_e| \ll_\varepsilon d^\varepsilon$. Hence :

$$|A| \ll_\varepsilon |\mathscr{R}_3(d)| + d^\varepsilon \sum_{\substack{|e| < d \\ e \equiv d \bmod q^2 \\ e \equiv \pm d \bmod p^{2\ell}}} 1$$

It remains to count the number of terms of this last sum. Since p and q are coprime, there is a unique integer satisfying the conditions $e \equiv d \bmod q^2$ and $e \equiv d \bmod p^{2\ell}$ in any interval of integers of length $q^2 p^{2\ell}$, and the same holds with the condition $e \equiv -d \bmod p^{2\ell}$ (this is a reformulation of chinese remainder theorem). Let us write the euclidean division of d by $q^2 p^{2\ell}$:

$$d = (q^2 p^{2\ell})m + b, \text{ with } m = \left\lfloor \frac{d}{q^2 p^{2\ell}} \right\rfloor \text{ and } 0 \leqslant b < q^2 p^{2\ell}$$

Then the interval $\{0,\dots,d\}$ is made of m successive intervals of length $q^2p^{2\ell}$, and a last interval of length strictly less than $q^2p^{2\ell}$. Each of these intervals contains at most 2 integers satisfying the congruences (20). Thus, there are at most $2(m+1)$ integers e such that $0 \leqslant e \leqslant d$, $e \equiv d \bmod q^2$ and $e \equiv \pm d \bmod p^{2\ell}$. We do the same argument for negative values of e, and conclude that the number of terms of the sum is bounded by $4(m+1)$. As $m \leqslant \frac{d}{q^2p^{2\ell}}$, this number of terms is also bounded by $4\left(1+\frac{d}{q^2p^{2\ell}}\right)$. Since the constants become implicit in the notation "$\ll$", we obtain

$$|A| \ll_\varepsilon |\mathscr{R}_3(d)| + d^\varepsilon\left(1+\frac{d}{q^2p^{2\ell}}\right)$$

as we wanted.

□

Remark. *In the previous statement, if ℓ is chosen so that $q^2p^{2\ell} \simeq \sqrt{d} \simeq |\mathscr{R}_3(d)|$, then the upper bound is $\ll_\varepsilon d^{\frac{1}{2}+\varepsilon}$ for any $\varepsilon > 0$ (here we use the upper bound for $|\mathscr{R}_3(d)|$ from section 4.4). In particular, since*

$$|A| = \left|\left\{(\mathbf{x},\mathbf{x}') \in \mathscr{R}_3(d)^2,\ \Gamma_{\mathbf{x}}^{(\ell)} = \Gamma_{\mathbf{x}'}^{(\ell)}\right\}\right| = \sum_{\mathbf{x}\in\mathscr{R}_3(d)} \left|\left\{\mathbf{x}' \in \mathscr{R}_3(d),\ \Gamma_{\mathbf{x}'}^{(\ell)} = \Gamma_{\mathbf{x}}^{(\ell)}\right\}\right|$$

we have

$$\underbrace{\sum_{\mathbf{x}\in\mathscr{R}_3(d)}}_{\simeq\sqrt{d}\ \text{terms}} \left|\left\{\mathbf{x}' \in \mathscr{R}_3(d),\ \Gamma_{\mathbf{x}'}^{(\ell)} = \Gamma_{\mathbf{x}}^{(\ell)}\right\}\right| \ll_\varepsilon d^{\frac{1}{2}+\varepsilon}$$

which implies that the map $\mathbf{x} \mapsto \Gamma_{\mathbf{x}}^{(\ell)}$ is essentially injective.

5.6 Expander graphs

The theory of expander graphs is a very wide subject, that I did not have time to explore. The introduction of these notes (which have now become a book), by Emmanuel Kowalski, gives many points of view and motivations on expander graphs : https://people.math.ethz.ch/~kowalski/expander-graphs.pdf

We will use the fact that $\mathscr{R}_3(d,q)$ is an expander :

Theorem 5.6.1. *For all q coprime with $6p$, the graph $\mathscr{R}_3(d,q)$ is an expander.*

Once again, this statement comes from the fact $\mathscr{R}_3(d,q)$ can be identified with a finite quotient of the Bruhat-Tits tree of $\mathrm{PGL}_2(\mathbf{Q}_p)$.

However, we will only use the following consequence of this fact, namely a large deviation inequality for non-backtracking walks on $\mathscr{R}_3(d,q)$:

Corollary 5.6.2. *Fix $\eta,\varepsilon > 0$. For any subset $\mathcal{B} \subseteq \mathscr{R}_3(d,q)$ with $|\mathcal{B}| \geqslant \eta|\mathscr{R}_3(d,q)|$, the fraction of non-backtracking walks $\Gamma_{\overline{\mathbf{x}}}$ of length 2ℓ centered at any fixed point $\overline{\mathbf{x}}$ of $\mathscr{R}_3(d,q)$ which satisfy :*

$$\left|\frac{|\Gamma_{\overline{\mathbf{x}}} \cap \mathcal{B}|}{2\ell+1} - \frac{|\mathcal{B}|}{|\mathscr{R}_3(d,q)|}\right| \geqslant \varepsilon$$

is bounded by $c_1\exp(-c_2\ell)$, where c_1,c_2 are strictly positive constants depending only on ε,η. In other words, if we denote by Λ_ℓ the set of all non-backtracking walks of length 2ℓ (see definition 5.4.2), and by M the subset of Λ_ℓ made of the walks satisfying the inequality above, then :

$$\frac{|M|}{|\Lambda_\ell|} \leqslant c_1\exp(-c_2\ell).$$

In this statement (and everywhere below), $|\Gamma_{\overline{\mathbf{x}}} \cap \mathcal{B}|$ denotes the number of indices $i \in \{-\ell, \dots, \ell\}$ such that $\overline{\mathbf{x}}_i$ (the i-th point of the walk $\Gamma_{\overline{\mathbf{x}}}$) belongs to $\mathcal{B}$. So we may interpret the term $|\Gamma_{\overline{\mathbf{x}}} \cap \mathcal{B}|/(2\ell+1)$ as the fraction of the time that the walk $\Gamma_{\overline{\mathbf{x}}}$ (of length 2ℓ) spends inside the subset $\mathcal{B}$.
On the other hand, if we endow $\mathscr{R}_3(d,q)$ with the uniform probability measure, the term $|\mathcal{B}|/|\mathscr{R}_3(d,q)|$ is the probability of $\mathcal{B}$. To put it differently, it is the probability that an element $\overline{\mathbf{x}} \in \mathscr{R}_3(d,q)$, taken at random with uniform distribution, belongs to $\mathcal{B}$.

Since the graph $\mathscr{R}_3(d,q)$ has good connectivity properties (this is a way to interpret theorem 5.6.1), it is natural to expect that a typical walk will spend a fraction of the time in $\mathcal{B}$ which is approximately the probability of being in $\mathcal{B}$. Thus, the inequality in the corollary is a large deviation inequality. The walks satisfying this inequality are "exceptional", and so there should not be many such walks. The corollary states that the fraction of such walks decays exponentially with ℓ.

5.7 Conclusion of the proof

We can finally prove theorem 5.0.3. Let $p > 3$ be a prime number, and let q be an integer coprime with $6p$. Our aim is to prove a refinement of the fact that the points of $\mathscr{R}_3(d)$ become equidistributed in $\mathscr{R}_3(d,q)$ (with respect to the uniform measure) as d goes to infinity among the values of d such that p is split in $\mathbf{Q}(\sqrt{-d})$ and d is coprime with q.
More precisely, let us fix $\nu, \delta > 0$, and suppose that $q^2 \leqslant d^{\frac{1}{2}-\nu}$ (in our refinement, q is no longer fixed, it just has to grow slowly compared to d). Then our aim is to prove that the fraction of $\overline{\mathbf{x}} \in \mathscr{R}_3(d,q)$ such that

$$|\mathrm{dev}_d(\overline{\mathbf{x}})| > \delta$$

tends to zero as d goes to infinity. As in the statement of the theorem, $\mathrm{dev}_d(\overline{\mathbf{x}})$ denotes the deviation at $\overline{\mathbf{x}}$:

$$\frac{\frac{|\mathrm{red}_q^{-1}(\overline{\mathbf{x}})|}{|\mathscr{R}_3(d)|}}{\frac{1}{|\mathscr{R}_3(d,q)|}} - 1$$

that is : the gap between the proportion of the points of $\mathscr{R}_3(d)$ that reduce to $\overline{\mathbf{x}}$ modulo q, and $\frac{1}{|\mathscr{R}_3(d,q)|}$ (which is the expected asymptotic result if the equidistribution indeed holds).

Let us denote

$$\mathcal{B}_\delta := \{\overline{\mathbf{x}} \in \mathscr{R}_3(d,q),\ \mathrm{dev}_d(\overline{\mathbf{x}}) > \delta\} \text{ and } \mathcal{B}_\delta^- := \{\overline{\mathbf{x}} \in \mathscr{R}_3(d,q),\ \mathrm{dev}_d(\overline{\mathbf{x}}) < -\delta\}$$

We want to prove that

$$\frac{|\{\overline{\mathbf{x}} \in \mathscr{R}_3(d,q),\ |\mathrm{dev}_d(\overline{\mathbf{x}})| > \delta\}|}{|\mathscr{R}_3(d,q)|} \underset{d\to+\infty}{\longrightarrow} 0$$

As $\{\overline{\mathbf{x}} \in \mathscr{R}_3(d,q),\ |\mathrm{dev}_d(\overline{\mathbf{x}})| > \delta\} = \mathcal{B}_\delta \sqcup \mathcal{B}_\delta^-$, it suffices to show that

$$\frac{|\mathcal{B}_\delta|}{|\mathscr{R}_3(d,q)|} \underset{d\to+\infty}{\longrightarrow} 0 \quad \text{and} \quad \frac{|\mathcal{B}_\delta^-|}{|\mathscr{R}_3(d,q)|} \underset{d\to+\infty}{\longrightarrow} 0$$

The proof goes the same way for the two limits above, so we just focus on the the first one.

Let $\eta > 0$. We want to show that for all d large enough, $|\mathcal{B}_\delta| \leqslant \eta|\mathscr{R}_3(d,q)|$. Let us assume that $|\mathcal{B}_\delta| > \eta|\mathscr{R}_3(d,q)|$, and look for a contradiction for all d large enough.

§5.7.1 Useful lemmas

Lemma 5.7.1. *Let $\mathcal{B}$ be a subset of $\mathscr{R}_3(d,q)$ and $\ell \geqslant 1$. Then*

$$|\mathrm{red}_q^{-1}(\mathcal{B})| = \frac{1}{2\ell+1} \sum_{\mathbf{x} \in \mathscr{R}_3(d)} |\Gamma_{\mathbf{x}}^{(\ell)} \cap \mathcal{B}|$$

where $|\Gamma_{\mathbf{x}}^{(\ell)} \cap \mathcal{B}|$ denotes the number of i's in $\{-\ell, \dots, \ell\}$ such that the i-th vertex $\overline{\mathbf{x}}_i$ of $\Gamma_{\mathbf{x}}$ is inside $\mathcal{B}$.

Proof. Since the action of $[\mathfrak{p}]^i$ on $\mathscr{R}_3(d)$ permutes $\mathscr{R}_3(d)$, we have : for all $i \in \{-\ell, \dots, \ell\}$,

$$|\mathrm{red}_q^{-1}(\mathcal{B})| = \sum_{\substack{\mathbf{x}\in\mathscr{R}_3(d)\\ \mathrm{red}_q(\mathbf{x})\in\mathcal{B}}} 1 = \sum_{\substack{\mathbf{x}\in\mathscr{R}_3(d)\\ \mathrm{red}_q([\mathfrak{p}]^i\mathbf{x})\in\mathcal{B}}} 1$$

Now, we sum over $i \in \{-\ell, \dots, \ell\}$ and divide by $2\ell+1$. This gives :

$$|\mathrm{red}_q^{-1}(\mathcal{B})| = \frac{1}{2\ell+1} \sum_{\mathbf{x}\in\mathscr{R}_3(d)} \sum_{\substack{i\in\{-\ell,\dots,\ell\}\\ \mathrm{red}_q([\mathfrak{p}]^i\mathbf{x})\in\mathcal{B}}} 1 = \frac{1}{2\ell+1} \sum_{\mathbf{x}\in\mathscr{R}_3(d)} |\Gamma_{\mathbf{x}}^{(\ell)} \cap \mathcal{B}|$$

□

Lemma 5.7.2. *If d is large enough, there exists an integer $\ell \geqslant 1$ such that :*

$$\frac{1}{p}|\mathscr{R}_3(d)| < q^2 p^{2\ell} \leqslant p|\mathscr{R}_3(d)| \tag{21}$$

Proof. First, note that it is not restrictive to assume d large enough, since we are looking for a contradiction when d is large enough. This lemma is where we use the assumption

$$q^2 \leqslant d^{\frac{1}{2}-\nu}$$

Thanks to theorem 4.4.1, we know that for any $\varepsilon > 0$, $d^{\frac{1}{2}-\varepsilon} \ll_\varepsilon |\mathscr{R}_3(d)|$. Therefore, for $\varepsilon := \frac{\nu}{2}$, there exists a constant C such that for all $d \geqslant 2$ admissible and square-free,

$$d^{\frac{1}{2}-\frac{\nu}{2}} \leqslant C|\mathscr{R}_3(d)|.$$

So for d large enough, we have :

$$q^2 \leqslant d^{\frac{1}{2}-\nu} < \frac{1}{Cp} d^{\frac{1}{2}-\frac{\nu}{2}} \leqslant \frac{|\mathscr{R}_3(d)|}{p}$$

Thus, $q^2 < \frac{|\mathscr{R}_3(d)|}{p}$, and this implies the lemma. □

Now, we choose ℓ as in the previous lemma, and we apply lemma 5.7.1 to $\mathcal{B} = \mathcal{B}_\delta$. We deduce that the average over $\mathscr{R}_3(d)$ of $\frac{|\Gamma_{\mathbf{x}}^{(\ell)}\cap\mathcal{B}_\delta|}{2\ell+1}$ satisfies :

$$\frac{1}{|\mathscr{R}_3(d)|} \sum_{\mathbf{x}\in\mathscr{R}_3(d)} \frac{|\Gamma_{\mathbf{x}}^{(\ell)} \cap \mathcal{B}_\delta|}{2\ell+1} = \frac{|\mathrm{red}_q^{-1}(\mathcal{B}_\delta)|}{|\mathscr{R}_3(d)|}$$

Now, for all $\overline{\mathbf{x}} \in \mathcal{B}_\delta$, we have (by definition of $\mathcal{B}_\delta$)

$$\frac{|\mathrm{red}_q^{-1}(\overline{\mathbf{x}})|}{|\mathscr{R}_3(d)|} > (1+\delta)\frac{1}{|\mathscr{R}_3(d,q)|}$$

Informally, this means that the points of $\mathscr{R}_3(d)$ tend to reduce to $\overline{\mathbf{x}}$ modulo q a little bit more often than what would be the perfect equidistribution behaviour. Now since $\mathrm{red}_q^{-1}(\mathcal{B}_\delta) = \bigsqcup_{\overline{\mathbf{x}}\in\mathcal{B}_\delta} \mathrm{red}_q^{-1}(\overline{\mathbf{x}})$, we deduce that

$$\frac{|\mathrm{red}_q^{-1}(\mathcal{B}_\delta)|}{|\mathscr{R}_3(d)|} > (1+\delta)\frac{|\mathcal{B}_\delta|}{|\mathscr{R}_3(d,q)|}$$

Hence :

$$\frac{1}{|\mathscr{R}_3(d)|} \sum_{\mathbf{x}\in\mathscr{R}_3(d)} \frac{|\Gamma_{\mathbf{x}}^{(\ell)} \cap \mathcal{B}_\delta|}{2\ell+1} > (1+\delta)\frac{|\mathcal{B}_\delta|}{|\mathscr{R}_3(d,q)|}$$

But we started this proof by contradiction by assuming $|\mathcal{B}_\delta| > \eta|\mathscr{R}_3(d,q)|$, so

$$\frac{1}{|\mathscr{R}_3(d)|}\sum_{\mathbf{x}\in\mathscr{R}_3(d)}\frac{|\Gamma_{\mathbf{x}}^{(\ell)}\cap\mathcal{B}_\delta|}{2\ell+1} > \frac{|\mathcal{B}_\delta|}{|\mathscr{R}_3(d,q)|}+\delta\eta \tag{22}$$

We will derive a very basic consequence of this inequality, but since the notations are a bit heavy, we state what we use in an independent lemma.

Lemma 5.7.3. *Let $x_1,\dots,x_n\in[0,1]$, and let A,B be two positive real numbers. Suppose that*

$$\frac{1}{n}\sum_{i=1}^{n}x_i > A+B$$

Then the number of indices i such that $x_i > \frac{B}{2}+A$ is strictly larger than $\frac{B}{2}n$.

Proof. We have

$$\frac{1}{n}\sum_{i=1}^{n}x_i \;=\; \frac{1}{n}\sum_{\substack{1\leqslant i\leqslant n\\ x_i>\frac{B}{2}+A}}x_i \;+\; \frac{1}{n}\sum_{\substack{1\leqslant i\leqslant n\\ x_i\leqslant\frac{B}{2}+A}}x_i$$

Now, if the number of terms of the first sum on the right hand side is less than or equal to $\frac{B}{2}n$, then we have :

$$\frac{1}{n}\sum_{\substack{1\leqslant i\leqslant n\\ x_i>\frac{B}{2}+A}}x_i \;\leqslant\; \frac{B}{2}$$

using the fact that the x_i's are less than or equal to 1. Since the second sum is less than or equal to $\frac{B}{2}+A$, we conclude that

$$\frac{1}{n}\sum_{i=1}^{n}x_i \leqslant A+B.$$

This contradicts the assumption. Thus, the number of indices i such that $x_i > \frac{B}{2}+A$ is strictly larger than $\frac{B}{2}n$.

□

§5.7.2 Conclusion of the proof

We apply lemma 5.7.3 to our inequality (22), and derive that the number of $\mathbf{x}\in\mathscr{R}_3(d)$ such that

$$\frac{|\Gamma_{\mathbf{x}}^{(\ell)}\cap\mathcal{B}_\delta|}{2\ell+1} > \frac{|\mathcal{B}_\delta|}{|\mathscr{R}_3(d,q)|}+\frac{\delta\eta}{2} \tag{23}$$

is strictly larger than $\frac{\delta\eta}{2}|\mathscr{R}_3(d)|$. Let us denote by L the set of $\mathbf{x}$'s in $\mathscr{R}_3(d)$ such that the inequality (23) holds :

$$L := \left\{\mathbf{x}\in\mathscr{R}_3(d),\ \frac{|\Gamma_{\mathbf{x}}^{(\ell)}\cap\mathcal{B}_\delta|}{2\ell+1} > \frac{|\mathcal{B}_\delta|}{|\mathscr{R}_3(d,q)|}+\frac{\delta\eta}{2}\right\}$$

We just proved that $|L| > \frac{\delta\eta}{2}|\mathscr{R}_3(d)|$. Now, we apply the lower bound from theorem 4.4.1 for the size of $\mathscr{R}_3(d)$. This gives us : for any $\varepsilon>0$,

$$|L| \gg_{\varepsilon,\delta,\eta} d^{\frac{1}{2}-\varepsilon}$$

Note that we can interpret (23) as follows :
if $\mathbf{x}$ is such that (23) holds, this means that the walk $\Gamma_{\mathbf{x}}^{(\ell)}$ is exceptional in the sense that it spends too much time in $|\mathcal{B}_\delta|$, compared to what we expect to be the typical behaviour of a walk on $\mathscr{R}_3(d,q)$.

Indeed, $\frac{|\Gamma_{\mathbf{x}}^{(\ell)} \cap \mathcal{B}_\delta|}{2\ell+1}$ is the amount of time that the walk $\Gamma_{\mathbf{x}}^{(\ell)}$ spends inside $\mathcal{B}_\delta$, and we compare it with the size of $|\mathcal{B}_\delta|$ inside $\mathscr{R}_3(d,q)$. It is natural to think that since the graph $\mathscr{R}_3(d,q)$ has "good connectivity properties", a typical walk on $\mathscr{R}_3(d,q)$ will spend half of the time in a subset of $\mathscr{R}_3(d,q)$ made of $\frac{|\mathscr{R}_3(d,q)|}{2}$ points. The fact that $\mathscr{R}_3(d,q)$ has "good connectivity properties" follows from theorem 5.6.1, but we did not have time to explore the wide subject of expander graphs, so this phrase will remain between quotes.

Thus, we have proved that if we assume for a contradiction that $|\mathcal{B}_\delta| > \eta|\mathscr{R}_3(d,q)|$, then there are at least $|L|$ points $\mathbf{x}$ in $\mathscr{R}_3(d)$ whose corresponding trajectory is exceptional in the sense of (23). Moreover, $|L|$ satisfies : for any $\varepsilon > 0$,

$$|L| \gg_{\varepsilon,\delta,\eta} d^{\frac{1}{2}-\varepsilon}$$

So, informally : *essentially all the points in $\mathscr{R}_3(d)$ give trajectories $\Gamma_{\mathbf{x}}^{(\ell)}$ that are exceptional.*

Now, we are going to use corollary 5.5.3 to deduce that many trajectories on $\mathscr{R}_3(d,q)$ are exceptional, and in fact, too many : this will contradict the large deviation equality from corollary 5.6.2, and conclude the proof.

For the moment, we just know that essentially all the points $\mathbf{x}$ in $\mathscr{R}_3(d)$ give exceptional truncated walks $\Gamma_{\mathbf{x}}^{(\ell)}$. But the problem could be that they all give the same truncated walk, so that this would not give us any information on the number of trajectories with this exceptional behaviour. This is why it is natural to use corollary 5.5.3 to prove that in fact, different points essentially lead to different truncated walks.

Notation :

- Let us denote by Λ_ℓ the set of non-backtracking marked walks of length 2ℓ on $\mathscr{R}_3(d,q)$, in the sense of definition 5.4.2.
- Let us denote by M the set of exceptional paths of length 2ℓ on $\mathscr{R}_3(d,q)$:

$$M := \left\{ \Gamma^{(\ell)} \in \Lambda_\ell \text{ such that } \frac{|\Gamma^{(\ell)} \cap \mathcal{B}_\delta|}{2\ell+1} > \frac{|\mathcal{B}_\delta|}{|\mathscr{R}_3(d,q)|} + \frac{\delta\eta}{2} \right\}$$

Note that in the set M, some paths may not arise as the trajectory $\Gamma_{\mathbf{x}}^{(\ell)}$ attached to a point of $\mathscr{R}_3(d)$, we really take into account all the possible paths in the sense of definition 5.4.2.

Lemma 5.7.4. *The fact that $|L| \gg_{\varepsilon,\delta,\eta} d^{\frac{1}{2}-\varepsilon}$ implies that :*

$$|M| \gg_{\varepsilon,\delta,\eta} d^{\frac{1}{2}-\varepsilon}$$

Proof. We consider the map

$$\begin{array}{rccc} f & : & L & \to & M \\ & & \mathbf{x} & \mapsto & \Gamma_{\mathbf{x}}^{(\ell)} \end{array}$$

which maps a point in L to its attached truncated walk (which is in M, by definition of L). This map is not injective in general, but if we denote by $\sim$ the equivalence relation on L defined as follows :

$$\mathbf{x} \sim \mathbf{x}' \iff \Gamma_{\mathbf{x}}^{(\ell)} = \Gamma_{\mathbf{x}'}^{(\ell)}$$

then f induces an injective map

$$\begin{array}{rccc} \overline{f} & : & L/\sim & \to & M \\ & & [\mathbf{x}] & \mapsto & \Gamma_{\mathbf{x}}^{(\ell)} \end{array}$$

(here we denoted by $[\mathbf{x}]$ the equivalence class of $\mathbf{x}$, that is : $[\mathbf{x}] = \{\mathbf{x}' \in L,\ \mathbf{x}' \sim \mathbf{x}\}$). This implies that

$$|M| \geqslant |L/\sim|\,.$$

Therefore, it suffices to prove that for any $\varepsilon > 0$, $|L/\!\sim| \gg_{\varepsilon,\delta,\eta} d^{\frac{1}{2}-\varepsilon}$. Let us take $\{\mathbf{x}_1, \dots, \mathbf{x}_r\}$ a set of representatives for $L/\!\sim$, and let us denote by $X_i := [\mathbf{x}_i]$ the equivalence class of each of these points. Note that $r = |L/\!\sim|$ is the quantity we want to bound from below.

We have

$$d^{\frac{1}{2}-\varepsilon} \ll_{\varepsilon,\delta,\eta} |L| = \sum_{i=1}^{r} |X_i| \leqslant \sqrt{r}\sqrt{\sum_{i=1}^{r} |X_i|^2}$$

(where the last inequality follows from Cauchy-Schwarz inequality), hence :

$$d^{\frac{1}{2}-\varepsilon} \ll_{\varepsilon,\delta,\eta} \sqrt{r}\sqrt{\sum_{i=1}^{r} |X_i|^2} \tag{24}$$

On the other hand, if we denote by C the number of pairs $(\mathbf{x}, \mathbf{x}')$ yielding the same truncated trajectory :

$$C := \left|\{(\mathbf{x}, \mathbf{x}') \in \mathscr{R}_3(d),\ \Gamma_{\mathbf{x}}^{(\ell)} = \Gamma_{\mathbf{x}'}^{(\ell)}\}\right|,$$

corollary 5.5.3 tells us that

$$C \ll_{\varepsilon} d^{\frac{1}{2}+\varepsilon}$$

(more precisely, we use the remark following corollary 5.5.3, and our choice of an integer ℓ satisfying (21)).
Now,

$$C = \sum_{\mathbf{x}\in\mathscr{R}_3(d)} \sum_{\substack{\mathbf{x}'\in\mathscr{R}_3(d)\\ \Gamma_{\mathbf{x}'}^{(\ell)}=\Gamma_{\mathbf{x}}^{(\ell)}}} 1 \geqslant \sum_{\mathbf{x}\in L} \sum_{\substack{\mathbf{x}'\in L\\ \Gamma_{\mathbf{x}'}^{(\ell)}=\Gamma_{\mathbf{x}}^{(\ell)}}} 1$$

and

$$\sum_{\mathbf{x}\in L} \sum_{\substack{\mathbf{x}'\in L\\ \Gamma_{\mathbf{x}'}^{(\ell)}=\Gamma_{\mathbf{x}}^{(\ell)}}} 1 = \sum_{i=1}^{r} \sum_{\mathbf{x}\in X_i} \underbrace{\sum_{\substack{\mathbf{x}'\in L\\ \Gamma_{\mathbf{x}'}^{(\ell)}=\Gamma_{\mathbf{x}}^{(\ell)}}} 1}_{|X_i| \text{ terms}}$$

hence :

$$\sum_{\mathbf{x}\in L} \sum_{\substack{\mathbf{x}'\in L\\ \Gamma_{\mathbf{x}'}^{(\ell)}=\Gamma_{\mathbf{x}}^{(\ell)}}} 1 = \sum_{i=1}^{r} |X_i|^2$$

Thus,

$$\sum_{i=1}^{r} |X_i|^2 \leqslant C \ll_{\varepsilon} d^{\frac{1}{2}+\varepsilon} \tag{25}$$

Combining (24) and (25), we obtain :

$$d^{\frac{1}{2}-\varepsilon} \ll_{\varepsilon,\delta,\eta} \sqrt{r}\sqrt{\sum_{i=1}^{r} |X_i|^2} \ll_{\varepsilon} \sqrt{r}\sqrt{d^{\frac{1}{2}+\varepsilon}}$$

which implies

$$r \gg_{\varepsilon,\delta,\eta} d^{\frac{1}{2}-3\varepsilon}$$

Since this holds for any $\varepsilon > 0$, this 3ε is not a problem, and we get the conclusion, because for any $\varepsilon > 0$,

$$d^{\frac{1}{2}-\varepsilon} \ll_{\varepsilon,\delta,\eta} r = |L/\!\sim| \leqslant |M|.$$

□

Thus, the number $|M|$ of marked truncated paths $\Gamma^{(\ell)}$ on $\mathscr{R}_3(d,q)$ such that (23) holds satisfies : for any $\varepsilon > 0$,

$$|M| \gg_{\varepsilon,\delta,\eta} d^{\frac{1}{2}-\varepsilon}$$

But on the other hand, we are going to find an upper bound for $|M|$. The total number of non-backtracking marked paths of length 2ℓ on the graph $\mathscr{R}_3(d,q)$ equals

$$|\Lambda_\ell| = |\mathscr{R}_3(d,q)|(p+1)p^{2\ell-1}$$

(the first factor corresponds to the choice of a marked point, the second to the choice of a first edge starting from our marked point, so we have $p+1 = |\mathcal{A}_p|$ choices, and then for all the other edges we only have p choices since we cannot take the edge which would make us backtrack).
As for any $\varepsilon > 0$, $|\mathscr{R}_3(d,q)| \ll_\varepsilon q^{2+\varepsilon}$ (see proposition 5.3.2) and $q^2 p^{2\ell} \leqslant p|\mathscr{R}_3(d)|$ (by assumption (21)), we deduce that

$$|\Lambda_\ell| = |\mathscr{R}_3(d,q)|(p+1)p^{2\ell-1} \ll_\varepsilon d^{\frac{1}{2}+\varepsilon} \tag{26}$$

Now, among all those non-backtracking paths of length 2ℓ, the proportion satisfying (23) is at most $c_1 \exp(-c_2\ell)$, where $c_1, c_2 > 0$ depend only on δ and η (this comes from corollary 5.6.2). Explicitly, this means that

$$\frac{|M|}{|\Lambda_\ell|} \leqslant c_1 \exp(-c_2\ell)$$

As a purely technical consequence, we obtain the following upper bound for $|M|$

Lemma 5.7.5. *There exists $\tau := \tau(\delta,\eta) > 0$, depending only on δ and η, such that for any $\varepsilon > 0$,*

$$|M| \ll_{\varepsilon,\delta,\eta} d^{\frac{1}{2}+\varepsilon-\tau}$$

Proof. see below, in order not to let technicalities overtake the conclusion of the proof. □

Thanks to this upper bound, we derive that for any $\varepsilon > 0$,

$$d^{\frac{1}{2}-\varepsilon} \ll_{\varepsilon,\delta,\eta} |M| \ll_{\varepsilon,\delta,\eta} d^{\frac{1}{2}-\tau+\varepsilon}$$

and this gives a contradiction for d large enough. Indeed, if we take $\varepsilon := \frac{\tau}{3}$ (for instance), then :

$$d^{\frac{1}{2}-\frac{\tau}{3}} \ll_{\delta,\eta} |M| \ll_{\delta,\eta} d^{\frac{1}{2}-\frac{2\tau}{3}}$$

for all $d \geqslant 2$ admissible and square-free. This is impossible for d large enough, and this concludes the proof. □

Remark. *We used theorem 4.4.1 to estimate $|\mathscr{R}_3(d)|$, and this theorem relied on Siegel's theorem, where the constant is ineffective. Thus, this proof does not provide an effective equidistribution rate. With this approach, one does not know from which value of d the fraction of $\overline{\mathbf{x}}$ such that $|\mathrm{dev}_d(\overline{\mathbf{x}})| > \delta$ falls below η.*

Proof of lemma 5.7.5 : Since we chose ℓ as in equation (21), we have $\frac{1}{p}|\mathscr{R}_3(d)| < q^2 p^{2\ell}$. Besides, $d^{\frac{1}{2}-\varepsilon} \ll_\varepsilon |\mathscr{R}_3(d)|$, so we obtain that for any $\varepsilon > 0$, there exists a constant $C(\varepsilon)$, depending only on ε, such that

$$C(\varepsilon) d^{\frac{1}{2}-\varepsilon} \leqslant q^2 p^{2\ell}$$

Taking logarithms, this yields :

$$\ln(C(\varepsilon)) + \left(\frac{1}{2} - \varepsilon\right)\ln(d) - 2\ln(q) \leqslant 2\ell \ln(p)$$

Now, we use the fact that $q^2 \leqslant d^{\frac{1}{2}-\nu}$ to deduce that $2\ln(q) \leqslant \left(\frac{1}{2} - \nu\right)\ln(d)$. Thus,

$$\ln(C(\varepsilon)) + \left(\frac{1}{2} - \varepsilon\right)\ln(d) - \left(\frac{1}{2} - \nu\right)\ln(d) \leqslant 2\ell \ln(p)$$

which implies that

$$\ell \geqslant \frac{\ln(C(\varepsilon)) + (\nu - \varepsilon)\ln(d)}{2p}$$

Therefore, the inequality

$$\frac{|M|}{|\Lambda_\ell|} \leqslant c_1 \exp(-c_2 \ell)$$

coming from corollary 5.6.2 implies that

$$|M| \leqslant c_1 \exp\left(-c_2 \frac{\ln(C(\varepsilon)) + (\nu - \varepsilon)\ln(d)}{2p}\right) |\Lambda_\ell|$$

Thus, if we put

$$\tau := \frac{c_2 \nu}{2p} > 0$$

it depends only on δ, η (because c_2 only depends on δ and η), and the previous inequality shows that :

$$|M| \ll_{\varepsilon,\delta,\eta} d^{-\tau} d^{c_2 \varepsilon/(2p)} |\Lambda_\ell|$$

Finally, we also know from equation (26) that

$$|\Lambda_\ell| \ll_\varepsilon d^{\frac{1}{2}+\varepsilon}$$

hence

$$|M| \ll_{\varepsilon,\delta,\eta} d^{\frac{1}{2}-\tau+\left(\frac{c_2}{2p}+1\right)\varepsilon}$$

Since this holds for any $\varepsilon > 0$, we can conclude that for any $\varepsilon > 0$,

$$|M| \ll_{\varepsilon,\delta,\eta} d^{\frac{1}{2}+\varepsilon-\tau}$$

□

Appendix A.

Classical facts about Dirichlet characters and their L-functions

Our presentation of the facts on Dirichlet characters follows a lot [Kow04].

Given a group G, a character of G is just a group homomorphism from G to $\mathbf{C}^\times$. We denote by $\widehat{G}$ the set of characters :

$$\widehat{G} := \mathrm{Hom}_{\mathrm{grp}}(G, \mathbf{C}^\times)$$

It is a group for the following law : given $\varphi, \psi \in \widehat{G}$, define $\varphi\psi$ as $g \in G \mapsto \varphi(g)\psi(g)$ (endowed with this law, $\widehat{G}$ is a subgroup of the group of functions from G to $\mathbf{C}^\times$). We call it the dual of G. The unit element in $\widehat{G}$ is the so-called trivial character : the character which is constant equal to 1. Note that even if G is not abelian, $\widehat{G}$ is always an abelian group. Thus, when G is not abelian, $\widehat{G}$ is not isomorphic to G. What is less clear is the fact that when G is a finite abelian group, G and $\widehat{G}$ are isomorphic. We will not prove it in detail here, but let us say a few words about the proof : the idea is that it is not hard to see that when G is a finite cyclic group, $G \simeq \widehat{G}$, and then we use the struture theorem of finite abelian groups to decompose any such group as a direct product of cyclic groups. Let us also remark that as long as G is a finite group, the characters of G take values in the $|G|$-th roots of unity in $\mathbf{C}^\times$.

Characters of finite abelian groups satisfy orthogonality relations that are very useful in analytic number theory.

Theorem A.1 (Orthogonality of characters)**.** *Let G be a finite abelian group, with unit element denoted by e.*

(i) *For all $\chi \in \widehat{G}$, we have*

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| \text{ if } \chi = 1 \text{ (i.e. if } \chi \text{ is the trivial character)} \\ 0 \quad \text{if } \chi \neq 1 \end{cases}$$

(ii) *For all $x \in G$, we have*

$$\sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} |G| \text{ if } x = e \\ 0 \quad \text{if } x \neq e \end{cases}$$

The main examples of characters we will encounter are the following :

- One can take the group G to be $(\mathbf{Z}/n\mathbf{Z}, +)$, and in this case the characters of G are called the additive characters modulo n
- Another example that will be of interest to us is the case where G is the group of units $(\mathbf{Z}/n\mathbf{Z})^\times$. Then a character of G is called a multiplicative character modulo n.

Definition A.2. *Let q be an integer larger than or equal to 1. Given a multiplicative character modulo q (i.e. a group homomorphism χ: $(\mathbf{Z}/q\mathbf{Z})^\times \to \mathbf{C}^\times$), we defined the so-called "Dirichlet character" attached to χ as follows :*

$$n \in \mathbf{Z} \mapsto \begin{cases} \chi(n \bmod q) \text{ if } \gcd(n, q) = 1 \\ 0 \text{ otherwise} \end{cases}$$

In other words, if the reduction of n modulo q is in $(\mathbf{Z}/q\mathbf{Z})^\times$, then we map n to $\chi(n \bmod q)$, and if not, we just map n to 0. We will still denote by χ this Dirichlet character, and we say that it is a "Dirichlet character modulo q". It follows from the definition that χ defines a completely multiplicative function on $\mathbf{Z}$:

$$\forall m, n \in \mathbf{Z},\ \chi(mn) = \chi(m)\chi(n)$$

and that χ is q-periodic. We say that χ is a real Dirichlet character if it takes values in $\mathbf{R}$.

Remark. *Even if we take for χ the trivial multiplicative character modulo q (which is constant equal to 1), the attached Dirichlet character is not constant, since it takes the value 0 for every integer which is not prime to q.*

If we start from a multiplicative character χ modulo q, we can construct a character modulo dq for any integer $d \geqslant 1$ as follows :
The natural ring homomorphism $\mathbf{Z}/dq\mathbf{Z} \to \mathbf{Z}/q\mathbf{Z}$ induces a group homomorphism between the groups of units, say $\varphi\colon\ (\mathbf{Z}/dq\mathbf{Z})^\times \to (\mathbf{Z}/q\mathbf{Z})^\times$, and then $\chi' := \chi \circ \varphi$ defines a multiplicative character modulo dq. We say that χ' is induced by χ.

Definition A.3. *A multiplicative character χ modulo q is said to be primitive if it is not induced by a character modulo q' for some $q' \mid q$ a proper divisor of q. Then we say that q is the conductor of χ.*

In fact, any Dirichlet character χ is induced by a unique primitive character, say χ', and we define the conductor of χ to be the conductor of χ'.

Let us state the following simple corollary of the orthogonality of characters in the context of our Dirichlet characters (we use this lemma in our proof of Dirichlet class number formula).

Lemma A.4. *If χ is a non-trivial Dirichlet character modulo q, and $I \subseteq \mathbf{N}$ is an interval of $\mathbf{N}$, then*

$$\left|\sum_{i \in I} \chi(i)\right| \leqslant \varphi(q)$$

where φ is the Euler's totient function.

Proof. Let us write $I = \{m, m+1, \ldots, m+n\}$. Then by orthogonality of characters and the fact that we extend χ by 0 at the integers not prime to q, we have

$$\sum_{k=m}^{m+q-1} \chi(k) = 0, \sum_{k=m+q}^{m+2q-1} \chi(k) = 0, \ldots$$

Therefore, in the sum over I, we can forget all the intervals $\{m+jq, \ldots, m+(j+1)q-1\}$ for all $j \in \mathbf{N}$ such that $m+(j+1)q-1 \leqslant m+n$. Then we are reduced to the case where the length of I is strictly less than q. And in this case the sum consists of at most $\varphi(q)$ non-zero terms, which all have absolute value equal to 1. □

Now let us give the definition and some classical results about the L-functions attached to Dirichlet characters. The proofs can be found in [Ser70] or [Kow04] for instance.

Definition A.5. *Let $q \geqslant 1$ be an integer, and let χ be a Dirichlet character modulo q. The L-function associated with χ is the holomorphic function define for $s \in \mathbf{C}$ such that $\mathrm{Re}(s) > 1$ by :*

$$L(s, \chi) := \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}$$

Since for all $n \in \mathbf{Z}$, $|\chi(n)| = 0$ or 1, this series is indeed absolutely convergent for any s with $\mathrm{Re}(s) > 1$.

Proposition A.6. *These L-functions admit an Euler product expansion : namely, with the notations of the previous definition, one has :*

$$\text{for all } s \in \mathbf{C} \text{ such that } \mathrm{Re}(s) > 1,\ L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

where the product ranges over the prime numbers.

A useful tool in the study of L-functions is the summation by part :

Lemma A.7. *Let $(a_n)_{n\geqslant 1}$ be a sequence of complex numbers, and let $f\colon]0,+\infty[\to \mathbf{C}$ be a function with continuous derivative on $]0,+\infty[$. For all $x\geqslant 1$, let us denote by $A(x)$ the truncated series with general term a_n, that is :*

$$A(x) := \sum_{1\leqslant n\leqslant x} a_n$$

Then, for all $x\geqslant 1$:

$$\sum_{1\leqslant n\leqslant x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)\mathrm{d}t$$

Moreover, if $A(x)f(x) \underset{x\to+\infty}{\longrightarrow} 0$, and if the series or the integral converges, then

$$\sum_{n=1}^{+\infty} a_n f(n) = -\int_1^{+\infty} A(t)f'(t)\mathrm{d}t$$

Proof. See [Kow04], lemme 2.2.1. page 29. □

One can use this summation by part, together with lemma A.4 to derive the following important property :

Proposition A.8. *When χ is non-trivial, the series defining $L(\cdot,\chi)$ converges on the half plane*

$$\{s\in\mathbf{C} \mid \mathrm{Re}(s) > 0\}$$

Proof. See [Kow04], remarque 3.2.6. page 61. □

In particular, this proposition allows us to speak about the value of $L(1,\chi)$, since the L-function is well defined at 1.

Another consequence of lemma A.7 is the following upper bound for $L(1,\chi)$ that we use in section 4.4 to estimate the size of $\mathscr{R}_3(d)$.

Proposition A.9. *Let $q\geqslant 2$, and let χ be a non-trivial Dirichlet character modulo q. Then*

$$|L(1,\chi)| \leqslant \ln(q) + 1$$

Proof. We apply lemma A.7 to $f(x) = \frac{1}{x}$ and $a_n = \chi(n)$. By lemma A.4, we have that for all $x\geqslant 1$, $|A(x)| \leqslant \varphi(q)$. From this, it is easy to check that the assumptions of the last part of lemma A.7 are satisfied and to derive the following equality :

$$\sum_{n=1}^{+\infty} \frac{\chi(n)}{n} = L(1,\chi) = \int_1^{+\infty} \left(\sum_{1\leqslant n\leqslant t} \chi(n)\right) \frac{1}{t^2}\mathrm{d}t$$

Then we split the integral in two parts, one from 1 to q, and the other one from q to $+\infty$. In the first integral, we remark that for all $t\leqslant q$, we have

$$\left|\sum_{1\leqslant n\leqslant t} \chi(n)\right| \leqslant t$$

and in the second integral we just bound the absolute value of the sum by q. Then

$$|L(1,\chi)| \leqslant \int_1^q \frac{1}{t}\mathrm{d}t + q\int_q^{+\infty} \frac{1}{t^2}\mathrm{d}t = \ln(q) + 1$$

□

Appendix B.

Definition of the Kronecker symbol

First we recall the definition of the Legendre symbol for odd primes. if p is an odd prime number, we denote by $\left(\mathbf{F}_p^\times\right)^2$ the set $\{x^2,\ x \in \mathbf{F}_p^\times\}$. Then, for all $a \in \mathbf{Z}$, we define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows :

$$\left(\frac{a}{p}\right) = \begin{cases} +1 \text{ if } \overline{a} \in \left(\mathbf{F}_p^\times\right)^2 \\ -1 \text{ if } \overline{a} \in \mathbf{F}_p^\times \setminus \left(\mathbf{F}_p^\times\right)^2 \\ 0 \quad \text{if } \overline{a} = 0 \text{ in } \mathbf{F}_p \end{cases}$$

(where $\overline{a}$ denotes the class of a modulo p).

Proposition B.1. *$\left(\frac{\cdot}{p}\right)$ is a Dirichlet character modulo p.*

It satisfies the famous quadratic reciprocity law :

Theorem B.2 (Quadratic reciprocity law)**.** *If p, q are two odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \quad \text{and} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Proof. There is a nice proof relying on the reduction of quadratic forms over $\mathbf{R}$ and over finite fields in [CG17]. □

We extend the symbol to the denominator 2, but we have to restrict the numerator. Proposition 2.1.8 is our motivation to set these values for $\left(\frac{D}{2}\right)$.

Definition B.3. *Let D be a discriminant (i.e. $D \in \mathbf{Z}$ and $D \equiv 0, 1 \bmod 4$). We set :*

$$\left(\frac{D}{2}\right) = \begin{cases} +1 \text{ if } D \equiv 1 \bmod 8 \\ -1 \text{ if } D \equiv 5 \bmod 8 \\ 0 \quad \text{if } D \equiv 0 \bmod 4 \end{cases}$$

Finally, we extend this symbol for any positive integer n by setting $\left(\frac{D}{1}\right) := 1$ and if $n \geqslant 2$ has the factorization into prime factors $n = 2^\alpha p_1^{\alpha_1} \dots p_n^{\alpha_n}$

$$\left(\frac{D}{n}\right) := \left(\frac{D}{2}\right)^\alpha \left(\frac{D}{p_1}\right)^{\alpha_1} \dots \left(\frac{D}{p_n}\right)^{\alpha_n}$$

The symbol $\left(\frac{D}{\cdot}\right)$ is called the Kronecker symbol. We will sometimes denote it by χ_D. Note that it is only well defined when D is a discriminant, and when n is positive. It can be extended to negative values of n (see [Hec81]), but we will not need it. By definition, the Kronecker symbol is completely multiplicative, but to see it as a Dirichlet character modulo D, we need to show that the value $\left(\frac{D}{n}\right)$ only depends on the class of n modulo D.

Proposition B.4. *If m, n are two positive integers such that $n \equiv m \bmod D$, then*

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right).$$

In particular, $\left(\frac{D}{\cdot}\right)$ represents a Dirichlet character modulo D for positive integers n.

Proof. See [Hec81], theorem 137. It is in the proof of this fact that we see that it is important to assume $D \equiv 0, 1 \bmod 4$. □

Proposition B.5. *If D is a fundamental discriminant, then the Kronecker symbol $\left(\frac{D}{\cdot}\right)$ is a real primitive Dirichlet character modulo $|D|$.*

Proof. See [Str08] theorem 4.35. □

Appendix C.

A correspondence between right ideals of $\mathcal{M}_n(K)$ and subspaces of K^n

Let us give a more detailed explanation of the correspondence between right ideals of $\mathcal{M}_2(\mathbf{F}_p)$ and subspaces of $\mathbf{F}_p^2$ that we used in the proof of proposition 5.3.1.

Let K be a field, and let $n \geqslant 1$. Let us denote by $\mathcal{I}_n(K)$ the set of right ideals of $\mathcal{M}_n(K)$, and by $\mathcal{V}_n(K)$ the set of vector-subspaces of K^n. Define

$$\begin{array}{rccc} S & : & \mathcal{I}_n(K) & \to & \mathcal{V}_n(K) \\ & & I & \mapsto & \sum_{u\in I} \mathrm{Im}(u) \end{array}$$

and

$$\begin{array}{rccc} T & : & \mathcal{V}_n(K) & \to & \mathcal{I}_n(K) \\ & & V & \mapsto & \{u \in \mathcal{M}_n(K) \mid \mathrm{Im}(u) \subseteq V\} \end{array}$$

It is easy to see that if $V \in \mathcal{V}_n(K)$, then $T(V)$ is indeed a right ideal of $\mathcal{M}_n(K)$, so that the map T is well defined. Let us also remark that when $I \in \mathcal{I}_n(K)$, we can rewrite $S(I)$ differently. Denote by $(e_1, \dots, e_n)$ the canonical basis of K^n, then

$$S(I) = \sum_{u\in I} Ku(e_1) = \sum_{u\in I} Ku(e_2) = \cdots$$

Indeed, we have $\sum_{u\in I} Ku(e_1) \subseteq \sum_{u\in I} \mathrm{Im}(u) = S(I)$. To prove the converse, it suffices to prove that for all $u \in I$, $\mathrm{Im}(u) \subseteq \sum_{v\in I} Kv(e_1)$. Let $y = u(x) \in \mathrm{Im}(u)$ for some $u \in I$. Then we can find $w \in \mathcal{M}_n(K)$ such that $w(e_1) = x$, and then $y = (u \circ w)(e_1) \in \sum_{v\in I} Kv(e_1)$ since $u \circ w \in I$ because I is a right ideal of $\mathcal{M}_n(K)$.

- We have $T \circ S = \mathrm{id}_{\mathcal{I}_n(K)}$: let $I \in \mathcal{I}_n(K)$ and let us denote by $V := S(I)$ and $I' := T(S(I))$. Then if $u \in I$, $\mathrm{Im}(u) \subseteq V = \sum_{v\in I} \mathrm{Im}(v)$, so $u \in T(V) = I'$. This proves that $I \subseteq I'$. Conversely, if $u \in I'$, then $u'(e_1) \in V$, so we can write it $u_1(e_1)$ for some $u_1 \in I$. Similarly, $u'(e_2) = u_2(e_2)$ for some $u_2 \in I$, and so on. In the end, we can write $u' = u_1 \circ E_{1,1} + u_2 \circ E_{2,2} + \cdots + u_n E_{n,n} \in I$ since I is a right ideal. This proves that $I' \subseteq I$, hence the conclusion.
- We have $S \circ T = \mathrm{id}_{\mathcal{V}_n(K)}$: let $V \in \mathcal{V}_n(K)$, and let us denote by $I = T(V)$ and $V' = S(T(V))$. By definition of I, for all $u \in I$, $\mathrm{Im}(u) \subseteq V$, so $V' = \sum_{u\in I} \mathrm{Im}(u) \subseteq V$. Conversely, if $x \in V$, then we can consider $u \in \mathcal{M}_n(K)$ such that $u(e_1) = x$ and for all $i \geqslant 2$, $u(e_i) = 0$. Then $\mathrm{Im}(u) \subseteq V$, so $u \in I$. Thus, $x \in \mathrm{Im}(u)$ for some $u \in I$, so $x \in V'$.

Thanks to these two points, we deduce that T and S are two bijections inverse one to the other. They give us a one to one correspondence between the right ideals of $\mathcal{M}_n(K)$ and the vector-subspaces of K^n.

Moreover, the bijection T raises the index to the power n, that is : if $V \subseteq K^n$ is a sub-vector space of index d, then $I := T(V)$ is a right ideal of index d^n inside $\mathcal{M}_n(K)$. Indeed, consider the map

$$\begin{array}{rccc} \psi & : & \mathcal{M}_n(K) & \to & (K^n/V)^n \\ & & u & \mapsto & (u(e_1) + V, \dots, u(e_n) + V) \end{array}$$

It is a surjective K-linear map, and its kernel is exactly the set of $u \in \mathcal{M}_n(K)$ such that $\mathrm{Im}(u) \subseteq V$, that is : I. Thus, we have an isomorphism of K-vector spaces :

$$\mathcal{M}_n(K)/I \simeq (K^n/V)^n$$

and the statement on the index follows from this fact. For instance (and this is what we use in the proof of proposition 5.3.1), under this correspondence, the right ideals of $\mathcal{M}_2(\mathbf{F}_p)$ of index p^2 correspond to the vector subspaces of $\mathbf{F}_p^2$ of index p.

References

[Bha04] Manjul Bhargava. *Higher composition laws I : A new view on gauss composition, and quadratic generalizations.* Annals of mathematics 159 (1), 2004.

[Bri] Olivier Brinon. *Théorie des nombres.* Notes of a Master 1 course at the University of Bordeaux, available at https://www.math.u-bordeaux.fr/~obrinon/enseignement/TAN/tan.pdf.

[Bri20] Olivier Brinon. *Number theory.* Notes of a Master 2 course at the University of Bordeaux, available at https://www.math.u-bordeaux.fr/~obrinon/enseignement/cl/cl.pdf, 2019/2020.

[CG17] Philippe Caldero and Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries.* Calvage & Mounet, 2017.

[Dav80] Harold Davenport. *Multiplicative number theory, 2^{nd} edition.* Springer-Verlag, GTM 74, 1980.

[Duk88] W. Duke. *Hyperbolic distribution problems and half-integral weight Maass forms.* Inventiones Mathematicae 92 (1), 1988.

[EMV10] Jordan S. Ellenberg, Philippe Michel, and Akshay Venkatesh. *Linnik's ergodic method and the distribution of integer points on spheres.* https://arxiv.org/abs/1001.0897, 2010.

[EW05] Graham Everest and Thomas Ward. *An Introduction to Number Theory.* Springer-Verlag, GTM 232, 2005.

[FG90] O.M. Fomenko and E.P. Golubeva. *Asymptotic distribution of lattice points on the three-dimensional sphere.* Journal of Soviet Mathematics 52, 1990.

[Gam06] Adam Gamzon. *The Hasse-Minkowski Theorem.* Honors Scholar Theses. 17. available at https://opencommons.uconn.edu/srhonors_theses/17/, 2006.

[Goz10] Ivan Gozard. *Théorie de Galois, 2^{e} édition.* Ellipses, 2010.

[Gra07] Andrew Granville. *Théorie analytique des nombres.* lecture notes based on Davenport's book, available at https://dms.umontreal.ca/~andrew/Courses/MAT6684.W07.html, 2007.

[Han81] Phil Hanlon. *Applications of the quaternions to the study of imaginary quadratic ring class groups.* PhD thesis at the California Institute of Technology, 1981.

[Hec81] Erich Hecke. *Lectures on the theory of algebraic numbers.* Springer-Verlag, GTM 77, 1981.

[Hin08] Marc Hindry. *Arithmétique.* Calvage & Mounet, 2008.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory.* American Mathematical Society, Colloquium publications, Volume 53, 2004.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory, 2^{nd} edition.* Springer-Verlag, GTM 84, 1990.

[Kow04] Emmanuel Kowalski. *Un cours de théorie analytique des nombres.* Cours spécialisés 13, Société Mathématique de France, 2004.

[Lan94] Serge Lang. *Algebraic Number Theory.* Springer-Verlag, GTM 110, 1994.

[Per96] Daniel Perrin. *Cours d'algèbre.* ellipses, 1996.

[PG12] Corentin Perret-Gentil. *The correspondence between binary quadratic forms and quadratic fields*. Master 1 semester project at the EPFL https://corentinperretgentil.gitlab.io/static/documents/correspondence-bqf-qf.pdf, 2012.

[Reh82] H.P. Rehm. *On a theorem of Gauss concerning the number of integral solutions of the equation* $x^2 + y^2 + z^2 = m$. Lecture Notes in Pure and Applied Mathematics, Volume 79, Ternary quadratic forms and norms, edited by Olga Taussky, Dekker, 1982.

[RMS18] *RMS 129-1 (anciennement Revue de Mathématiques Spéciales)*. epistemon, octobre 2018.

[Sam71] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, 1971.

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique*. Presses Universitaires de France (PUF), 1970.

[Str08] Andreas Strömbergsson. *Analytic number theory*. lecture notes based on Davenport's book, available at http://www2.math.uu.se/~astrombe/analtalt08/www_notes.pdf, 2008.

[Tao14] Terrence Tao. *A little bit of algebraic number theory*. https://terrytao.wordpress.com/2014/11/28/245a-supplement-1-a-little-bit-of-algebraic-number-theory-optional/, 2014.

[Ven22] B. A. Venkov. *On the arithmetic of quaternion algebras, parts I & II*. Bulletin de l'Académie des Sciences de l'URSS, 1922.

[Ven29] B. A. Venkov. *On the arithmetic of quaternion algebras, parts III,IV & V*. Bulletin de l'Académie des Sciences de l'URSS, 1929.