UCLouvain

FACULTE DES SCIENCES

Faculté des sciences

Groupes de classes d'idéaux des corps quadratiques

Auteure : Delhelle Morine
Promoteur : Tignol Jean-Pierre
Lecteurs : Caprace Pierre-Emmanuel, Haine Luc
Année académique 2019-2020
Master[120] en sciences mathématiques, à finalité approfondie

Groupes de classes d'idéaux des corps quadratiques

Delhelle Morine

Promoteur : Tignol Jean-Pierre

Lecteurs : Caprace Pierre-Emmanuel, Haine Luc

UCLouvain–Université catholique de Louvain
Faculté des sciences
École de Mathématique
2019–2020

Remerciements

Je tiens tout d'abord à remercier mon directeur de mémoire, le professeur Jean-Pierre Tignol. Tant pour sa patience, sa bienveillance et sa disponibilité que pour ses remarques toujours pertinentes et constructives ainsi que les corrections réalisées qui m'auront permis d'améliorer ce travail. Je lui suis très reconnaissante pour tout ce qu'il m'a apporté ces derniers mois et même ces dernières années, à la fois sur le plan scientifique - il m'aura entre autres encouragé à développer une lecture critique des documents - mais également plus personnel - il aura renforcé ma passion pour la théorie des nombres et été un modèle pour moi.

Je voudrais remercier également les professeurs Pierre-Emmanuel Caprace et Luc Haine pour le temps qu'ils consacreront à la lecture de ce mémoire.

Enfin, je remercie ma famille qui subit depuis des années mon rythme de vie intense, le stress lié à tous les travaux ainsi que les désagréments qui y sont liés, sans oublier les livres et feuilles de mathématiques étalés dans toute la maison, etc.

Je tiens également à remercier tout particulièrement ma maman qui m'apporte un soutient moral considérable au jour le jour et s'évertue à ce que je sois dans le contexte le plus propice à la réussite depuis le début de mes études et plus encore en cette période de rédaction du mémoire. Elle m'encourage énormément et sans elle je ne serais pas le personne que je suis aujourd'hui.

Merci aussi à mon papa qui m'aura laissé l'utilisation exclusive de son ordinateur pendant ces longs mois.

J'aimerais enfin adresser un petit mot à mon grand-père qui ne pensait pas avoir la plaisir d'encore être là pour me voir arriver à la fin de mes études et qui a toujours cru en moi.

C'est grâce à toutes ces personnes que la réalisation de ce document a pu être possible et je leur exprime toute ma gratitude.

Table des matières

Introduction

Le théorème fondamental de l'arithmétique porte ce nom car la factorisation unique en produit de facteurs premiers dans les entiers rationnels est un outil particulièrement utile. Il semble si naturel qu'on pourrait se laisser aller à penser qu'il est toujours valable. Or, dans d'autres corps de nombres que $\mathbb{Q}$ la factorisation des entiers en premiers n'est pas toujours unique, loin de là. L'histoire raconte [1] qu'au cours du $19^{\text{ème}}$ siècle le mathématicien allemand Kummer en aurait d'ailleurs pris conscience au cours de ses travaux sur le dernier théorème de Fermat [2] car il ne parvenait pas à utiliser pour le résoudre de simples méthodes de factorisation et pour cause, dans un anneau engendré par une racine de l'unité, en général, la décomposition en facteurs premiers n'est pas unique. Pour en quelques sortes sauver une factorisation unique Kummer introduit alors les nombres idéaux qui furent plus largement développés dans la théorie des idéaux par Dedekind.
Le groupe des classes d'idéaux d'un corps quadratique donné permet, en se basant sur des notions telles que les idéaux fractionnaires, les idéaux principaux, etc., de capturer l'information de si la factorisation des entiers de ce corps en premiers est unique ou non. Nous en verrons la raison dans ce document.

Les méthodes utilisées sont sensiblement différentes en fonction de si le corps quadratique est imaginaire ou réel, c'est la cas imaginaire qui sera traité majoritairement dans ce document.
Le livre de référence principalement utilisé est *Algebraic Theory of Quadratic Numbers* de Mak Trifković [**1**]. Certaines démonstrations sont également inspirées du travail *Anneaux d'entiers des corps quadratiques imaginaires* de

1. Bien que parfois controversée par certains
2. "Il n'existe pas de nombres entiers strictement positifs x, y et z tels que

$$x^n + y^n = z^n$$

dès que n est un entier strictement supérieur à 2."
(Démontré en 1994 par le mathématicien britannique Andrew Wiles.)

Daniel Perrin [**4**], une référence y sera faite lorsque nécessaire. Enfin, certaines notions ont parfois été combinées avec celles du livre *Théorie algébrique des nombres* de Pierre Samuel [**2**].

Le corps du texte se présentera de la manière suivante. Le premier chapitre sera une sorte de grande introduction mettant en place des concepts de base indispensables pour la suite. Le deuxième chapitre sera une approche théorique du groupe de classes d'idéaux d'un corps quadratique imaginaire avec la théorie générale des corps quadratiques. Quant au troisième chapitre, à nouveau assez théorique, il permettra de mettre en lumière la correspondance existant entre les idéaux et les formes quadratiques, ce qui permet d'avoir une approche sous un autre angle du groupe de classes d'idéaux. Enfin, le dernier chapitre permettra de mettre en pratique les notions vues en effectuant des calculs explicites du groupe de classes d'idéaux de certains corps quadratiques ; des méthodes utilisant les deux approches seront développées.

Chapitre 1

Concepts de base

Dans ce premier chapitre nous allons rappeler quelques concepts de base sur les entiers rationnels afin d'avoir des fondements solides pour développer les théories dans les anneaux d'entiers que nous aborderons ensuite.
Avant toute chose, précisons que dans ce document tous les anneaux et tous les corps considérés sont commutatifs.

1. Arithmétique

En arithmétique, dans les entiers rationnels, une des notions incontournables est celle de nombre premier dont la définition est la suivante.

DÉFINITION 1.1. *Un nombre entier p est dit* premier *lorsqu'il possède exactement deux diviseurs entiers distincts positifs.*

Cette définition peut également se réécrire comme suit, en englobant $-p$ comme étant tout aussi premier que p.

DÉFINITION 1.2. *Un entier $p \in \mathbb{Z}, p \neq \pm 1$ est dit* premier *si pour tout $a, b \in \mathbb{Z}$, $p = ab$ implique $a = \pm 1$ ou $b = \pm 1$.*

REMARQUE 1.3. Nous verrons que dans la suite nous utiliserons plutôt le terme *irréductible* et que *premier* représentera autre chose.

Cette deuxième formulation sera plus aisément adaptable lorsque nous souhaiterons travailler dans les corps quadratiques.

Lorsque nous parlons d'arithmétique et de nombres premiers, il est difficile de ne pas citer le *théorème fondamental de l'arithmétique* qui nous assure une factorisation unique en facteurs premiers de tous les entiers non nuls (à permutations près).

THÉORÈME 1.4 (Théorème fondamental de l'arithmétique dans $\mathbb{Z}$). *Tout entier non nul $a \in \mathbb{Z}\backslash\{0\}$ et différent de ± 1 peut s'écrire comme produit de nombres premiers d'une unique façon, à l'ordre et au signe des facteurs près.*

Il est également possible d'introduire une terminologie plus générale, qui nous sera d'ailleurs utile par la suite, afin d'écrire ce théorème d'une autre manière. C'est ce que nous allons faire ci-dessous en commençant par quelques définitions.
La première que nous allons aborder est celle d'*unité* qui correspond, dans le cas des entiers rationnels, à ± 1 et qui est en fait une notion équivalente à *l'inversibilité*.

DÉFINITION 1.5. *Dans un anneau A, une* unité *est un élément $a \in A$ pour lequel il existe un $b \in A$ tel que $ab = 1$, b est appelé* inverse multiplicatif *de a. Cet inverse est alors noté a^{-1}.*
L'ensemble des unités de l'anneau A forme un groupe sous la multiplication et est noté $A^\times$.

EXEMPLE 1.6. Nous avons par exemple que pour un corps F tous les éléments non nuls sont des unités $F^\times = F\backslash\{0\}$.
Pour les entiers rationnels nous avons, comme déjà cité, que $\mathbb{Z}^\times = \{\pm 1\}$.

REMARQUE 1.7. Nous mentionnons déjà, même si la norme dans un corps quadratique n'a pas encore été proprement définie, que les unités sont les éléments de norme égale à ± 1.

Un autre concept important est celui d'*élément irréductible* qui, dans un anneau d'entiers, est la généralisation directe du concept de nombre premier dans $\mathbb{Z}$.
Rappelons tout d'abord ce qu'est un *anneau intègre*.

DÉFINITION 1.8. *Un anneau A est dit* intègre *si $A \neq \{0\}$ et si pour tout $a, b \in A$ tels que $ab = 0$, nous avons $a = 0$ ou $b = 0$.*

Les éléments irréductibles se définissent dans les anneaux intègres.

DÉFINITION 1.9. *Soit A un anneau intègre et $p \in A\backslash A^\times$. Nous dirons que p est* irréductible *si, pour tout $a, b \in A$, $p = ab$ implique soit $a \in A^\times$ ou $b \in A^\times$.*

REMARQUE 1.10. Nous voyons bien la similitude avec la définition des entiers premiers où les unités étaient alors simplement ± 1. Mais la notion d'*élément premier* est également présente dans les anneaux intègres en plus de celle d'irréductible et sa définition est celle ci-dessous.

DÉFINITION 1.11. *Soit A un anneau intègre et $p \in A\backslash A^\times$. Nous dirons que p est* premier *si p est non nul et si, pour tout $a, b \in A$, $p|ab$ implique $p|a$ ou $p|b$* [1].

1. Notation : $p|a$ se lit *p divise a*.

Introduisons également la définition d'anneau *factoriel* qui est un cas particulier des anneaux intègres.

DÉFINITION 1.12. *Un anneau intègre A est dit* factoriel *si tout élément non nul et non inversible de A est un produit d'éléments irréductibles, la factorisation d'un élément de A étant unique à permutations et multiplications par unités près.*

Sur base de ces définitions nous pouvons remarquer que la notion de premier est donc plus forte que celle d'irréductible puisque dans tout anneau intègre, être premier implique être irréductible mais non l'inverse. De plus, il est intéressant de noter que dans un anneau factoriel, au vu de la propriété de factorisation unique, la réciproque est vraie et les premiers non nuls sont exactement les irréductibles, ces deux notions sont équivalentes [2].
En effet, dans le cas d'un anneau intègre, le fait d'être factoriel est équivalent au fait que tout élément non nul admet une factorisation en un nombre fini de facteurs irréductibles et que tout élément irréductible est premier [3].

Lorsque nous parlons d'unités, il est intéressant de souligner ce que sont des *éléments associés*.

DÉFINITION 1.13. *Soit A un anneau intègre. Deux éléments $a, b \in A$ sont dit* associés *si a divise b (il existe $c \in A$ tel que $a = bc$) et b divise a (il existe $d \in A$ tel que $b = ad$). Ou, de manière équivalente, s'il existe une unité $u \in A^\times$ telle que $a = bu$, c'est-à-dire que l'un peut être obtenu à partir de l'autre en le multipliant par une unité.*

Nous pouvons, pour terminer cette section, à nouveau énoncer le théorème fondamental à la lueur de ces nouvelles définitions.

THÉORÈME 1.14 (Théorème fondamental de l'arithmétique). *Tout entier rationnel non nul est produit d'une unité et d'un nombre fini d'éléments irréductibles. Cette factorisation est unique à permutations et associations près.*
Ou encore, de manière plus concise : $\mathbb{Z}$ est factoriel.

2. Corps quadratiques

La notion de *corps quadratique* est primordiale et le chapitre 2 lui est consacré. Nous ne donnerons donc pas ici de définitions générales, ce que

2. Dans la suite, ce sera principalement *irréductible* qui sera employé.
3. Une démonstration peut être trouvée par exemple dans *Algebras, Rings and Modules* [**5**, Théorème 7.2.2].

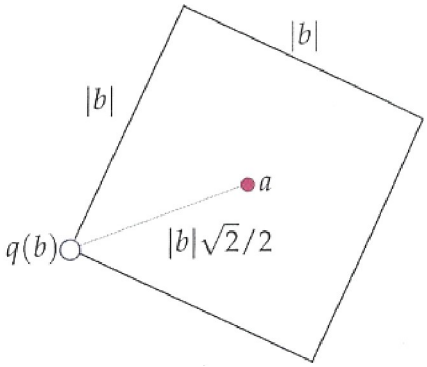
nous allons faire ci-dessous est analyser des cas particuliers d'une situation plus générale qui sera étudiée au chapitre suivant et à partir desquels nous pourrons tirer des observations importantes.

Le premier exemple que nous allons aborder est l'anneau bien connu des entiers de Gauss $\mathbb{Z}[i]$. C'est un sous-ensemble de $\mathbb{C}$ consistant en les nombres complexes pour lesquels la partie réelle et la partie imaginaire sont des entiers. Cet anneau est noté $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. La norme considérée dans ce cas est donc identique à celle dans les complexes.
Une des premières choses qui peut être remarquée est qu'il y a plus d'unités dans cet anneau que dans celui des entiers rationnels. En effet, ici les éléments possédant un inverse sont $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, car ce sont ceux de norme 1 et que si $a \in \mathbb{Z}[i]$ est tel que $a = \alpha + \beta i$ alors

$$\mathrm{N}(a) = \alpha^2 + \beta^2 = 1 \text{ ce qui entraine } \alpha^2 = 0, \beta^2 = 1 \text{ ou } \alpha^2 = 1, \beta^2 = 0$$

et donc $a \in \{\pm 1, \pm i\}$.
Mais ce qu'il faut surtout savoir c'est que dans cet anneau la factorisation en irréductibles est unique et cela vient du fait que nous avons un algorithme de division [4].
Pour arriver à cette conclusion, commençons par remarquer que les opérations dans $\mathbb{Z}[i]$ sont pour la plupart assez évidentes. En effet, l'addition, la soustraction, la division et la conjugaison sont identiques à celles dans les nombres complexes. La relation de divisibilité est facile également, il suffit juste de savoir qu'un entier de Gauss z en divise un autre w s'il existe un entier de Gauss m tel que $w = z \cdot m$, nous écrivons alors comme à notre habitude $z|m$.
Ce qui est peut-être un peu plus délicat est la division avec reste et l'algorithme d'Euclide. Pour bien comprendre ce qu'il se passe, rappelons nous que la division avec reste dans les entiers rationnels provient de la géométrie des multiples. Si nous visualisons la droite réelle, $a = qb + r$ signifie que nous coupons la droite en intervalles de longueur b et que a se situe dans le $(q+1)^{\text{ème}}$ intervalle à une distance r de son début, cela explique d'ailleurs pourquoi nous devons avoir $|r| < |b|$. Nous pouvons alors représenter de manière géométrique également la division avec reste dans les entiers de Gauss. Dans ce cas, c'est le plan complexe qui va être subdivisé en carrés par les multiples de b comme nous pouvons en voir un exemple sur l'image ci-dessous [5].

4. L'anneau est alors factoriel et les irréductibles sont égaux aux premiers.
5. Issue du livre *An illustrated theory of numbers* [3].



Les carrés dont il est question étant donc ceux dont les sommets sont les points du plan complexe de la forme $b \cdot (x + iy)$ avec $x, y \in \mathbb{Z}$. Nous pouvons alors également déduire une division avec reste $a = qb + r$ où cette fois q indique dans quel carré a se trouve et r détermine où il se situe dans le carré. Nous avons alors logiquement que $|r| \leq |b| \cdot \frac{\sqrt{2}}{2}$ où la borne est obtenue en prenant une demi-diagonale du carré. Nous remarquons que $\frac{\sqrt{2}}{2} < 1$ et donc la valeur absolue du reste est plus petite que celle du diviseur. L'algorithme d'Euclide suit alors directement, de la même manière que pour les nombres réels, en appliquant la division avec reste dans les entiers de Gauss un nombre fini de fois nous pouvons calculer le plus grand commun diviseur de deux entiers de Gauss qui est le dernier reste non nul. Nous pouvons ajouter à tout cela la notion d'irréductible dans les entiers de Gauss ainsi que le lemme d'Euclide qui est analogue à celui dans $\mathbb{Z}$.

DÉFINITION 1.15. *Un élément $\pi \in \mathbb{Z}[i], \pi \notin \{\pm 1, \pm i\}$ est irréductible si $\pi = \alpha\beta$ implique $\alpha \in \{\pm 1, \pm i\}$ ou $\beta \in \{\pm 1, \pm i\}$, pour tout $\alpha, \beta \in \mathbb{Z}[i]$.*

LEMME 1.16 (Euclide). *Soient $b, c \in \mathbb{Z}[i]$ et $p \in \mathbb{Z}[i]$, p irréductible. Si p divise le produit bc, alors p divise b ou c.*

En combinant tout ceci, la factorisation unique devient alors facile à déduire avec un raisonnement similaire à celui pour les entiers rationnels [6].

Le deuxième exemple est celui de l'anneau des entiers $\mathbb{Z}[\sqrt{-5}]$.
Contrairement à l'exemple précédent, la factorisation en irréductibles n'est pas unique dans cet anneau d'entiers.
Pour s'en convaincre, une des premières choses à faire est de voir quelles

6. Pour plus de précisions, voir *An illustrated theory of numbers* à la page 111 pour un schéma représentant le raisonnement déductif ou encore les deux premiers chapitres pour les détails dans le cas des entiers quadratiques [**3**, Chapter 1, Chapter 2].

sont les unités dans $\mathbb{Z}[\sqrt{-5}]$. À nouveau, la norme considérée ici est identique à celle dans les complexes et en particulier la norme de tout élément est positive. Par la remarque 1.7 nous savons que les unités sont les éléments dans $\mathbb{Z}[\sqrt{-5}]$ de norme 1. Nous cherchons donc les solutions de $a^2 + 5\beta^2 = 1$ et nous obtenons $\alpha = \pm 1, \beta = 0$ c'est-à-dire que $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$.
Nous remarquons alors directement que dans $\mathbb{Z}[\sqrt{-5}]$ nous pouvons par exemple factoriser 6 des deux manières suivantes

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

qui sont deux factorisations non équivalentes en irréductibles.
Voyons que ce sont bien des éléments irréductibles. Pour cela observons que leurs normes sont respectivement $4, 9, 6$ et 6 et raisonnons par l'absurde. Si $(1 + \sqrt{-5})$ n'était pas irréductible, cela voudrait dire qu'il existerait $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ tels que $(1 + \sqrt{-5}) = \alpha\beta$ et $\alpha, \beta \notin \mathbb{Z}[\sqrt{-5}]^\times$. Mais alors nous devrions avoir $6 = \mathrm{N}(1 + \sqrt{-5}) = \mathrm{N}(\alpha).\mathrm{N}(\beta)$ avec $\mathrm{N}(\alpha), \mathrm{N}(\beta) \neq 1$. C'est-à-dire qu'il faut que $\mathrm{N}(\alpha) = 2$ et $\mathrm{N}(\beta) = 3$ (ou l'inverse) ce qui est impossible puisque $a^2 + 5b^2 = 2$ et $a^2 + 5b^2 = 3$ ne possèdent pas de solution dans les entiers naturels. Cela nous montre donc bien que $(1 + \sqrt{-5})$ est irréductible. Nous pouvons faire un raisonnement similaire pour voir que $(1 - \sqrt{-5}), 2$ et 3 sont irréductibles également.

Au vu de ces deux exemples, ce qu'il est important de noter est que, de manière plus générale, si nous nous plaçons dans un corps quadratique différent des rationnels, et que nous nous intéressons à son anneau des entiers plutôt qu'aux entiers rationnels, le théorème fondamental de l'arithmétique nous fait malheureusement défaut. En effet il existe des anneaux d'entiers pour lesquels la décomposition en irréductibles n'est plus unique à permutations près.

3. Idéal d'un anneau

Même si, comme nous venons de le voir, la factorisation en irréductibles n'est pas toujours unique dans les anneaux d'entiers des corps quadratiques, il est possible d'obtenir une certaine unicité en introduisant le concept d'idéaux dans un anneau. Il existe alors une version adaptée du théorème fondamental de l'arithmétique appliquée à la factorisation en idéaux et c'est ce que nous allons voir dans cette section.

Commençons par une approche théorique avec quelques définitions. Avant toute chose rappelons ce qu'est un *idéal* dans un anneau.

DÉFINITION 1.17. *Soit A un anneau. Un* idéal $I \subseteq A$ *est un sous-groupe additif absorbant pour la multiplication : si $a \in A$ et $x \in I$, alors $ax \in I$.*

Au sein de ces idéaux, il existe également l'analogue des entiers premiers qui sont les *idéaux premiers*. Ils sont définis de la manière suivante.

DÉFINITION 1.18. *Un idéal P de A est* premier *si $P \neq A$ et si, pour tout $a, b \in A$, $ab \in P$ implique $a \in P$ ou $b \in P$.*

Un idéal peut également être dit *principal* s'il possède la caractéristique suivante.

DÉFINITION 1.19. *Un idéal I d'un anneau A est* principal *si*

$$I = Ax = \{ax \mid a \in A\} \quad \textit{pour } x \in A.$$

Un tel x est alors appelé générateur *de I.*

Notons que tous les générateurs d'un même idéal sont associés.

REMARQUE 1.20. L'idéal principal Ax est le plus petit idéal contenant x. Si x est l'élément neutre ou une unité alors l'idéal est trivial ($\{0\}$ si x est neutre et A si x est une unité).

EXEMPLE 1.21. Dans $\mathbb{Z}$ tout idéal est principal étant donné que tout sous-groupe est monogène.
De même, dans $\mathbb{Z}[i]$ tout idéal est principal. C'est une conséquence de l'algorithme de division avec reste (tout anneau euclidien est principal [7]). Soit I un idéal de $\mathbb{Z}[i]$, montrons qu'il existe $x \in \mathbb{Z}[i]$ tel que $I = \mathbb{Z}[i]x$. Plus précisément, prenons $x \in I$ tel que x soit de norme minimale non nulle. Le fait que $\mathbb{Z}[i]x \subseteq I$ est évident par définition d'idéal. Il reste à voir que $I \subseteq \mathbb{Z}[i]x$. Soit $\alpha \in I$, nous allons prouver que $\alpha = z.x$ où $z \in \mathbb{Z}[i]$, c'est-à-dire que $\frac{\alpha}{x} = z \in \mathbb{Z}[i]$. A priori, $\frac{\alpha}{x} = z$ est dans $\mathbb{Q}[i]$. Comme nous l'avons vu, la division avec reste nous dit que si x ne divise pas α alors, pour $q, r \in \mathbb{Z}[i]$, $\alpha = q.x + r$ où $\mathrm{N}(r) \leq \mathrm{N}(x) \cdot \frac{\sqrt{2}}{2} < \mathrm{N}(x)$. Il en résulte que $\mathrm{N}(\alpha - q.x) = \mathrm{N}(r) < \mathrm{N}(x)$. Or, $(\alpha - q.x) \in I$ donc par minimalité il faut que $\mathrm{N}(\alpha - q.x) = 0$. Nous en déduisons que $\alpha = q.x \in \mathbb{Z}[i]x$. Nous avons donc nos deux inclusions et nous pouvons conclure que tout idéal de $\mathbb{Z}[i]$ est principal.
Dans $\mathbb{Z}[\sqrt{-5}]$ par contre ce n'est pas le cas. En effet, nous observons que l'idéal I engendré par 2 et $(1 + \sqrt{-5})$ n'est pas principal. Raisonnons par

7. Le raisonnement qui suit peut être adapté pour le cas plus général.

l'absurde. Si I était principal, il existerait $x \in \mathbb{Z}[\sqrt{-5}]$ tel que $I = \mathbb{Z}[\sqrt{-5}]x$. Pour que $2 \in \mathbb{Z}[\sqrt{-5}]x$, il faut qu'il existe $\alpha \in \mathbb{Z}[\sqrt{-5}]$ tel que $2 = \alpha.x$ et donc $4 = \mathrm{N}(2) = \mathrm{N}(\alpha)\,\mathrm{N}(x)$. Étant donné qu'un élément de $\mathbb{Z}[\sqrt{-5}]$ ne peut pas avoir une norme ni strictement négative, ni égale à 2 (comme nous l'avons vu à la fin de la section précédente), il faut que soit $\mathrm{N}(\alpha) = 1$ et $\mathrm{N}(x) = 4$ soit l'inverse. Par le même type de raisonnement, nous observons que pour que $(1 + \sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]x$, il faut $\beta \in \mathbb{Z}[\sqrt{-5}]$ tel que $(1 + \sqrt{-5}) = \beta.x$ et tel que $\mathrm{N}(\beta) = 1$ et $\mathrm{N}(x) = 6$ ou l'inverse. En combinant les deux conditions, cela nous donne que $\mathrm{N}(x) = 1$. Or, $I \subset \mathbb{Z}[\sqrt{-5}]$ mais $\mathbb{Z}[\sqrt{-5}] \not\subset I$ et donc I n'est pas principal.

Avec la notion d'idéaux principaux vient celle d'*anneau principal*.

DÉFINITION 1.22. *Un anneau intègre A est dit* principal *si tous ses idéaux sont principaux.*

REMARQUE 1.23. Tout anneau principal est factoriel. Mais la réciproque est fausse, il existe des anneaux factoriels non principaux comme par exemple l'anneau des polynômes en plusieurs indéterminées sur un corps.

EXEMPLE 1.24. Puisque l'exemple 1.21 nous montre que $\mathbb{Z}[i]$ est principal, nous en déduisons qu'il est factoriel.

Il est intéressant de voir qu'il existe des liens entres ces différentes notions dont la propriété suivante.

PROPRIÉTÉ 1.25. *Soit A un anneau et I un idéal de A. Si I est un idéal principal non trivial, il est premier si et seulement si il est engendré par un élément premier de A.*

DÉMONSTRATION. Dans un sens nous avons que si I est non trivial, principal et premier alors $I = Ax = \{ax \mid a \in A\}$ pour $x \in A$. De plus, pour tout $m, n \in A$, $mn \in Ax$ implique $m \in Ax$ ou $n \in Ax$.
Dit avec d'autres mots, cela signifie que pour tout $m, n \in A$, $mn = ax$ pour un certain $a \in A$ implique que $m = bx$ pour un certain $b \in A$ ou $n = cx$ pour un certain $c \in A$.
Mais alors nous avons que pour tout $m, n \in A$, $x|mn$ implique $x|m$ ou $x|n$. Pour que x soit premier dans A il ne nous reste plus qu'à remarquer que $x \notin A^\times$. Ce dernier point vient du fait que par hypothèse I est non trivial, x ne peut donc être une unité.

Dans l'autre sens, supposons que I soit non trivial, principal et engendré par un élément premier de A alors $I = Ax = \{ax \mid a \in A\}$ pour

$x \in A \backslash A^\times$ et tel que pour tout $a, b \in A$, $x|ab$ implique $x|a$ ou $x|b$.
Nous avons alors que pour tout $a, b \in A$, $ab \in Ax$ signifie que $ab = rx$ pour un certain $r \in A$, mais puisque x est premier cela implique que soit x divise a soit x divise b. Dans le premier cas cela signifie que $a = sx$ pour un certain $s \in A$ (c'est-à-dire que $a \in Ax$) et dans le deuxième cas, avec un raisonnement similaire, cela signifie que $b \in Ax$. Nous obtenons donc bien que $Ax = I$ est un idéal premier. □

Une chose importante à souligner est que cette propriété correspond à la définition même d'un élément premier. En effet, un élément $x \in A$ est dit premier si et seulement si l'idéal principal qu'il engendre est un idéal premier. Nous voyons donc que ces deux définitions sont intimement liées.

Une autre notion utile à préciser pour arriver au théorème souhaité est celle de *produit d'idéaux*.

DÉFINITION 1.26. *Soient I et J deux idéaux d'un anneau A, nous définissons leur* produit *comme étant l'idéal*

$$IJ = \{\sum_{i=1}^{m} x_i y_i \mid x_i \in I, y_i \in J\}.$$

Cet idéal IJ est le plus petit idéal contenant tous les produits xy lorsque $x \in I$ et $y \in J$.

REMARQUE 1.27. Cette définition permet d'étendre la multiplication des éléments d'un anneau à celle des idéaux puisque $(Aa)(Ab) = A(ab)$.

Nous pouvons maintenant énoncer la variante du théorème fondamental de l'arithmétique pour les idéaux. Certains termes employés seront précisés plus loin dans ce document.

THÉORÈME 1.28 (Factorisation unique des idéaux). *Soit un corps quadratique $F = \mathbb{Q}[\sqrt{D}]$ et $\mathcal{O}$ son anneau d'entiers. Pour tout idéal I de $\mathcal{O}$, différent de 0 et $\mathcal{O}$, il existe des idéaux premiers $P_1, P_2, \cdots, P_n$ de $\mathcal{O}$, non nécessairement distincts, tels que $I = P_1 P_2 \cdots P_n$. Cette factorisation est unique à permutation des facteurs près.*

REMARQUE 1.29. Il est important ici de remarquer que nous pouvons déduire de toute cette théorie un lien important avec la validé de la factorisation unique en premiers dans des anneaux d'entiers. En effet, dans des anneaux comme $\mathbb{Z}$ ou $\mathbb{Z}[i]$, chaque idéal se factorise de manière unique en idéaux premiers. Nous savons également que dans de tels anneaux, tous les idéaux sont principaux. Les idéaux principaux sont donc factorisés en

un produit d'idéaux principaux premiers P_i, ce qui signifie par définition que ces P_i sont engendrés par des éléments premiers. Finalement cela correspond à dire que dans de tels anneaux, des idéaux engendrés par un élément x quelconque se factorisent de manière unique en idéaux engendrés par un élément premier. Cela est équivalent à dire que chaque élément se factorise de manière unique en produit d'éléments premiers, il y a un glissement de la factorisation unique des idéaux en la factorisation unique des éléments. Et nous avions effectivement vu que le théorème fondamental de l'arithmétique était valable dans $\mathbb{Z}$ et $\mathbb{Z}[i]$.
Pour pouvoir faire ce raisonnement nous avons eu besoin du fait que dans ces anneaux tous les idéaux étaient principaux. C'est pourquoi ça ne fonctionne par exemple pas pour $\mathbb{Z}[\sqrt{-5}]$.
De manière plus concise, ce que cela nous montre est que dans un anneau principal, la factorisation unique des idéaux est une propriété équivalente à la factorisation unique des éléments. Nous voyons donc que l'introduction des idéaux est primordiale.

Terminons ce chapitre en illustrant le théorème sur l'exemple déjà rencontré de $\mathbb{Z}[\sqrt{-5}]$, que nous noterons A pour simplifier les notations.

EXEMPLE 1.30. Soit l'idéal premier $I = 2A + (1+\sqrt{-5})A$ engendré par 2 et $(1+\sqrt{-5})$.
Observons que I peut aussi être engendré par 2 et $(1-\sqrt{-5})$. Pour cela, posons $I' = 2A + (1-\sqrt{-5})A$ l'idéal engendré par 2 et $1-\sqrt{-5}$. Nous remarquons alors que

- d'une part, $1-\sqrt{-5} = 2-(1+\sqrt{-5})$, ce qui nous montre donc $(1-\sqrt{-5}) \in I$ et par conséquent $I' \subseteq I$,
- d'autre part, $1+\sqrt{-5} = 2-(1-\sqrt{-5})$, donc $(1+\sqrt{-5}) \in I'$ et $I \subseteq I'$.

Ce qui nous montre bien que $I' = I$.

Nous calculons également que $I^2 = 2A$.
En effet, par définition, I^2 est engendré par 4, $(1+\sqrt{-5})^2$ et $2(1+\sqrt{-5})$. Nous remarquons que puisque $(1+\sqrt{-5})^2 = -4+2\sqrt{-5}$ ces trois générateurs sont tous dans $2A$, donc $I^2 \subseteq 2A$. Réciproquement nous avons bien que $2A \subseteq I^2$ puisque $2 \in I^2$ car

$$2 = 2(1+\sqrt{-5}) - (-4+2\sqrt{-5}) - 4 = 2(1+\sqrt{-5}) - (1+\sqrt{-5})^2 - 4.$$

De plus, si $J = 3A + (1+\sqrt{-5})A$ et $J' = 3A + (1-\sqrt{-5})A$ alors nous avons les produits suivants.

— $JJ' = 3A$

- Par définition JJ' est engendré par $9, 3(1-\sqrt{-5}), 3(1+\sqrt{-5})$ et $(1+\sqrt{-5})(1-\sqrt{-5})$.
- Puisque $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$, tous les générateurs sont dans $3A$ et donc $JJ' \subseteq 3A$.
- Réciproquement $3 = 9-6 = 9-(1+\sqrt{-5})(1-\sqrt{-5})$ donc $3A \subseteq JJ'$.

— $IJ = (1+\sqrt{-5})A$

- Par définition IJ est engendré par $6, 2(1+\sqrt{-5}), 3(1+\sqrt{-5})$ et $(1+\sqrt{-5})^2$.
- Puisque $6 = (1+\sqrt{-5})(1-\sqrt{-5})$, tous les générateurs sont dans $(1+\sqrt{-5})A$ et donc $IJ \subseteq (1+\sqrt{-5})A$.
- Réciproquement, $(1+\sqrt{-5}) = 3(1+\sqrt{-5}) - 2(1+\sqrt{-5})$ donc $(1+\sqrt{-5})A \subseteq IJ$.

— $IJ' = (1-\sqrt{-5})A$

- Par définition IJ' est engendré par $6, 2(1-\sqrt{-5}), 3(1-\sqrt{-5})$ et $(1-\sqrt{-5})^2$.
- Puisque $6 = (1+\sqrt{-5})(1-\sqrt{-5})$, tous les générateurs sont dans $(1-\sqrt{-5})A$ et donc $IJ' \subseteq (1+\sqrt{-5})A$.
- Réciproquement, $(1-\sqrt{-5}) = 3(1-\sqrt{-5}) - 2(1-\sqrt{-5})$ donc $(1-\sqrt{-5})A \subseteq IJ'$.

Ces calculs nous permettent d'illustrer que la décomposition

$$6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

peut se réinterpréter en termes de factorisation unique des idéaux. En effet, puisque $6A = 2A \cdot 3A = I^2JJ'$ et $6A = (1+\sqrt{-5})A \cdot (1-\sqrt{-5})A = IJIJ'$, nous observons que ces deux factorisations en idéaux sont identiques à permutation près.
Cet exemple montre bien comment la factorisation en idéaux permet de sauver l'unicité.

Chapitre 2

Corps quadratiques

Dans ce deuxième chapitre nous allons aborder la théorie des corps quadratiques, ainsi que quelques notions qui leur sont liées.

1. Entiers

La première chose à faire est de définir ce qu'est un *corps quadratique* en précisant ce que signifie le fait qu'il soit *imaginaire* ou *réel*.

DÉFINITION 2.1. *Un* corps quadratique *F est un sous-corps de $\mathbb{C}$ engendré par une racine d'un polynôme quadratique irréductible à coefficients rationnels.*
Un corps quadratique est de la forme

$$F = \mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$$

où $D = e^2 - 4df$ est un entier rationnel, appelé discriminant, *pour une équation $dx^2 + ex + f = 0$ avec $d, e, f \in \mathbb{Z}$.*
Le corps $\mathbb{Q}[\sqrt{D}]$ est dit imaginaire *si $D < 0$ et* réel *si $D > 0$.*
Les éléments d'un corps quadratique sont des nombres quadratiques.

REMARQUE 2.2. Nous pouvons, sans perte de généralité, supposer que $D \in \mathbb{Z}$ est sans facteur carré autre que 1. En effet, si $D' = n^2 D$ alors nous avons que $a + b\sqrt{D'} = a + bn\sqrt{D}$ et dans ce cas $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$.

Tout comme dans les nombres complexes, chaque nombre quadratique a un *conjugué* qui permet de définir sa *trace* et sa *norme*.

DÉFINITION 2.3. *Soit $\alpha \in \mathbb{Q}[\sqrt{D}]$. Le* conjugué *de $\alpha = a + b\sqrt{D}$ est $\bar{\alpha} = a - b\sqrt{D}$.*
Nous définissons la trace *et la* norme *de α par $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha}$ et $\mathrm{N}(\alpha) = \alpha\bar{\alpha}$.*

REMARQUE 2.4. Soit $\alpha \in \mathbb{Q}[\sqrt{D}]$, sa trace et sa norme peuvent être utilisées pour obtenir son polynôme minimal sur $\mathbb{Q}$. Ce polynôme minimal est $X - \alpha$ si $\alpha \in \mathbb{Q}$ et $X^2 - \mathrm{Tr}(\alpha)X + \mathrm{N}(\alpha) = (X - \alpha)(X - \bar{\alpha})$ si $\alpha \notin \mathbb{Q}$.

Parmi les nombres quadratiques, certains se distinguent, ce sont les *entiers quadratiques* qui peuvent être définis de la manière suivante.

DÉFINITION 2.5. *Un* entier quadratique *est un nombre complexe qui est racine d'un polynôme quadratique unitaire à coefficients entiers. C'est-à-dire un* $\alpha \in \mathbb{C}$ *satisfaisant* $\alpha^2 + a\alpha + b = 0$ *où* $a, b \in \mathbb{Z}$.

Il existe d'autres manières de définir les entiers quadratiques comme nous le montre le lemme ci-dessous.

LEMME 2.6. *Un élément dans un corps quadratique* $\alpha \in \mathbb{Q}[\sqrt{D}]$ *est un entier quadratique si et seulement si sa trace* $\mathrm{Tr}(\alpha)$ *et sa norme* $\mathrm{N}(\alpha)$ *sont des entiers.*

DÉMONSTRATION. [1] Au vu de la remarque 2.4 il est évident que si $\mathrm{Tr}(\alpha)$ et $\mathrm{N}(\alpha)$ sont des entiers alors α est racine d'un polynôme quadratique unitaire à coefficients entiers et donc par définition α est bien un entier quadratique.

En ce qui concerne l'autre implication, supposons que $\alpha \in \mathbb{Q}[\sqrt{D}]$ est un entier quadratique. Par hypothèse il est donc racine d'un polynôme quadratique unitaire à coefficients entiers, notons-le $P(X)$. Nous pouvons supposer que ce polynôme est irréductible sur $\mathbb{Z}$ (si ce n'est pas le cas, il nous suffit de le remplacer par un de ses facteurs irréductibles puisque $\mathbb{Z}[X]$ est factoriel). Dans ce cas $P(X)$ est le polynôme minimal de α sur $\mathbb{Q}$ qui, par la remarque 2.4, est $X^2 - \mathrm{Tr}(\alpha)X + \mathrm{N}(\alpha) = (X - \alpha)(X - \bar{\alpha})$. Il en découle que la norme et la trace de α sont bien des entiers. □

Cette deuxième définition pour les entiers quadratiques nous permet d'introduire la notation suivante.

NOTATION 2.7. L'ensemble des entiers quadratiques sur un corps $\mathbb{Q}[\sqrt{D}]$ est noté

$$\begin{aligned} \mathcal{O} &= \{\alpha \in \mathbb{Q}[\sqrt{D}] \mid \alpha^2 + a\alpha + b = 0 \text{ pour } a, b \in \mathbb{Z}\} \\ &= \{\alpha \in \mathbb{Q}[\sqrt{D}] \mid \mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in \mathbb{Z}\}. \end{aligned}$$

Il est important de donner une caractérisation de l'ensemble des entiers quadratiques en fonction du corps quadratique de départ et également de noter que $\mathcal{O}$ est un anneau, nommé *anneau des entiers quadratiques* (il peut être mis en parallèle avec l'anneau des entiers rationnels $\mathbb{Z}$ dans le corps $\mathbb{Q}$).
C'est ce que nous faisons dans la proposition suivante.

1. Cette démonstration est inspirée du document *Anneaux d'entiers des corps quadratiques imaginaires* [**4**, Lemme 2.6].

PROPOSITION 2.8. *L'ensemble des entiers $\mathcal{O}$ d'un corps quadratique $\mathbb{Q}[\sqrt{D}]$ est un anneau. Il est donné par $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\delta = \mathbb{Z}[\delta]$, où*

$$\delta = \begin{cases} \sqrt{D} \text{ pour } D \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} \text{ pour } D \equiv 1 \pmod 4 \end{cases}$$

DÉMONSTRATION. [2] Commençons par montrer que $\mathbb{Z} + \mathbb{Z}\delta \subseteq \mathcal{O}$.
Dans les deux cas $\delta \in \mathbb{Q}[\sqrt{D}]$ est racine d'un polynôme quadratique unitaire à coefficients entiers. Dans le premier cas $\delta = \sqrt{D}$ est racine de $x^2 - D$ et dans le deuxième cas $\delta = \frac{1+\sqrt{D}}{2}$ est racine de $x^2 - x + \frac{1-D}{4}$. Nous en déduisons que δ est un entier quadratique, $\delta \in \mathcal{O}$.
Plus généralement, pour voir que $\mathbb{Z} + \mathbb{Z}\delta$ est dans $\mathcal{O}$, c'est-à-dire pour voir que tout élément de la forme $\lambda = x + y\delta$ avec $x, y \in \mathbb{Z}$ est dans $\mathcal{O}$, par la notation 2.7, il suffit de vérifier que $\mathrm{Tr}(\lambda)$ et $\mathrm{N}(\lambda)$ sont dans $\mathbb{Z}$. Nous devons analyser les deux cas possibles

— $D \equiv 2,3 \pmod 4$:
Dans ce cas $\delta = \sqrt{D}$ donc

$$\mathrm{Tr}(\lambda) = 2x \text{ et } \mathrm{N}(\lambda) = x^2 - y^2 D$$

qui sont évidemment bien dans $\mathbb{Z}$.

— $D \equiv 1 \pmod 4$:
Dans ce cas $\delta = \frac{1+\sqrt{D}}{2}$ donc

$$\mathrm{Tr}(\lambda) = 2x + y \text{ et } \mathrm{N}(\lambda) = x^2 + xy + y^2 \frac{1-D}{4}$$

qui sont également dans $\mathbb{Z}$.

Nous en concluons que $\mathbb{Z} + \mathbb{Z}\delta \subseteq \mathcal{O}$.

Montrons maintenant l'autre inclusion $\mathcal{O} \subseteq \mathbb{Z} + \mathbb{Z}\delta$.
Soit $\alpha = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$ un entier quadratique. Nous savons par le lemme 2.6 que $\mathrm{Tr}(\alpha) = 2a, \mathrm{N}(\alpha) = a^2 - Db^2 \in \mathbb{Z}$.
Nous pouvons distinguer deux cas, soit a est un entier soit non. Dans les deux cas b est a priori dans $\mathbb{Q}$ et donc nous posons $b = \frac{p}{q}$ tel que p et q sont premiers entre eux, $p \in \mathbb{Z}$ et $q \neq 0, q \in \mathbb{N}$.
Si $a \in \mathbb{Z}$ alors $a^2 \in \mathbb{N}$ et puisque $\mathrm{N}(\alpha) \in \mathbb{Z}$ nous en déduisons que $Db^2 = D\frac{p^2}{q^2} \in \mathbb{Z}$. Il faut donc que q^2 divise Dp^2 mais nous savons que p et q sont premiers entre eux. Le lemme d'Euclide implique alors que q^2 divise D qui est sans facteur carré différent de 1, nous en déduisons que $q = 1$. Dans le

2. Cette démonstration est inspirée du document *Anneaux d'entiers des corps quadratiques imaginaires* [**4**, Théorème 2.4].

cas où a est entier, $b \in \mathbb{Z}$ l'est également et donc $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{D}$.
Supposons maintenant que $a \notin \mathbb{Z}$. Puisque $\mathrm{Tr}(\alpha) = 2a \in \mathbb{Z}$ nous avons que $a = \frac{k}{2}$ avec $k \in \mathbb{Z}$ impair. Cette fois, le fait que la norme de α doit être entière nous donne que

$$\frac{k^2}{4} - D\frac{p^2}{q^2} = n \in \mathbb{Z} \quad \text{donc} \quad 4q^2n = k^2q^2 - 4Dp^2. \tag{2.1}$$

Nous en déduisons que 4 divise k^2q^2. Or nous savons que k est impair et nous obtenons que 4 divise q^2, q est donc pair et nous notons $q = 2q'$. Dans ce cas, 2.1 devient

$$\begin{aligned} 16q'^2n = 4k^2q'^2 - 4Dp^2 &\Leftrightarrow 4q'^2n = k^2q'^2 - Dp^2 \\ &\Leftrightarrow Dp^2 = q'^2(k^2 - 4n). \end{aligned}$$

Avec un raisonnement similaire à celui effectué dans le cas où $a \in \mathbb{Z}$ nous déduisons que q'^2 doit diviser Dp^2 mais puisque q' et p sont premiers entre eux q'^2 divise D qui est sans facteur carré différent de 1. Cela implique que $q' = 1$ et donc $q = 2$. À présent 2.1 est donc $16n = 4k^2 - 4Dp^2$ qui est équivalent à $4n = k^2 - Dp^2$. Puisque p et q sont premiers entre eux et q est pair, nous avons que p est impair tout comme k. Étant donné que des nombres impairs ont un carré congru à 1 modulo 4, nous en déduisons que $k^2 \equiv p^2 \equiv 1 \pmod 4$. L'équation 2.1 modulo 4 nous donne $0 = 1 - D$ et donc $D \equiv 1 \pmod 4$.
Cela signifie que $a \notin \mathbb{Z}$ ne peut survenir que si $D \equiv 1 \pmod 4$. Et donc si $D \equiv 2, 3 \pmod 4$, il faut que $a \in \mathbb{Z}$ et nous avons montré ci-dessus qu'alors $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{D}$. Donc pour $D \equiv 2, 3 \pmod 4$, nous avons tout α de $\mathcal{O}$ est dans $\mathbb{Z} + \mathbb{Z}\sqrt{D}$ donc $\mathcal{O} \subseteq \mathbb{Z} + \mathbb{Z}\sqrt{D}$ qui dans ce cas signifie que $\mathcal{O} \subseteq \mathbb{Z} + \mathbb{Z}\delta$.
Il ne reste plus qu'à traiter le cas où $D \equiv 1 \pmod 4$ et $a \in \mathbb{Z}$. Par les calculs précédents nous savons qu'alors $\alpha = \frac{k}{2} + \frac{p}{2}\sqrt{D}$ où k, p sont impairs. Cette expression peut se réécrire $\alpha = \frac{1+\sqrt{D}}{2} + \frac{k-1}{2} + \frac{(p-1)}{2}\sqrt{D}$. Nous observons alors que $\frac{k-1}{2}$ et $\frac{p-1}{2}$ sont dans $\mathbb{Z}$. De plus, il faut remarquer que $\mathbb{Z} + \mathbb{Z}\sqrt{D} \subset \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2}$. En effet, si nous prenons $x = \frac{1+\sqrt{D}}{2}$ alors nous pouvons écrire $\sqrt{D} = 2x - 1$. En sachant tout cela, il devient alors évident que $\alpha \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2}$ et donc $\mathcal{O} \subseteq \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2}$, ce qui pour $D \equiv 1 \pmod 4$ signifie que $\mathcal{O} \subseteq \mathbb{Z} + \mathbb{Z}\delta$.
Finalement nous avons bien que $\mathcal{O} \subseteq \mathbb{Z} + \mathbb{Z}\delta$ pour chaque cas avec le δ adéquat en fonction de la valeur de D modulo 4.

Enfin, au vu de la manière dont nous pouvons à présent écrire $\mathcal{O}$, nous avons bien que $\mathcal{O}$ est un anneau. □

Nous avions déjà défini ce qu'est une *unité* dans un anneau au chapitre précédent et la remarque 1.7 nous annonçait qu'il était possible de les reconnaître grâce à leur norme. Maintenant que nous avons une définition correcte de la norme d'un nombre quadratique, qui de plus respecte comme indiqué ci-dessous la propriété d'être un homomorphisme, nous pouvons mieux formuler et vérifier cette remarque.

PROPRIÉTÉ 2.9. *Soit* $\mathbb{Q}[\sqrt{D}]$ *un corps quadratique et soient* $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$, $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)$.

Il est alors équivalent de dire qu'un élément du corps quadratique est une unité si et seulement si sa norme est ± 1.

PROPOSITION 2.10. $\epsilon \in \mathcal{O} = \mathbb{Z}[\delta]$ *est une unité si et seulement si* $\mathrm{N}(\epsilon) = \pm 1$.

DÉMONSTRATION. Dans un sens, nous avons que si ϵ est une unité alors il existe $v \in \mathcal{O}$ tel que $\epsilon v = 1$. En prenant la norme cela nous donne que $\mathrm{N}(\epsilon)\,\mathrm{N}(v) = 1$. Et comme les normes sont dans $\mathbb{Z}$, cela implique que $\mathrm{N}(\epsilon) \in \mathbb{Z}^\times = \{\pm 1\}$.
Dans l'autre sens, si $\mathrm{N}(\epsilon) = \epsilon\bar{\epsilon} = \pm 1$, nous avons que $\epsilon^{-1} = \pm\bar{\epsilon} \in \mathcal{O}$. Donc ϵ est bien une unité. □

2. Décomposition des nombres premiers

Nous avions déjà observé au chapitre précédent qu'il existe un lien entre idéaux et nombres premiers, au travers des idéaux principaux premiers. Nous allons développer plus en détails ces liens en abordant notamment les décompositions possibles des nombres premiers.

Tout d'abord, remarquons qu'en plus des idéaux, il est utile de considérer la notion d'*idéaux fractionnaires* afin que ces idéaux forment un groupe puisque ceux de $\mathcal{O}$ n'ont pas d'inverse.
Dans les deux définitions qui suivent, le δ correspond à celui défini dans la proposition 2.8.

DÉFINITION 2.11. *Soit un corps quadratique* F *et* $\mathcal{O}$ *son anneau d'entiers. Un* idéal fractionnaire $\mathcal{I}$ *de* F *par rapport à* $\mathcal{O}$ *est un sous-groupe additif* $\mathcal{I}$ *de* F *qui satisfait les deux conditions suivantes*

— $\mathcal{I} = \mathbb{Z}\alpha + \mathbb{Z}\beta$, *où* $\alpha, \beta \in F$ *sont linéairement indépendants sur* $\mathbb{Z}$;

— $\delta\mathcal{I} \subseteq \mathcal{I}$.

Remarquons qu'il faut faire attention à l'appellation piégeuse puisque les idéaux fractionnaires de F ne sont pas toujours des idéaux de $\mathcal{O}$ (lesquels sont en fait ceux, parmi les idéaux fractionnaires, qui sont inclus dans $\mathcal{O}$). Lorsqu'il y a risque d'ambiguïté les idéaux fractionnaires de $\mathcal{O}$ sont appelés *idéaux entiers*.

REMARQUE 2.12. La deuxième condition de la définition est en fait équivalente à dire que $\mathcal{O}.\mathcal{I} \subseteq \mathcal{I}$, c'est-à-dire que $\mathcal{I}$ est un module sur $\mathcal{O}$. Une autre manière de définir les idéaux fractionnaires de F est de dire que ce sont des sous-$\mathcal{O}$-modules de type fini de F.

REMARQUE 2.13. L'ensemble des idéaux fractionnaires est noté $\mathbb{I}_F$ et est un groupe. En effet, l'ensemble des idéaux non nuls de $\mathcal{O}$, noté $\mathbb{I}_F^+$ satisfait l'associativité, la commutativité et l'annulation pour la multiplication des idéaux [3] mais ne possède qu'un unique élément inversible qui est $\mathcal{O}$ lui-même. La manière dont nous avons défini $\mathbb{I}_F$ nous a permis d'élargir $\mathbb{I}_F^+$ en ajoutant un inverse à tout idéal non nul en conservant les propriétés de $\mathbb{I}_F^+$ et nous obtenons donc un groupe $\mathbb{I}_F$.

Parmi les idéaux fractionnaires se trouvent les *idéaux fractionnaires principaux* qui seront assez utiles et s'écrivent de la manière suivante.

DÉFINITION 2.14. *Pour tout $\alpha \in F\backslash\{0\}$, l'ensemble*

$$\mathcal{O}\alpha = \{\beta\alpha : \beta \in \mathcal{O}\} = \mathbb{Z}\alpha + \mathbb{Z}\delta\alpha$$

est un idéal fractionnaire.
Les idéaux fractionnaires de cette forme sont appelés idéaux fractionnaires principaux.

Voyons à présent ce que deviennent les nombres premiers dans les corps quadratiques. Mais pour cela nous aurons besoin de la définition de *norme d'un idéal* qui elle-même nécessite celle d'*anneau quotient*.

DÉFINITION 2.15. *Soient A un anneau commutatif et I un idéal de A. Nous définissons une relation d'équivalence pour $a, b \in A$ par aRb si et seulement si $a - b \in I$. L'*anneau quotient *A/I est alors l'ensemble des classes d'équivalence de cette relation.*

3. L'annulation provient directement du fait que si I est un idéal de $\mathcal{O}$ alors $I\bar{I} = \mathcal{O}\,\mathrm{N}(I)$ (voir [**1**, Theoreme 4.6.5] ou note au bas de la page suivante). En effet, cela implique que si $I, J, K \subset \mathcal{O}$ et si $IJ = IK$ alors $(I\bar{I})J = (I\bar{I})K$ ce qui implique $\mathrm{N}(I)J = \mathrm{N}(I)K$ et $J = K$ puisque nous pouvons diviser par la norme des deux côtés.
Pour la définition de la norme d'un idéal de $\mathcal{O}$, voir 2.16.

DÉFINITION 2.16. *La* norme d'un idéal $I \subset \mathcal{O}$, $I \neq 0$, $I \neq \mathcal{O}$ *est le nombre naturel* $\mathrm{N}(I) = |\mathcal{O}/I|$.

REMARQUE 2.17. Une fois que nous avons défini la norme d'un idéal de $\mathcal{O}$, une propriété utile à remarquer est que si $I \subset \mathcal{O}$ alors $\mathrm{N}(I)$ divise la norme de tout élément de I. En effet, cela découle du fait que pour tout idéal non nul $I \subset \mathcal{O}$ nous avons que $I\bar{I} = O\,\mathrm{N}(I)$, c'est-à-dire que le produit de l'idéal et de son conjugué est l'idéal principal engendré par leur norme [4]. Mais puisque si $\lambda \in I$ alors la norme $\mathrm{N}(\lambda)$ est dans $I\bar{I}$, cela nous dit que $\mathrm{N}(\lambda)$ est donc dans $\mathcal{O}\,\mathrm{N}(I)$ et donc $\mathrm{N}(I)$ divise $\mathrm{N}(\alpha)$ (puisque $\mathrm{N}(\lambda), \mathrm{N}(I) \in \mathbb{Z}$ et $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$).

C'est la proposition suivante qui nous renseigne sur la décomposition des nombres premiers.

PROPOSITION 2.18. *Soit $p \in \mathbb{Z}$ un nombre premier. La factorisation première de $\mathcal{O}p$ a une des formes suivantes :*

— $\mathcal{O}p = P$ *avec* $\mathrm{N}(P) = p^2$. *Nous disons que p est* inerte.

— $\mathcal{O}p = P^2$ *avec* $\mathrm{N}(P) = p$. *Nous disons que p est* ramifié.

— $\mathcal{O}p = P\bar{P}$ *avec* $\mathrm{N}(P) = p$ *et* $P \neq \bar{P}$. *Nous disons que p est* décomposé.

où le fait qu'un nombre premier p soit *inerte* signifie que p reste premier quand il est vu comme un idéal principal de $\mathcal{O}$.
Les termes *inerte*, *ramifié* et *décomposé* sont aussi utilisés pour parler des idéaux premiers P et $\bar{P}$.

DÉMONSTRATION. Puisqu'il doit exister une factorisation de $\mathcal{O}p$ en idéaux premiers, prenons P un de ces idéaux. La norme de P doit être un diviseur de $\mathrm{N}(\mathcal{O}p) = p^2$, il y a plusieurs cas possibles :

— $\mathrm{N}(P) = p^2$, cela correspond alors au premier cas de l'énoncé ;

— $\mathrm{N}(P) = p$, la factorisation en idéaux premiers étant unique, il faut que $\mathcal{O}p = P\bar{P}$

  • si $P = \bar{P}$ nous sommes dans le deuxième cas de l'énoncé ;

4. Par la multiplication des idéaux il est facile de voir que si I est engendré par α et β alors le produit $I\bar{I}$ est engendré par α, β, $\alpha\bar{\alpha}$ et $\beta\bar{\beta}$. Sans trop de difficulté on peut en fait montrer que $I\bar{I}$ est engendré par $\mathrm{pgcd}(\alpha\bar{\alpha}, \beta\bar{\beta}, \alpha\bar{\beta} + \beta\bar{\alpha})$. Cela revient à montrer que le produit est bel et bien un idéal principal. C'est la multiplicité de la norme qui permet alors de conclure.
Pour une autre preuve de ce fait, le lecteur peut également se référer au livre *Algebraic Theory of Quadratic Numbers*, [**1**, Theoreme 4.6.5].

- sinon nous sommes dans le dernier cas.

□

Ce que cette propriété nous dit est donc qu'il peut y avoir soit $0, 1$ ou 2 idéaux premiers de norme p dans $\mathcal{O}$ en fonction de si p est inerte, ramifié ou décomposé respectivement.

REMARQUE 2.19. Si nous notons Q le polynôme minimal de δ, les différentes décompositions d'un nombre premier p correspondent aux cas suivants : Dans $\mathcal{O}$ un nombre premier p est

— inerte si Q n'a pas de racine dans $\mathbb{F}_p$;

— ramifié si Q a une racine double dans $\mathbb{F}_p$;

— décomposé si Q a deux racines distinctes dans $\mathbb{F}_p$.

3. Groupe de classes d'idéaux

Nous aimerions savoir, étant donné un corps quadratique, si la factorisation dans l'anneau des entiers est unique ou non. Une notion permettant de capturer cette information est celle de *groupe de classes d'idéaux*.
En effet, nous allons voir que lorsque le groupe des classes d'idéaux d'un corps quadratique est trivial, alors la décomposition des entiers en irréductibles est unique à permutation des facteurs près.

Dans cette section nous n'allons pas entrer dans le calcul des groupes de classes d'idéaux qui sera développé dans le chapitre 4.

DÉFINITION 2.20. *Soit $\mathbb{P}_F$ le sous-groupe de $\mathbb{I}_F$ consistant en tous les idéaux fractionnaires principaux. Le quotient*

$$\mathrm{Cl}(F) = \mathbb{I}_F / \mathbb{P}_F$$

est un groupe abélien appelé le groupe de classes d'idéaux *de F.*

Afin de pouvoir faire quelques observations utiles introduisons la notion suivante qui vient s'ajouter à toutes celles déjà rencontrées sur les idéaux.

DÉFINITION 2.21. *Un idéal M d'un anneau A est dit* maximal *si $M \neq A$ et A est le seul idéal contenant strictement M.*

REMARQUE 2.22. Dans l'anneau des entiers d'un corps quadratique, tout idéal premier non nul est maximal. Cela découle directement du fait que pour tout idéal I non nul le quotient $\mathcal{O}/I$ est fini. En particulier, si P est

un idéal premier non nul, $\mathcal{O}/P$ est alors un anneau intègre fini, c'est donc un corps car la multiplication par tout élément non nul est injective donc aussi surjective. Cela entraine que P est maximal [5].

Il est également utile de définir le concept suivant.

DÉFINITION 2.23. *Un anneau A est dit* Noethérien *si tous ses idéaux sont de type fini.*

REMARQUE 2.24. Il existe d'autres manières équivalentes de caractériser un anneau Noethérien mais c'est cette définition qui nous sera utile par la suite.

PROPRIÉTÉ 2.25. *Pour l'anneau $\mathcal{O}$ des entiers d'un corps quadratique, la factorialité et la principalité sont deux propriétés équivalentes.*

DÉMONSTRATION. [6] Par la remarque 1.23 nous savons que tout anneau principal est factoriel. Il ne reste donc plus qu'à vérifier que pour $\mathcal{O}$ le fait d'être factoriel implique le fait d'être principal.

Supposons donc $\mathcal{O}$ factoriel. Commençons par observer que ses idéaux maximaux sont principaux. Soient donc M un idéal maximal et $x \in M$ un élément non nul. Par la factorialité de $\mathcal{O}$ il existe une factorisation unique en facteurs premiers $x = p_1 \cdots p_n$. L'idéal M étant maximal, il est premier et donc l'un des p_i est dans M. Nous avons donc un élément irréductible p_i dans M, nous en obtenons l'inclusion $0 \subset \mathcal{O}p_i \subset M$. Par la remarque 2.22, tout idéal premier non nul est maximal et donc $\mathcal{O}p_i$ est maximal, ce qui entraine que $\mathcal{O}p_i = M$. L'idéal maximal M est donc principal comme souhaité.

Prenons cette fois un idéal I quelconque et voyons qu'il est principal également. Puisque $\mathcal{O}$ est un module de type fini sur $\mathbb{Z}$ et donc en particulier Noethérien nous savons que I est engendré par un nombre fini d'éléments $x_1, \cdots, x_n$. Nous pouvons montrer par récurrence sur n que I est bel et bien principal. Pour $n = 1$ c'est vrai par définition. Il nous suffit de le faire pour $n = 2$. Supposons donc que I soit engendré par x et y, ce que nous notons $I = (x, y)$ pour plus de facilités. Puisque $\mathcal{O}$ est factoriel $d = \text{pgcd}(x, y)$

5. Si ce n'était pas le cas, il existerait $J \subset \mathcal{O}$ contenant P avec x dans J mais pas dans P. La classe de x serait inversible dans $\mathcal{O}/P$, il existerait donc un élément $y \in \mathcal{O}$ et un élément $z \in P$ tels que $z + xy = 1$. Nous aurions donc $1 \in J$. Or, dans un anneau commutatif $\mathcal{O}$ tout idéal contenant 1 est égal à $\mathcal{O}$. Donc $J = \mathcal{O}$, ce qui montre bien que P est maximal.

6. Cette démonstration est inspirée du document *Anneaux d'entiers des corps quadratiques imaginaires* [**4**, Proposition 2.10].

existe. Nous avons alors $x = dx'$ et $y = dy'$ avec x', y' premiers entre eux et donc $I = (x, y) \subset \mathcal{O}d$. Si l'idéal (x', y') n'est pas $\mathcal{O}$ tout entier, il doit alors être contenu dans un idéal maximal. Or, nous venons de montrer que tout idéal maximal est principal, nous aurions alors $(x', y') \subset \mathcal{O}p$ et p diviserait x' et y' ce qui est impossible puisque x' et y' sont premiers entre eux. Nous en déduisons donc que l'idéal engendré par x' et y' est $\mathcal{O}$ tout entier, ce que nous pouvons écrire

$$(x', y') = \mathcal{O} = \mathcal{O}1. \tag{2.2}$$

L'équation 2.2 nous donne la relation de Bézout $1 = \lambda x' + \mu y'$ ou encore $d = \lambda x + \mu y$, cela nous indique que $d \in I$, c'est-à-dire que $\mathcal{O}d \subset I$. Nous en concluons que $I = \mathcal{O}d$ est principal comme souhaité.
Nous venons de démontrer que le fait que $\mathcal{O}$ soit factoriel implique que $\mathcal{O}$ est principal, ce qui conclut la preuve. □

4. Minkowski

Un autre résultat incontournable est la finitude des groupes de classes d'idéaux. Il sera obtenu, entre autres grâce à une *borne de Minkowski* qui requiert la notion de *discriminant de corps*.

DÉFINITION 2.26. *Soit un corps quadratique $F = \mathbb{Q}[\sqrt{D}]$ avec D un entier sans facteur carré, le* discriminant *qui lui est associé est noté D_F. Il dépend de la valeur de D modulo 4.*

$$D_F = \begin{cases} 4D \text{ pour } D \equiv 2, 3 \pmod 4 \\ D \text{ pour } D \equiv 1 \pmod 4 \end{cases}$$

La borne de Minkowski est alors définie de la manière suivante.

DÉFINITION 2.27. *Soit F un corps quadratique, nous définissons la* borne de Minkowski *comme*

$$\mathfrak{M}_F = \sqrt{|D_F|} \cdot \begin{cases} \frac{2}{\pi} \text{ pour } F \text{ imaginaire} \\ \frac{1}{2} \text{ pour réel} \end{cases}$$

Cette borne nous permet d'obtenir deux résultats primordiaux sur les groupes de classes d'idéaux. Le premier concerne son ordre.

PROPOSITION 2.28. *Chaque classe d'idéaux dans* $\mathrm{Cl}(F)$ *contient un idéal de norme au plus $\mathfrak{M}_F$.*

Nous voyons donc que cette proposition nous permet presque de borner le nombre d'éléments dans le groupe de classes d'idéaux. Il suffira d'un

argument supplémentaire pour arriver à la finitude du groupe de classes d'idéaux. C'est ce que nous verrons dans le théorème 2.30.

Le second résultat obtenu à partir de la borne de Minkowski concerne les générateurs de $\mathrm{Cl}(F)$.

PROPOSITION 2.29. *Le groupe de classes d'idéaux d'un corps quadratique F est engendré par un nombre fini de classes $[P]$, où P parcourt les idéaux ayant pour norme un nombre premier borné par $\mathrm{N}(P) \leq \mathfrak{M}_F$.*

Ces deux propositions sont, comme nous le verrons plus concrètement au chapitre 4, indispensables puisque c'est leur combinaison qui sera le squelette du calcul du groupe de classes d'idéaux.

THÉORÈME 2.30 (Finitude du groupe de classes d'idéaux). *Le groupe de classes d'idéaux d'un corps quadratique $\mathrm{Cl}(F)$ est fini.*

DÉMONSTRATION. Nous n'allons pas faire les détails de cette preuve mais simplement en donner les grandes lignes[7].

La finitude du groupe de classes d'idéaux peut être obtenue à partir de la proposition 2.28. En effet, puisqu'elle nous dit que toutes les classes d'idéaux dans $\mathrm{Cl}(F)$ contiennent un idéal de norme au plus $\mathfrak{M}_F$, il suffit de voir qu'il y a seulement un nombre fini d'idéaux non nuls dans $\mathcal{O}$ de norme inférieure à la borne de Minkowski. Faire cela revient à montrer qu'un $k \in \mathbb{N}$ est la norme d'un nombre fini d'idéaux.
En effet, nous pourrions a priori penser qu'il serait possible qu'il y ait une infinité d'idéaux de norme donnée et que le groupe $\mathrm{Cl}(F)$ ne soit alors pas fini. Ce qui nous assure que ce n'est pas le cas est la factorisation unique des idéaux. Soit I_k un idéal de norme disons $k \in \mathbb{N}$ dont la factorisation en entiers premiers est $k = \prod_{i=1}^{n} p_i^{\alpha_i}$. Puisque le produit de $I \subset \mathcal{O}$ avec son conjugué $\bar{I}$ est l'idéal principal engendré par leur norme commune, nous avons alors que $I_k \bar{I}_k = \mathcal{O}k = \prod_{i=1}^{n} P_{p_i}^{\alpha_i} \bar{P}_{p_i}^{\alpha_i}$ et par la factorisation unique des idéaux nous en déduisons qu'il n'y a qu'un nombre fini de possibilités pour I_k.
A présent nous avons donc bien que le groupe de classes d'idéaux est fini et une borne sur son ordre est donné par la propriété précédente. □

7. Remarque : Il y a dans le chapitre suivant une autre preuve de la finitude du nombre de classes pour les corps quadratiques imaginaires. Elle découlera de la réduction des formes quadratiques définies positives et de l'unicité des formes réduites.

Squelette du raisonnement.
Les éléments de la preuve de la finitude du groupe de classes d'idéaux présentés dans cette section sont évidemment corrects mais ils reposent sur d'autres arguments. Dans cette sous-section est présenté un squelette du raisonnement à suivre pour arriver à la conclusion du théorème 2.30. Nous n'entrerons pas dans les détails et il n'y aura pas de preuve le but étant d'apporter l'idée dans les grandes lignes [8].

Il faut savoir que la proposition 2.28 permettant d'obtenir le théorème 2.30 est valable si chaque idéal fractionnaire $\mathcal{I}$ contient un $\alpha \neq 0$ pour lequel $|\mathrm{N}(\alpha)| \leq \mathfrak{M}_F \cdot \mathrm{N}(\mathcal{I})$. [9]

Il nous faudrait alors être sûr que cette condition soit toujours vérifiée afin d'obtenir la finitude de $\mathrm{Cl}(F)$ pour tout corps quadratique F.
Soit la définition suivante de *réseau*.

DÉFINITION 2.31. *Soit V un plan. Un* réseau $\Lambda \subset V$ *est un sous-groupe additif de V de la forme $\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 = \{av_1 + bv_2 \mid a, b \in \mathbb{Z}\}$, où les vecteurs $v_1, v_2 \in V$ ne sont pas colinéaires. Chaque paire $\{v_1, v_2\}$ respectant ces conditions est appelée une* base de Λ.

Le fait est que tout idéal fractionnaire d'un corps quadratique a la propriété géométrique qu'il peut être vu comme un réseau dans le plan complexe. L'idée est alors de trouver un point non nul (α) du réseau $\mathcal{I}$ assez près de l'origine pour respecter la borne sur la norme.
Ce qui est heureux est que l'existence d'un tel point est toujours assurée par un théorème dû à Minkowski. Avant de pouvoir l'énoncer il nous faut la définition d'ensemble *agréable*.

DÉFINITION 2.32. *Un ensemble $S \subseteq \mathbb{R}^2$ est dit* agréable *s'il satisfait les conditions suivantes*

- *S est symétrique centralement autour de 0 : si $x \in S$, alors $-x \in S$;*
- *S est convexe ;*
- *S est mesurable.*

La troisième condition ne doit pas nous préoccuper car elle sera toujours respectée dans les cas qui nous concernent.
Si nous notons $\mathrm{A}(\Lambda)$ l'aire du parallélogramme fondamental du réseau Λ nous pouvons énoncer le théorème.

8. Pour plus de détails, voir le chapitre 5 du livre de Trifković [**1**].
9. Il peut être prouvé que cette condition implique la validité de la proposition 2.28.

THÉORÈME 2.33 (Théorème de Minkowski). *Soient $\Lambda, S \subseteq \mathbb{R}^2$ un réseau et une région agréable. Si $\mathrm{A}(S) > 4\,\mathrm{A}(\Lambda)$, alors il existe un point non nul dans $S \cap \Lambda$. Si S est fermé, la condition plus faible $\mathrm{A}(S) \geq 4\,\mathrm{A}(\Lambda)$ suffit.*

Ce théorème nous sert à obtenir l'existence de notre point α sous certaines conditions mais encore faudrait-il avoir une expression qui convienne pour la borne $\mathfrak{M}_F$.

Cette borne de Minkowski doit être assez grande pour que la condition du théorème de Minkowski soit respectée et que nous ayons un α vérifiant $|\mathrm{N}(\alpha)| \leq \mathfrak{M}_F \cdot \mathrm{N}(\mathcal{I})$. Mais il serait intéressant qu'elle ne soit pas trop grande pour que l'utilisation que nous ferons de la proposition 2.28 lors du calcul de groupe de classes d'idéaux soit pratique.
Nous avons alors deux propositions qui nous aident à déterminer la borne cherchée.

PROPOSITION 2.34. *Soit $\mathcal{I}$ un idéal fractionnaire dans un corps quadratique imaginaire F. Le parallélogramme fondamental de $\mathcal{I}$ a une aire égale à*

$$\mathrm{A}(\mathcal{I}) = \frac{\sqrt{|D_F|}}{2} \cdot \mathrm{N}(\mathcal{I}).$$

À partir de cette proposition la condition d'aire pour pouvoir appliquer le théorème de Minkowski devient, pour un disque S centré à l'origine, $\mathrm{A}(S) \geq 2\sqrt{|D_F|} \cdot \mathrm{N}(\mathcal{I})$. Le plus petit tel disque est donc donné par

$$S = \left\{ z \mid |z| \leq \sqrt{\frac{2}{\pi}\sqrt{|D_F|} \cdot \mathrm{N}(\mathcal{I})} \right\}.$$

Et le théorème de Minkowski nous assure l'existence de $\alpha \neq 0, \alpha \in S \cap \mathcal{I}$ qui est donc tel que $\mathrm{N}(\alpha) \leq \frac{2}{\pi}\sqrt{|D_F|} \cdot \mathrm{N}(\mathcal{I})$ où nous voyons apparaitre $\mathfrak{M}_F = \frac{2}{\pi}\sqrt{|D_F|}$.

Avant de pouvoir faire le même type de raisonnement pour les corps quadratiques réels, il est nécessaire d'utiliser une astuce permettant de voir l'anneau des entiers $\mathcal{O}$, qui dans ce cas est un sous-ensemble dense de la droite réelle, comme un réseau dans le plan et de même pour ses idéaux. Pour cela nous définissons l'injection $\rho : F \hookrightarrow \mathbb{R}^2, \rho(\alpha) = (\bar{\alpha}, \alpha)$. De cette façon pour chaque idéal fractionnaire $\mathcal{I}$, $\rho(\mathcal{I})$ est un réseau et nous avons la proposition ci-dessous.

PROPOSITION 2.35. *Soit $\mathcal{I}$ un idéal fractionnaire dans un corps quadratique réel F. Le parallélogramme fondamental de $\rho(\mathcal{I})$ a une aire égale à*

$$\mathrm{A}(\mathcal{I}) = \sqrt{|D_F|} \cdot \mathrm{N}(\mathcal{I}).$$

En utilisant un raisonnement semblable à celui pour le cas imaginaire (bien que l'obtention d'un S agréable soit un peu moins directe) nous trouvons un $\alpha \neq 0$ tel que $|\mathrm{N}(\alpha)| \leq \frac{\sqrt{D_F}}{2} \cdot \mathrm{N}(\mathcal{I})$, nous en tirons que $\mathfrak{M}_F = \frac{\sqrt{D_F}}{2}$.

Nous avons à présent les expressions de $\mathfrak{M}_F$ données dans la définition 2.26 et nous avons une meilleure idée de pourquoi il y a une différence en fonction de si le corps quadratique est imaginaire ou réel.
C'est ce qui termine de tracer les grandes lignes de la preuve de la finitude du groupe de classes d'idéaux d'un corps quadratique.

Chapitre 3

Correspondance entre idéaux et formes quadratiques

Dans ce troisième chapitre nous allons aborder les formes quadratiques qui jouent un rôle important dans la recherche d'informations sur le groupe de classes d'idéaux. En effet, il existe une correspondance entre les idéaux et ces formes quadratiques. Cela permettra, comme nous le verrons dans le chapitre suivant, d'approcher d'une manière différente le calcul du groupe de classes d'idéaux d'un corps quadratique et même dans certains cas de le simplifier.

Nous considérons pour ce chapitre que le lecteur a des bases solides en théorie des groupes.

1. Formes quadratiques

Dans cette première section nous allons simplement aborder des notions théoriques qui nous seront utiles lorsque nous souhaiterons faire le parallèle avec les idéaux.

Commençons par définir les *applications quadratiques*.

DÉFINITION 3.1. *Soient un $\mathbb{Z}$-module Λ libre de rang 2 et une application $\varphi : \Lambda \to \mathbb{Z}$. Si elle satisfait les deux conditions suivantes*

- *$\varphi(\lambda z) = \varphi(\lambda) z^2$ pour $\lambda \in \Lambda$ et $z \in \mathbb{Z}$;*
- *l'application $b_\varphi : \Lambda \times \Lambda \to \mathbb{Z}$ définie par $b_\varphi(\lambda, \mu) = \varphi(\lambda + \mu) - \varphi(\lambda) - \varphi(\mu)$ est bilinéaire;*

elle est appelée application quadratique.
La paire (Λ, φ) est un module quadratique.

Les *formes quadratiques* considérées dans ce chapitre seront alors les suivantes.

DÉFINITION 3.2. *Soit $e = (\alpha, \beta)$ une base de Λ, alors pour $x, y \in \mathbb{Z}$*

$$\varphi(\alpha x + \beta y) = \varphi(\alpha x) + b_\varphi(\alpha x, \beta y) + \varphi(\beta y) = \varphi(\alpha) x^2 + b_\varphi(\alpha, \beta) xy + \varphi(\beta) y^2.$$

La forme quadratique *associée à l'application φ par rapport à la base e est alors notée*

$$\varphi_e \left(\begin{smallmatrix} X \\ Y \end{smallmatrix} \right) = \varphi(\alpha) X^2 + b_\varphi(\alpha, \beta) XY + \varphi(\beta) Y^2 \in \mathbb{Z}[X, Y].$$

Elle peut également s'écrire sous forme matricielle

$$\varphi_e\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = (X\ Y) \begin{pmatrix} \varphi(\alpha) & \frac{1}{2}b_\varphi(\alpha,\beta) \\ \frac{1}{2}b_\varphi(\alpha,\beta) & \varphi(\beta) \end{pmatrix} \left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right).$$

En notant $M(\varphi_e)$ la matrice carrée du membre de droite, nous avons

$$\varphi(\alpha x + \beta y) = (x\ y) M(\varphi_e) \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \qquad \textit{pour } x, y \in \mathbb{Z}.$$

REMARQUE 3.3. Observons que

$$b_\varphi(\alpha,\alpha) = \varphi(2\alpha) - 2\varphi(\alpha) = 4\varphi(\alpha) - 2\varphi(\alpha) = 2\varphi(\alpha)$$

et donc $\varphi(\alpha) = \frac{1}{2}b_\varphi(\alpha,\alpha)$. De même $\varphi(\beta) = \frac{1}{2}b_\varphi(\beta,\beta)$. La matrice $M(\varphi_e)$ peut alors s'écrire

$$M(\varphi_e) = \frac{1}{2}\begin{pmatrix} b_\varphi(\alpha,\alpha) & b_\varphi(\alpha,\beta) \\ b_\varphi(\alpha,\beta) & b_\varphi(\beta,\beta) \end{pmatrix}.$$

Puisque la définition de forme quadratique est liée à la base e, il est utile de voir l'effet d'un changement de base. Pour cela utilisons la bilinéarité de b_φ.

Soit $e' = (\alpha', \beta')$ une autre base de Λ. Nous pouvons trouver une matrice carrée inversible $A \in \mathrm{GL}_2(\mathbb{Z})$ telle que $e' = e \cdot A$. C'est-à-dire que si

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{alors} \quad \alpha' = \alpha a_{11} + \beta a_{21} \quad \text{et} \quad \beta' = \alpha a_{12} + \beta a_{22}.$$

Dans ce cas, par bilinéarité de b_φ, nous avons

$$M(\varphi_{e'}) = A^t \cdot M(\varphi_e) \cdot A$$

ce qui implique

$$\varphi_{e'}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = (X\ Y) M(\varphi_{e'}) \left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = (X\ Y) A^t \cdot M(\varphi_e) \cdot A \left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = \varphi_e\left(A\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)\right).$$

Ces changements base nous mènent à la définition de formes quadratiques *équivalentes*.

DÉFINITION 3.4. *Deux formes quadratiques $q, q' \in \mathbb{Z}[X,Y]$ sont dites* équivalentes *s'il existe une matrice $A \in \mathrm{GL}_2(\mathbb{Z})$ telle que*

$$q'\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = q\left(A\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)\right) \qquad \textit{c'est-à-dire} \qquad M(q') = A^t M(q) A.$$

On note alors $q' = q^A$.
Si de plus $A \in \mathrm{SL}_2(\mathbb{Z})$, nous dirons que q et q' sont proprement équivalentes.

Nous remarquons que deux formes quadratiques associées à une même application quadratique mais par rapport à des bases différentes sont alors équivalentes, $\varphi_{eA}\left(\begin{smallmatrix}X\\Y\end{smallmatrix}\right) = \varphi_e^A\left(\begin{smallmatrix}X\\Y\end{smallmatrix}\right) = \varphi_e\left(A\left(\begin{smallmatrix}X\\Y\end{smallmatrix}\right)\right)$. Cela établit un lien direct entre changement de base d'un module quadratique et changement de variables dans une forme quadratique.

2. Invariants

Plusieurs invariants sont associés aux formes quadratiques.

Voyons-en ici deux à valeurs dans $\mathbb{Z}$ qui sont le *discriminant* et le *contenu*. Observons tout d'abord que si deux formes quadratiques $q, q' \in \mathbb{Z}[X,Y]$ sont équivalentes, puisque le déterminant de toute matrice $A \in \mathrm{GL}_2(Z)$ est ± 1, nous avons que

$$\det(M(q')) = \det(A^t M(q) A) = (\pm 1)\det(M(q))(\pm 1) = \det(M(q)),$$

les déterminants des matrices associées sont égaux.

DÉFINITION 3.5. *Le* discriminant d'une forme quadratique *est donné par*

$$\mathrm{disc}(q) = -4\det(M(q)),$$

de sorte que $\mathrm{disc}(aX^2 + bXY + cY^2) = b^2 - 4ac$.

Il est alors évident que deux formes équivalentes ont même discriminant, ce qui nous permet de définir le *discriminant d'un module quadratique*.

DÉFINITION 3.6. *Le* discriminant d'un module quadratique (Λ, φ) *est défini comme le discriminant de la forme quadratique associée à l'application quadratique* φ *par rapport à n'importe quelle base.*

Le discriminant des formes quadratiques permet également de les caractériser grâce à la définition suivante.

DÉFINITION 3.7. *Une forme quadratique q est dite :*

- indéfinie *si* $\mathrm{disc}(q) > 0$. *Dans ce cas q peut tout aussi bien prendre une valeur positive ou négative.*
- définie *si* $\mathrm{disc}(q) < 0$. *Dans ce cas, a et c doivent avoir le même signe. Nous dirons que q est*
  - définie positive *si* $a, c > 0$, *donc* $q(x,y) > 0$ *pour tout* $x, y \in \mathbb{Z}$ *non nuls ;*
  - définie négative *si* $a, c < 0$, *donc* $q(x,y) < 0$ *pour tout* $x, y \in \mathbb{Z}$ *non nuls.*

REMARQUE 3.8. Dans ce document nous nous intéressons aux corps quadratiques imaginaires, c'est pourquoi ce sont les formes quadratiques définies qui retiendront plus particulièrement notre attention dans ce chapitre.

La définition de *contenu* ci-dessous va ensuite nous permettre de définir ce qu'est une forme quadratique *primitive*.

DÉFINITION 3.9. *A tout module quadratique* (Λ, φ) *(resp. forme quadratique* q*) on associe l'idéal de* $\mathbb{Z}$ *engendré par les* $\varphi(\lambda)$ *pour* $\lambda \in \Lambda$ *(resp. par les* $q\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ *pour* $x, y \in \mathbb{Z}$*). C'est cet idéal qui est appelé le* contenu *de* (Λ, φ) *(resp. de* q*). On le note* $\mathrm{cont}(q)$.

DÉFINITION 3.10. *Une forme quadratique* q *est dite* primitive *si*

$$\mathrm{cont}(q) = \mathbb{Z}.$$

PROPOSITION 3.11. *Soit une forme quadratique* $q = aX^2 + bXY + cY^2$ *son contenu est l'idéal engendré par* a, b *et* c *ou, de manière équivalente, par le plus grand commun diviseur de* a, b *et* c*. En particulier,* q *est primitive si et seulement si* a, b *et* c *sont premiers entre eux.*

DÉMONSTRATION. L'inclusion $\mathrm{cont}(q) \subseteq a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z}$ est évidente puisque $ax^2 + bxy + cy^2$ est une combinaison linéaire à coefficients entiers des a, b et c pour $x, y \in \mathbb{Z}$.
Réciproquement, nous avons

$$a = q\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \qquad a + b + c = q\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right), \qquad c = q\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right),$$

donc $a, b, c \in \mathrm{cont}(q)$ et par conséquent $a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z} \subseteq \mathrm{cont}(q)$. □

3. Réduction des formes quadratiques

Une autre notion indispensable pour la suite et que nous allons développer dans cette section est celle de *forme quadratique réduite*.

DÉFINITION 3.12. *Une forme quadratique* $q\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = aX^2 + bXY + cY^2$ *est dite* réduite *si*

$$|b| \leq |a| \leq |c|$$

et $b \geq 0$ *quand* $|a| = |b|$ *ou* $|a| = |c|$.

Une chose importante est que si nous avons une forme quadratique quelconque $q\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = aX^2 + bXY + cY^2$, elle est toujours proprement équivalente à une unique forme quadratique réduite comme nous allons le voir

dans une proposition ultérieure.
En effet, si $T^k = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ alors il suffit de lui appliquer un nombre fini de changements de variables parmi les deux types suivants.

— $(q^{T^k})\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = q\left(T^k\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)\right) = q\left(\begin{smallmatrix} X-kY \\ Y \end{smallmatrix}\right) = aX^2 + (b-2ak)XY + (ak^2 - bk + c)Y^2$, $k \in \mathbb{Z}$.

— $(q^S)\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = q\left(\begin{smallmatrix} Y \\ -X \end{smallmatrix}\right) = cX^2 - bXY + aY^2$.

Nous remarquons que chaque forme quadratique obtenue suite à l'application d'un de ces changements de variables est proprement équivalente à la précédente puisque $T^k, S \in \mathrm{SL}_2(\mathbb{Z})$.
Nous avons alors la proposition suivante qui nous assure que nous pouvons toujours réduire une forme quadratique.

PROPOSITION 3.13. *Pour toute forme quadratique, il existe une suite de changements de variables linéaires du type T^k ou S qui produit une forme quadratique $aX^2 + bXY + cY^2$ réduite.*

C'est un résultat général que nous ne prouvons ici que pour le cas où la forme quadratique est définie. En particulier, il nous suffit de le prouver pour les formes définies positives puisque les formes définies négatives peuvent alors être obtenues en multipliant une forme définie positive par un facteur -1. C'est pour cela que les valeurs absolues pour a et c apparaissant dans la définition de forme réduite ne sont plus présentes dans cette démonstration.

DÉMONSTRATION. Si nous souhaitons réduire une forme quadratique il nous faut lui appliquer l'algorithme de réduction pour les formes définies suivant.

(1) INPUT : coefficients $a, b, c \in \mathbb{Z}$. Posons $q\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = aX^2 + bXY + cY^2$.
(2) Une variante de l'algorithme de division donne $k, r \in \mathbb{Z}$ tels que $b = k(2a) + r$ et $|r| \leq a$. Le changement de variable $q := q^{T^k}$ pour ce k donne une forme quadratique telle que $|b| \leq a$.
(3) Si $a \leq c$ aller à l'étape 5.
(4) Poser $q := q^S$ afin de produire une forme quadratique avec $a \leq c$ et retourner à l'étape 2.
(5) Si $b = -a$, poser $q := q^T$ pour remplacer $aX^2 - aXY + cY^2$ par $aX^2 + aXY + cY^2$.

(6) Si $b < 0$ et $a = c$, poser $q := q^S$ pour remplacer $aX^2 + bXY + cY^2$ par $cX^2 - bXY + aY^2$.

(7) OUTPUT : $q\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)$.

Nous observons d'une part que la forme quadratique obtenue est bien proprement équivalente à la forme quadratique de départ car la forme obtenue est du type $q^P\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = q\left(P\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)\right)$ où P est un produit de matrices du type T^k et S qui sont toutes les deux dans $\mathrm{SL}_2(\mathbb{Z})$ qui est un groupe sous la multiplication matricielle.
Et d'autre part, elle est bien une forme réduite et le processus s'arrête bien. En effet, en appliquant l'algorithme $|b|$ ne fait que diminuer à l'étape (2) ou rester constante à l'étape (4). Or, l'étape (4) n'est pas appliquée deux fois de suite ce qui entraine que $|b|$ continue à diminuer et nous finissons par sortir de la boucle faite des étapes (2) et (4). Et dans le cas où nous aurions $b < 0$ alors que $a = |b|$ ou $a = c$, les étapes (4) ou (5) permettent de changer b en $-b$. □

4. Action de $\mathrm{SL}_2(\mathbb{Z})$ sur les formes quadratiques et leurs paramètres

Une chose très importante pour le calcul du groupe de classes d'idéaux est la correspondance entre les formes quadratiques et les idéaux fractionnaires d'un corps quadratique imaginaire.

REMARQUE 3.14. Nous aurons besoin dans cette section de savoir comment est défini le signe de la racine carrée d'un nombre négatif.
Soit $D < 0$, le corps quadratique imaginaire $F = \mathbb{Q}[\sqrt{D}]$ peut être identifié au sous-corps de $\mathbb{C}$ engendré par $i\sqrt{-D}$ (où $\sqrt{-D}$ est la racine carrée positive du nombre naturel $-D$, et est donc un nombre réel positif).
Pour $d < 0$, $\sqrt{d}$ dénote donc la racine carrée ayant sa partie imaginaire positive, c'est-à-dire $i\sqrt{-d}$ et non $-i\sqrt{-d}$.

Avant d'entrer dans le vif du sujet de cette section, définissons les ensembles $\mathcal{Q}$ et $\mathcal{H}$.

DÉFINITION 3.15. *Les ensembles $\mathcal{Q}$ et $\mathcal{H}$ sont respectivement l'ensemble de toutes les formes quadratiques entières primitives et définies positives et l'ensemble de tous les nombres complexes qui sont des éléments irrationnels de corps quadratiques imaginaires.*

Dans le contexte de ce chapitre nous utiliserons plus particulièrement les formes quadratiques entières primitives définies positives, de discriminant D fixé et donc $\mathcal{Q}_D$.

DÉFINITION 3.16. *Soit $D < 0$ un entier strictement négatif. L'ensemble $\mathcal{Q}_D$ est simplement défini par*

$$\mathcal{Q}_D = \{q \in \mathcal{Q} \mid \mathrm{disc}(q) = D\}.$$

Tout comme nous avons $\mathcal{Q}$ et $\mathcal{H}$, puisque nous avons défini $\mathcal{Q}_D$ nous pouvons définir $\mathcal{H}_D$.

DÉFINITION 3.17. $\mathcal{H}_D = \{u + v\sqrt{D} \mid u, v \in \mathbb{Q}, v > 0\} \subset \mathbb{C}$.

Il se fait que ces deux ensembles $\mathcal{Q}_D$ et $\mathcal{H}_D$ peuvent être mis en bijection. Afin de voir comment, intéressons nous à un autre objet nécessaire lorsque nous parlons de formes quadratiques et de correspondance avec les idéaux qui est le *paramètre d'une forme quadratique*. C'est la *fonction paramètre* qui envoie une forme quadratique sur le paramètre qui lui est associé.

DÉFINITION 3.18. *La* fonction paramètre $\iota_{\mathcal{Q}_D\mathcal{H}_D} : \mathcal{Q}_D \to \mathcal{H}_D$ *est donnée par*

$$q\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = aX^2 + bXY + cY^2 \mapsto \eta_q = \frac{-b + \sqrt{D}}{2a}.$$

Le paramètre *de la forme quadratique q est donc η_q.*

Le paramètre η_q est en fait l'unique racine du polynôme $q\left(\begin{smallmatrix} X \\ 1 \end{smallmatrix}\right)$ se trouvant dans le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C} \mid \Im z > 0\}$ où $\Im z$ est la partie imaginaire du nombre complexe z. Ou encore, pour toute forme quadratique $q \in \mathcal{Q}_D$, η_q est la seule racine du polynôme $q\left(\begin{smallmatrix} X \\ 1 \end{smallmatrix}\right)$ dans $\mathcal{H}_D$.

Réciproquement, tout $\eta = u + v\sqrt{D} \in \mathcal{H}_D$ est racine d'un unique polynôme quadratique unitaire de discriminant D à coefficients rationnels qui est $X^2 - 2uX + (u^2 - Dv^2)$. Nous pouvons alors associer à ce polynôme une forme quadratique primitive définie positive dans $\mathcal{Q}_D$ en chassant les dénominateurs, c'est cette forme quadratique qui est la *forme quadratique associée au paramètre*.

DÉFINITION 3.19. *Soit le paramètre $\eta = u + v\sqrt{D}$ de $\mathcal{H}_D$, la forme quadratique q_η de $\mathcal{Q}_D$ qui lui est associée est*

$$q_\eta\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = aX^2 + bXY + cY^2$$

où a est le plus petit commun dénominateur positif de $-2u$ et $u^2 - Dv^2$, $b = -2ua$ et $c = (u^2 - Dv^2)a$.

REMARQUE 3.20. Cette forme quadratique associée est bien dans $\mathcal{Q}_D$ puisque par le choix de a nous avons que $a > 0$ et $\mathrm{pgcd}(a, b, c) = 1$ et par

construction le discriminant est D.
De plus, cette forme quadratique a été obtenue de manière unique.

Tout comme nous avions défini $\iota_{\mathcal{Q}\mathcal{H}}$ nous pouvons maintenant définir $\iota_{\mathcal{H}\mathcal{Q}}$.

DÉFINITION 3.21. *L'application $\iota_{\mathcal{H}_D\mathcal{Q}_D}$ définie par $\eta \mapsto q_\eta$ associe à chaque paramètre de $\mathcal{H}_D$ une forme quadratique dans $\mathcal{Q}_D$.*

C'est alors que nous pouvons remarquer que $\mathcal{Q}_D$ et $\mathcal{H}_D$ sont en bijection et donc que $\mathcal{H}_D$ est l'ensemble des paramètres associés aux formes quadratiques de $\mathcal{Q}_D$. En effet, nous avons la proposition suivante.

PROPOSITION 3.22. *Les applications $\iota_{\mathcal{H}_D\mathcal{Q}_D}$ et $\iota_{\mathcal{Q}_D\mathcal{H}_D}$ sont des bijections réciproques entre $\mathcal{Q}_D$ et $\mathcal{H}_D$.*

DÉMONSTRATION. Par définition de q_η, nous avons que $q_\eta\left(\begin{smallmatrix}\eta\\1\end{smallmatrix}\right) = 0$. Par définition de paramètre associé à une forme quadratique, cela nous montre que $\iota_{\mathcal{Q}_D\mathcal{H}_D} \circ \iota_{\mathcal{H}_D\mathcal{Q}_D} = \mathrm{Id}_{\mathcal{H}_D}$.
Réciproquement, si nous démarrons d'une forme quadratique

$$q\left(\begin{smallmatrix}X\\Y\end{smallmatrix}\right) = aX^2 + bXY + cY^2 \text{ dans } \mathcal{Q}_D$$

nous avons par définition que $\eta_q = \frac{-b+\sqrt{D}}{2a} = \frac{-b}{2a} + \frac{1}{2a}\sqrt{D}$. Si nous calculons maintenant q_{η_q}, nous avons par définition que

$$q_{\eta_q}\left(\begin{smallmatrix}X\\Y\end{smallmatrix}\right) = aX^2 - 2\frac{-b}{2a}aXY + a\Big(\big(\frac{-b}{2a}\big)^2 - D\big(\frac{1}{2a}\big)^2\Big)Y^2 = aX^2 + bXY + cY^2 = q\left(\begin{smallmatrix}X\\Y\end{smallmatrix}\right).$$

Et donc $\iota_{\mathcal{H}_D\mathcal{Q}_D} \circ \iota_{\mathcal{Q}_D\mathcal{H}_D} = \mathrm{Id}_{\mathcal{Q}_D}$. □

Comme nous savons qu'à chaque forme quadratique est associé un paramètre, il est logique de penser qu'un changement de variable de la forme quadratique doit se faire ressentir au niveau du paramètre également. C'est ce à quoi nous allons nous intéresser.

REMARQUE 3.23. Une chose à voir est que comme $q \in \mathcal{Q}_D$ est un polynôme homogène, nous avons que, pour $x, y \in \mathbb{C}$ tels que $y \neq 0$, $q\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) = 0$ si et seulement si $q\left(\begin{smallmatrix}\frac{x}{y}\\1\end{smallmatrix}\right) = 0$.

NOTATION 3.24. Dans la suite, dès que nous parlerons d'une matrice $A \in \mathrm{GL}_2(\mathbb{Z})$, nous la supposerons de la forme $A = \begin{pmatrix} j & k \\ l & m \end{pmatrix}$ par pure préférence visuelle au niveau des calculs.

La remarque 3.23 entraine que pour $A \in \mathrm{GL}_2(\mathbb{Z})$ et pour $\eta \in \mathcal{H}_D$, $q^A\left(\begin{smallmatrix}\eta\\1\end{smallmatrix}\right) = q\left(A\left(\begin{smallmatrix}\eta\\1\end{smallmatrix}\right)\right) = q\left(\begin{smallmatrix}j\eta+k\\l\eta+m\end{smallmatrix}\right) = 0$ si et seulement si $q\left(\begin{smallmatrix}\frac{j\eta+k}{l\eta+m}\\1\end{smallmatrix}\right) = 0$ c'est-à-dire si et seulement si $\frac{j\eta+k}{l\eta+m}$ est racine du polynôme $q\left(\begin{smallmatrix}X\\1\end{smallmatrix}\right)$. Nous avons donc la définition suivante que nous écrivons de manière générale pour tout le demi-plan complexe supérieur $\mathbb{H}$.

DÉFINITION 3.25. *Soient $A \in \mathrm{GL}_2(\mathbb{Z})$ et $\eta \in \mathbb{H}$. L'action de A sur $q \in \mathcal{Q}_D$ entraine une action sur les paramètres et nous posons*

$$^A\eta = \frac{j\eta + k}{l\eta + m} \in \mathbb{C}.$$

Remarquons que le dénominateur dans la définition ci-dessus n'est pas nul. En effet, $\eta \neq 0$ puisque sa partie imaginaire est strictement positive et l et m ne peuvent pas être simultanément égaux à zéro sans quoi la matrice A ne serait pas dans $\mathrm{GL}_2(\mathbb{Z})$.

REMARQUE 3.26. Une chose que nous pouvons remarquer et qui sera utile pour la suite est que l'action de $\mathrm{SL}_2(\mathbb{Z})$ préserve $\mathbb{H}$.

Soit $\eta = u + vi \in \mathbb{H}$ et $^A\eta$ tel que défini ci-dessus. Nous calculons que

$$^A\eta = \frac{(ju+k)+jvi}{(lu+m)+lvi} = \frac{(ju+k)(lu+m)+jlv^2}{(lu+m)^2+l^2v^2} + \frac{(jm-kl)vi}{(lu+m)^2+l^2v^2}.$$

La partie imaginaire de $^A\eta$ est donc

$$\frac{(jm-kl)v}{(lu+m)^2+l^2v^2} = \frac{\det(A)v}{(lu+m)^2+l^2v^2}.$$

Le dénominateur est strictement positif, de même pour v (puisque $\eta \in \mathbb{H}$ par hypothèse), il ne reste donc que $\det(A)$. Mais si $A \in \mathrm{SL}_2(\mathbb{Z})$ alors $\det(A) = 1$ et $^A\eta \in \mathbb{H}$.

Une chose intéressante est que la correspondance entre $\mathcal{Q}_D$ et $\mathcal{H}_D$ est équivariante pour l'action de $\mathrm{SL}_2(\mathbb{Z})$.

PROPOSITION 3.27. *Soit $A \in \mathrm{SL}_2(\mathbb{Z})$, les applications $\iota_{\mathcal{Q}_D\mathcal{H}_D}$ et $\iota_{\mathcal{H}_D\mathcal{Q}_D}$ sont $\mathrm{SL}_2(\mathbb{Z})$-équivariantes.*
C'est-à-dire que pour tout $q \in \mathcal{Q}_D$ une forme quadratique ayant pour paramètre $\eta_q \in \mathcal{H}_D$, le paramètre de q^A est $\eta_{q^A} = {}^A\eta_q$. De même, pour tout $\eta \in \mathcal{H}_D$ de forme quadratique associée $q_\eta \in \mathcal{Q}_D$, la forme quadratique associée de $^A\eta$ est $q_{^A\eta} = q_\eta^A$.

DÉMONSTRATION. Soient $\eta = u + v\sqrt{D} \in \mathcal{H}_D$ et ${}^A\eta$ tel que défini ci-dessus. Par un calcul similaire à celui de la remarque 3.26 nous avons que

$${}^A\eta = \frac{(ju+k)(lu+m) - jlv^2D}{(lu+m)^2 - l^2v^2D} + \frac{(jm-kl)v\sqrt{D}}{(lu+m)^2 - l^2v^2D}.$$

Il en découle que

$${}^A\eta - \overline{{}^A\eta} = 2\frac{(jm-kl)v\sqrt{D}}{(lu+m)^2 - l^2v^2D} = \frac{\det(A)(\eta - \overline{\eta})}{\mathrm{N}((lu+m) + lv\sqrt{D})}.$$

Or, nous savons qu'un nombre complexe ξ est compris dans le demi-plan supérieur $\mathbb{H} = \{z \in \mathbb{C} \mid \Im z > 0\}$ si et seulement si $i(\xi - \bar{\xi}) < 0$.
Dans notre cas, puisque $\eta \in \mathcal{H}_D \subset \mathbb{H}$, nous avons que $i(\eta - \bar{\eta}) < 0$ et donc

$$\begin{aligned} i({}^A\eta - \overline{{}^A\eta}) < 0 &\Leftrightarrow \tfrac{\det(A)i(\eta-\overline{\eta})}{\mathrm{N}((lu+m)+lv\sqrt{D})} < 0 \\ &\Leftrightarrow \tfrac{\det(A)}{\mathrm{N}((lu+m)+lv\sqrt{D})} > 0 \\ &\Leftrightarrow \det(A) > 0 \\ &\Leftrightarrow A \in \mathrm{SL}_2(\mathbb{Z}) \end{aligned}$$

ce qui nous montre que ${}^A\eta$ est dans le demi-plan supérieur et donc dans $\mathcal{H}_D$ si est seulement si $A \in \mathrm{SL}_2(\mathbb{Z})$.

Par la définition de ${}^A\eta$ et les calculs ci-dessus il devient évident que $\iota_{\mathcal{Q}_D\mathcal{H}_D}(q^A) = {}^A\iota_{\mathcal{Q}_D\mathcal{H}_D}(q)$ et que $\iota_{\mathcal{H}_D\mathcal{Q}_D}({}^A\eta) = \iota_{\mathcal{H}_D\mathcal{Q}_D}(\eta)^A$, ce qui conclut. □

Les notions que nous venons de voir peuvent entre autres être utilisées pour prouver qu'à toute forme quadratique $q \in \mathcal{Q}_D$ est associée une unique forme quadratique réduite. C'est ce que nous allons faire dans la suite de cette section.

Pour cela, intéressons nous plus en détails à l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{H}_D$. Nous avons démontré ci-dessus que si $\eta \in \mathcal{H}_D$ et si $A \in \mathrm{SL}_2(\mathbb{Z})$ alors ${}^A\eta \in \mathcal{H}_D$ ce qui signifie que η et ${}^A\eta$ sont $SL_2(\mathbb{Z})$-équivalents. Il existe donc des orbites $\mathrm{SL}_2(\mathbb{Z})\eta$ pour l'action de $\mathrm{SL}_2(\mathbb{Z})$.
Cela entraine que nous pouvons trouver un domaine fondamental de $\mathcal{H}_D$ pour l'action de $\mathrm{SL}_2(\mathbb{Z})$, c'est ce que nous allons faire.

Nous avons déjà défini le demi-plan complexe supérieur $\mathbb{H}$ et nous savons que $\mathcal{H}_D \subset \mathbb{H}$. Nous avons également une action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$, il nous suffit de définir, pour $z \in \mathbb{H}$ et $A \in \mathrm{SL}_2(\mathbb{Z})$, ${}^Az = \frac{jz+k}{lz+m}$ que est bien dans $\mathbb{H}$ par la remarque 3.26.
Considérons la région du demi-plan supérieur suivante

$$\mathcal{F} = \{z \in \mathbb{H} \mid |\Re(z)| < \frac{1}{2}, |z| > 1\} \sqcup \{-\frac{1}{2} + yi \mid y \geq \frac{\sqrt{3}}{2}\} \sqcup \{z \in \mathbb{H} \mid -\frac{1}{2} \leq \Re(z) \leq 0, |z| = 1\}.$$

La proposition ci-dessous nous montre que c'est un domaine fondamental pour l'action de $\mathrm{SL}_2(\mathbb{Z})$.

PROPOSITION 3.28. *La région $\mathcal{F}$ est un domaine fondamental pour l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$.*

DÉMONSTRATION. L'idée pour vérifier cela est de montrer que chaque $z \in \mathbb{H}$, à l'aide d'actions répétées de matrices dans $\mathrm{SL}_2(\mathbb{Z})$, peut être amené en un unique point de $\mathcal{F}$.
Nous n'avons pour cela besoin que des matrices déjà rencontrées T et S qui, rappelons-le, sont telles que $T^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
C'est l'algorithme de réduction pour $\mathbb{H}$ suivant qui permet de voir comment $z \in \mathbb{H}$ peut être amené sur son représentant dans $\mathcal{F}$.

(1) INPUT : $z \in \mathbb{H}$. Poser $z_0 := z$, $M := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et mettre le compteur à zéro $i := 0$.

(2) Choisir $a \in \mathbb{Z}$ tel que $z_i + a$ soit dans la bande $|w| \leq \frac{1}{2}$. Poser $z_{i+1} := z_i + a = {}^{T^{-a}}z_i$, $M := T^{-a}M$, et $i := i + 1$.

(3) Si $|z_i| \geq 1$, aller à l'étape (5).

(4) Poser $z_{i+1} := -\frac{1}{z_i} = {}^{S^{-1}}z_i$, $M := S^{-1}M$, $i := i + 1$ et aller à l'étape (2).

(5) (Condition au bord) Si $\Re(z_i) = \frac{1}{2}$, poser $z_i := z_i - 1$ et $M := TM$, de façon à ce que maintenant $\Re(z) = -\frac{1}{2}$.

(6) (Condition au bord) Si $|z_i| = 1$ et $0 < \Re(z_i) < \frac{1}{2}$, poser $z_i := -\frac{1}{z_i}$ et $M := S^{-1}M$, de façon à ce que maintenant $|z_i| = 1$ ainsi que $-\frac{1}{2} < \Re(z_i) < 0$.

(7) OUTPUT : $z_i = Mz \in \mathcal{F}$ est un point $\mathrm{SL}_2(\mathbb{Z})$-équivalent à z et M est la matrice qui déplace z sur z_i.

Cet algorithme est construit sur l'idée d'après laquelle répéter un certain nombre de fois l'action de T permet de déplacer z dans la bande $|\Re(z)| \leq \frac{1}{2}$ et l'action de S permet d'interchanger l'intérieur et l'extérieur du demi-disque $|z| \leq 1$.

Il nous reste encore à prouver que nous sortons toujours de cet algorithme et que le z_i obtenu est bien le seul représentant de l'orbite $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathcal{F}$ afin que ce soit bien un domaine fondamental.

La raison pour laquelle la procédure de l'algorithme se termine est que si ce n'était pas le cas nous devrions avoir que l'étape (3) permettant d'en

sortir ne devrait jamais être satisfaite.
Cela signifierait que toujours nous aurions $|z_i| < 1$ et puisque $z_i \in \mathbb{H}$ cela entraine que $\Im(z_i) < 1$ pour tout $i \geq 0$. Nous effectuerions donc une boucle composée des étapes (2), (3) et (4).
Or, de manière générale, pour $A \in \mathrm{SL}_2(\mathbb{Z})$, nous observons par un raisonnement similaire à celui effectué dans la démonstration de la propriété 3.27 que $\Im^A z = \frac{\det(A)}{|lz+m|^2}\Im z = \frac{\Im z}{|lz+m|^2}$. Et dans le cas particulier des matrices T^{-1} et S^{-1} qui nous intéressent, nous avons que soit $|lz+m|^2 = 1$ soit $|lz+m|^2 = |z|^2$ et donc $\Im^A z \geq \Im z$. En fait, à l'étape (2) $\Im z_{i+1} = \Im z_i$ et à l'étape (4) $\Im z_{i+1} = \frac{\Im z_i}{|z_i|^2} > \Im z_i$.
Nous obtenons donc une suite croissante bornée par 1 qui est

$$\Im z_0 < \Im z_2 < \Im z_4 < \cdots < 1.$$

De plus nous observons que pour tout i, nous pouvons écrire $z_i = A_i z_0$ où $A_i = \begin{pmatrix} j_i & k_i \\ l_i & m_i \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Par le même argument que précédemment nous en déduisons que

$$\Im z_0 < \frac{\Im z_0}{|l_2 z_0 + m_2|^2} < \cdots < \frac{\Im z_0}{|l_i z_0 + m_i|^2} < \cdots < 1$$

ou de manière équivalente

$$1 > |l_2 z_0 + m_2| > \cdots > |l_i z_0 + m_i| > \cdots > \sqrt{\Im z_0}.$$

Nous avons donc trouvé une infinité de points du réseau $\mathbb{Z}z_0 + \mathbb{Z}$ dans l'anneau $\sqrt{\Im z_0} < |z| < 1$. Or, ce réseau est un ensemble discret de points donc le disque $|z| < 1$ ne peut pas en contenir une infinité. Cette contradiction montre que nous devons bien avoir la condition (3) satisfaite à un moment donné, ce qui signifie que nous sortons bien de la boucle et que l'algorithme se termine. Donc chaque point dans $\mathbb{H}$ est bien $\mathrm{SL}_2(\mathbb{Z})$-équivalent à un point dans $\mathcal{F}$.

Enfin, terminons cette preuve en observant que pour tout $A \in \mathrm{SL}_2(\mathbb{Z})$, si z et ${}^A z$ sont tous deux dans $\mathcal{F}$ alors $z = {}^A z$.
Une première chose à remarquer est que par définition ${}^A z = {}^{-A} z$ et donc nous pouvons supposer sans perte de généralité que $l > 0$ ou $l = 0$ et $m > 0$. Pour plus de facilité nous supposons également que $\Im^A z \geq \Im z$ (nous pouvons échanger z et ${}^A z$ si nécessaire).
Dans ce cas, puisque $\Im^A z = \frac{\Im z}{|lz+m|^2}$ cela implique que nous devons avoir $lz + m \in C = \{z \in \mathbb{H} \mid |z| \leq 1\}$, ce qui revient à dire que $lz \in l\mathcal{F} \cap (C + \mathbb{Z})$.

Cela n'étant possible que pour $|l| < 2$ et au vu des suppositions faites ci-dessus il ne nous reste que les cas suivants à analyser

— $l = 0$: Nous nous retrouvons donc avec la condition $m \in C$ qui est équivalente à $|m| \leq 1$, donc pour que la matrice A soit dans $SL_2(\mathbb{Z})$ il faut que $m = 1$ et $A = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$. Nous avons alors que ${}^A z = z + k$. Si z et $z + k$ étaient deux éléments différents dans $\mathcal{F}$ il faudrait que $k = \pm 1$ puisque $\mathcal{F}$ est de largeur 1. Nous aurions alors un des deux éléments étant sur la ligne $\Re z = -\frac{1}{2}$ et l'autre sur la ligne $\Re z = \frac{1}{2}$. Mais $\Re z = \frac{1}{2}$ n'est pas dans $\mathcal{F}$, donc il faut que $k = 0$ ce qui implique que ${}^A z = z$.

— $l = 1$: Cette fois la condition est $z + m \in C$. Les seules possibilités sont $z = \xi = e^{\frac{2i\pi}{3}}$ et $m = 1$. La matrice A est donc $\begin{pmatrix} j & j-1 \\ 1 & 1 \end{pmatrix}$ ce qui implique que ${}^A z = \frac{j\xi + j - 1}{\xi + 1} = j + \xi$. Pour que ${}^A z \in \mathcal{F}$ il faut donc que $j = 0$. Mais alors ${}^A z = z$.

Nous avons donc bien que dans tous les cas ${}^A z = z$ ce qui termine de prouver que $\mathcal{F}$ est un domaine fondamental pour l'action de $SL_2(\mathbb{Z})$ sur $\mathbb{H}$. □

Ce résultat sur le demi-plan complexe supérieur nous donne directement l'information qui nous intéressait via le corollaire suivant.

COROLLAIRE 3.29. *Un domaine fondamental pour l'action de* $SL_2(\mathbb{Z})$ *sur* $\mathcal{H}_D$ *consiste en les nombres quadratiques de discriminant D dans* $\mathcal{F}$*, c'est-à-dire en les éléments de* $\mathcal{F}$ *compris dans* $\mathcal{H}_D$*.*
Nous noterons ce domaine fondamental $\mathcal{F}_{\mathcal{H}_D}$*.*

Le fait que nous ayons un domaine fondamental de $\mathcal{H}_D$ pour l'action de $SL_2(\mathbb{Z})$ nous assure qu'il n'y a dans $\mathcal{F}_{\mathcal{H}_D}$ qu'un unique représentant de chaque orbite $SL_2(\mathbb{Z})\eta$. Ce que nous allons voir ci-dessous est que ce représentant correspond au paramètre associé à la forme quadratique réduite de la forme quadratique associée à η. C'est-à-dire que pour tout $\eta \in \mathcal{H}_D$, le représentant de $SL_2(\mathbb{Z})\eta$ dans $\mathcal{F}_{\mathcal{H}_D}$ est $\eta_{q'}$ où $q' \in \mathcal{Q}_D$ est la forme quadratique réduite associée à q_η.
L'idée clef est d'observer l'algorithme de réduction pour $\mathbb{H}$ présenté ci-dessus en comparaison à celui pour les formes quadratiques définies de la démonstration 3. Nous remarquons alors que si l'étape (n) de celui sur les formes quadratiques modifie q en q' alors l'étape (n) dans l'algorithme sur

les paramètres envoie η_q sur $\eta_{q'}$. De manière plus formelle nous avons la proposition suivante.

PROPOSITION 3.30. *Une forme quadratique primitive définie positive* $q\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = aX^2 + bXY + cY^2 \in \mathcal{Q}_D$ *est réduite si et seulement si* $\eta_q \in \mathcal{F}$.

DÉMONSTRATION. Nous avons par définition que

$$\eta_q = \frac{-b + \sqrt{D}}{2a} = \frac{-b + i\sqrt{-D}}{2a} \in \mathbb{H}$$

avec comme partie réelle $\Re\eta_q = -\frac{b}{2a}$ ainsi que $|\eta_q|^2 = \frac{c}{a}$.
Nous allons voir qu'à partir de cela et des conditions d'appartenance à $\mathcal{F}$ nous retombons sur les conditions pour être une forme quadratique primitive définie positive données dans la définition 3.12.
Les conditions $|\Re z| \leq \frac{1}{2}$ et $|z| \geq 1$ qui définissent la fermeture de $\overline{\mathcal{F}}$, se traduisent pour η_q en $\left| -\frac{b}{2a} \right| \leq \frac{1}{2}$ et $\frac{c}{a} \geq 1$. Nous pouvons alors multiplier par $a > 0$ et obtenir $|b| \leq a$ et $c \geq a$ qui combinées nous donnent la première condition pour que la forme quadratique soit réduite.
Quand à la condition au bord, $a = |b|$ ou $a = c$, elle se produit lorsque η_q est sur la frontière de $\overline{\mathcal{F}}$. En effet, $a = |b|$ si et seulement si $\Re\eta_q = \pm\frac{1}{2}$ et $a = c$ si et seulement si $|\eta_q| = 1$. Le choix de $b > 0$ dans la définition de forme quadratique réduite signifie simplement que nous choisissons la forme quadratique q telle que son paramètre associé η_q ait une partie réelle strictement négative $\Re\eta_q < 0$ ce qui est nécessaire pour être dans $\mathcal{F}$. □

De cette dernière proposition et du fait que $\mathcal{F}$ est un domaine fondamental pour l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{H}_D$ nous déduisons le corollaire ci-dessous.

COROLLAIRE 3.31 (Unicité de la forme réduite équivalente à une forme donnée). *Pour chaque forme quadratique* $q \in \mathcal{Q}_D$*, la forme quadratique réduite équivalente associée est unique.*

Ce corollaire aura des conséquences importantes lorsque nous allons nous intéresser plus en particulier aux formes quadratiques associées aux idéaux.

Puisque nous avons ici étudié l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{H}_D$ et que nous avons trouvé un domaine fondamental $\mathcal{F}_{\mathcal{H}_D}$, il peut être naturel de vouloir étudier l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{Q}_D$ et c'est ce que nous allons faire.

Pour trouver un domaine fondamental pour l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{Q}_D$, puisque nous savons que $\mathcal{Q}_D$ et $\mathcal{H}_D$ sont en bijection et au vu de la proposition 3.30, il nous faut lister les formes quadratiques primitives définies

positives réduites dans $\mathcal{Q}_D$. C'est la proposition suivante qui montre comment le faire.

PROPOSITION 3.32. *Soit $D < 0$. Une liste complète des formes quadratiques $q\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = aX^2 + bXY + cY^2 \in \mathcal{Q}_D$ réduites de discriminant D est déterminée par les conditions suivantes sur les coefficients a, b, c :*

- $|b| \leq \sqrt{\frac{|D|}{3}}, \qquad b \equiv D \pmod 2$,
- $a_{\min} = |b| \leq a \leq \sqrt{\frac{b^2-D}{4}} = a_{\max}$,
- $c = \frac{b^2-D}{4a} \in \mathbb{Z}$,
- $b \geq 0$ *quand* $a = |b|$ *ou* $a = c$,
- a, b, c *sont premiers entre eux.*

DÉMONSTRATION. En ce qui concerne la première implication, supposons que $q \in \mathcal{Q}_D$ est réduite. Par définition nous avons donc les inégalités $|b| \leq a \leq c$. Cela entraine que $-D = 4ac - b^2 \geq 4|b|^2 - |b| = 3|b|^2$, ce qui est équivalent à $|b| \leq \sqrt{\frac{|D|}{3}}$. De plus, par définition du discriminant $b \equiv b^2 \equiv D \pmod 2$. Toujours à partir de $|b| \leq a \leq c$ nous pouvons déduire que $a^2 \leq ac = \frac{b^2-D}{4}$ ce qui nous permet d'obtenir la deuxième condition désirée. Quant à la troisième condition elle nous limite simplement aux a pour lesquels c est également dans les entiers. La quatrième condition est directement donnée par l'hypothèse que q est réduite. Enfin la dernière condition découle du fait que $q \in \mathcal{Q}_D$.
Réciproquement, prenons q satisfaisant les conditions de la propriété. Dans ce cas nous avons la condition limite de la définition de forme quadratique réduite. Il reste simplement à vérifier que nous ayons bien $|b| \leq a \leq c$. Comme $|b| \leq a$ est donnée par la deuxième condition, il faut uniquement montrer que $a \leq c$. Nous obtenons cela facilement en combinant $a \leq \sqrt{\frac{b^2-D}{4}}$ et $c = \frac{b^2-D}{4a} \in \mathbb{Z}$. Nous avons donc une forme quadratique réduite de discriminant D. De plus elle est primitive par la dernière condition sur les coefficients, ce qui conclut. □

Cette propriété sera très intéressante une fois le lien entre formes quadratiques et idéaux établi. Elle permettra en effet de calculer assez facilement le nombre de classes du corps quadratique imaginaire considéré. Une observation importante pouvant alors en être tirée est que cela montre la finitude du nombre de classes d'un corps quadratique imaginaire. Ce résultat central qui, au chapitre précédent découlait avec pas mal de travail

du théorème de Minkowski peut cette fois être obtenu à partir des arguments de ce chapitre de manière plus simple.

5. Correspondance entre formes quadratiques et idéaux fractionnaires d'un corps quadratique imaginaire

Nous allons dans cette section développer plus en détails la correspondance annoncée qui est très utile pour le calcul du groupe de classes d'idéaux d'un corps quadratique imaginaire.

REMARQUE 3.33. Rappelons que la formulation des résultats présentés dans cette section sera celle concernant les corps quadratiques imaginaires, pour les corps quadratiques réels des adaptations seraient nécessaires.

Avant toute chose, définissons ce qu'est l'application quadratique associée à un idéal et la forme quadratique associée à cette application pour une base donnée.

Pour cela nous avons besoin de savoir ce qu'est la norme d'un idéal fractionnaire. Nous avions vu à la définition 2.16 comment définir la norme d'un idéal fractionnaire se trouvant dans $\mathcal{O}$. Nous allons utiliser cette définition pour définir la norme d'un idéal fractionnaire en général.
Ce qu'il faut remarquer est simplement que si nous avons un idéal fractionnaire $\mathcal{I} \not\subset \mathcal{O}$, il est possible de trouver un entier rationnel $d \neq 0$ tel que $d\mathcal{I} \subset \mathcal{O}$ et donc $d\mathcal{I}$ est un idéal de $\mathcal{O}$. Un tel d peut être un dénominateur commun aux générateurs de $\mathcal{I}$. Le fait que $d\mathcal{I}$ soit dans $\mathcal{O}$ nous permet d'avoir $\mathrm{N}(dJ)$ défini comme dans 2.16 et nous en tirons la définition suivante.

DÉFINITION 3.34. *Soit $\mathcal{I}$ un idéal fractionnaire d'un corps quadratique imaginaire et soit d un entier non nul tel que $d\mathcal{I}$ soit un idéal de $\mathcal{O}$. La* norme d'un idéal fractionnaire *est alors définie de la manière suivante*

$$\mathrm{N}(\mathcal{I}) = \frac{\mathrm{N}(d\mathcal{I})}{d^2}.$$

Cette définition étant indépendante du choix de d.

DÉFINITION 3.35. *Soit $\mathcal{I} \subset F$ un idéal fractionnaire d'un corps quadratique imaginaire, nous pouvons considérer le module quadratique $(\mathcal{I}, \varphi_{\mathcal{I}})$ où l'application quadratique est donnée par*

$$\varphi_{\mathcal{I}} : \mathcal{I} \to \mathbb{Z}, \quad \varphi_{\mathcal{I}}(\lambda) = \frac{\mathrm{N}(\lambda)}{\mathrm{N}(\mathcal{I})} \quad \textit{pour } \lambda \in \mathcal{I}.$$

REMARQUE 3.36. Dans la définition précédente la norme est celle d'un corps quadratique imaginaire $F \subset \mathbb{C}$ qui est donc identique à celle bien connue de $\mathbb{C}$.

Remarquons que le quotient $\varphi_{\mathcal{I}}(\lambda) = \frac{\mathrm{N}(\lambda)}{\mathrm{N}(\mathcal{I})}$ est bel et bien dans $\mathbb{Z}$ puisque pour un idéal non nul dans $\mathcal{O}$, l'entier positif $\mathrm{N}(\mathcal{I})$ divise la norme de tout élément dans l'idéal comme nous l'indique la remarque 2.17. En fait, $\mathrm{N}(\mathcal{I})$ est même le plus grand commun diviseur des entiers $\mathrm{N}(\lambda)$ pour tout $\lambda \in \mathcal{I}$. Cela nous dit donc également que l'application quadratique est primitive.
Et pour les idéaux fractionnaires ne se trouvant pas dans $\mathcal{O}$, il suffit simplement de les multiplier pour un entier non nul d comme expliqué ci-dessus. Si nous avons $\mathcal{J} \not\subset \mathcal{O}$ et $\lambda \in \mathcal{J}$, $\frac{\mathrm{N}(\lambda)}{\mathrm{N}(\mathcal{J})} = \mathrm{N}(\lambda)\frac{d^2}{\mathrm{N}(d\mathcal{J})} = \frac{\mathrm{N}(d\lambda)}{\mathrm{N}(d\mathcal{J})}$ avec $d\lambda \in d\mathcal{J}$ et $\mathrm{N}(d\mathcal{J})$ qui divise $\mathrm{N}(\lambda)$.
Nous observons par la même occasion que $\varphi_{\mathcal{J}}(\lambda) = \varphi_{d\mathcal{J}}(d\lambda)$, donc la forme $\varphi_{\mathcal{I}}$ ne change pas sous l'action de $F^\times$ par homothétie sur les idéaux fractionnaires.

Soit maintenant une $\mathbb{Z}$-base $e = (\alpha, \beta)$ de $\mathcal{I}$, c'est aussi une $\mathbb{Q}$-base de F. Nous pouvons considérer la forme quadratique associée à $\varphi_{\mathcal{I}}$ de la manière suivante.

DÉFINITION 3.37. *Soient $\varphi_{\mathcal{I}}$ telle que définie ci-dessus et e une base de $\mathcal{I}$. La forme quadratique $\varphi_{\mathcal{I},e}$ associée à $\varphi_{\mathcal{I}}$ par rapport à la base e est*

$$\varphi_{\mathcal{I},e}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = \varphi_{\mathcal{I}}(\alpha X + \beta Y) \qquad \text{si } e = (\alpha, \beta).$$

Une autre notion liée à la base d'un idéal fractionnaire est celle d'*orientation*.

DÉFINITION 3.38. *Étant donné que toute $\mathbb{Z}$-base $e = (\alpha, \beta)$ de $\mathcal{I}$ est aussi une $\mathbb{Q}$-base de F, $\frac{\beta}{\alpha} \in \mathbb{C} \setminus \mathbb{R}$. On dit alors que la base est* orientée positivement *si $\Im(-\frac{\beta}{\alpha}) > 0$, c'est-à-dire si $-\frac{\beta}{\alpha} \in \mathbb{H}$.*

REMARQUE 3.39. Nous observons que puisque $\frac{\alpha}{\beta} = \mathrm{N}(\frac{\alpha}{\beta})(\overline{\frac{\beta}{\alpha}})$ alors $\Im(-\frac{\alpha}{\beta}) = \Im(-\mathrm{N}(\frac{\alpha}{\beta})(\overline{\frac{\beta}{\alpha}}))$ si $\Im(-\frac{\beta}{\alpha}) < 0$. Cela implique que la base (β, α) est orientée positivement si (α, β) ne l'est pas.

Nous pouvons définir également les *idéaux fractionnaires orientés*.

DÉFINITION 3.40. *Un* idéal fractionnaire orienté *est un triplet $(\mathcal{I}, \alpha, \beta)$ où $\mathcal{I}$ est un idéal fractionnaire de F avec une base orientée positivement (α, β).*
L'ensemble de tous les idéaux fractionnaires orientés de F est noté

$$\mathcal{I}_F = \{(\mathcal{I}, e) \mid \mathcal{I} \in \mathbb{I}_F,\ e \text{ base de } \mathcal{I} \text{ orientée positivement}\}.$$

Annonçons déjà le résultat central de ce chapitre qui est le théorème ci-dessous.
La notation que nous allons utiliser, étant donné un corps quadratique imaginaire F de discriminant D_F tel que défini en 2.26, est $\mathcal{Q}_F$ pour $\mathcal{Q}_{D_F}$ et $\mathcal{H}_F$ pour $\mathcal{H}_{D_F}$.

THÉORÈME 3.41. *Il existe des bijections*

$$\mathrm{Cl}(F) \cong \mathcal{Q}_F / \mathrm{SL}_2(\mathbb{Z}) \cong \mathcal{H}_F / \mathrm{SL}_2(\mathbb{Z}).$$

Ce théorème est assez puissant car il permet d'étudier un seul et même objet sous trois points de vue différents. En effet, il met en bijection le groupe de classes d'idéaux d'un corps quadratique imaginaire avec les classes d'équivalence propre des formes quadratiques dans $\mathcal{Q}_F$ sous l'action de $\mathrm{SL}_2(\mathbb{Z})$ et avec l'ensemble des orbites des paramètres associés à ces formes quadratiques sous l'action de $\mathrm{SL}_2(\mathbb{Z})$.
Ce théorème nous dit donc que pour trouver le nombre d'objets dans le groupe de classes d'idéaux il suffit de trouver le nombre d'orbites $\varphi_{\mathcal{I},e}^{\mathrm{SL}_2(\mathbb{Z})}$ pour $\varphi_{\mathcal{I},e} \in \mathcal{Q}_F$. Au vu de ce qui a été fait dans la section précédente, cela revient à trouver les formes quadratiques dans le domaine fondamental $\mathcal{F}_{\mathcal{Q}_F}$ de $\mathcal{Q}_F$ pour l'action de $\mathrm{SL}_2(\mathbb{Z})$. Nous avons vu que ces formes quadratiques sont en fait exactement les formes quadratiques réduites dans $\mathcal{Q}_F$ et nous savons également que nous pouvons facilement les lister grâce à la proposition 3.32.
La seconde bijection représentant simplement le fait que, $\mathcal{Q}_F$ étant en bijection avec $\mathcal{H}_F$, nous pouvons de manière équivalente regarder quels sont les paramètres associés aux formes quadratiques réduites qui sont dans le domaine fondamental $\mathcal{F}_{\mathcal{H}_F}$.
C'est la première bijection que nous allons mettre en application dans la section 2 du chapitre suivant pour voir une méthode de calcul de l'ordre de $\mathrm{Cl}(F)$ plus rapide.

Au vu des définitions du début de cette section, il y a une application surjective évidente $\phi : \mathcal{I}_F \to \mathbb{I}_F, \phi((\mathcal{I}, \alpha, \beta)) = \mathcal{I}$ qui consiste simplement à oublier la base.
De plus, $\mathrm{SL}_2(\mathbb{Z})$ agit sur les bases, nous en déduisons que $\mathrm{SL}_2(\mathbb{Z})$ agit sur $\mathcal{I}_F$ de la manière suivante.

PROPOSITION 3.42. *Soient $A \in \mathrm{SL}_2(\mathbb{Z})$ et $(\mathcal{I}, e) \in \mathcal{I}_F$. Une action du groupe $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{I}_F$ est définie en posant*

$$(\mathcal{I}, e)^A = (\mathcal{I}, eA).$$

Nous obtenons de cette action de groupe une bijection induite, c'est le lemme ci-dessous.

LEMME 3.43. *L'application ϕ induit une bijection $\tilde{\varphi} : \mathcal{I}_F / \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{I}_F$.*

DÉMONSTRATION. Soient e et e' deux bases d'un même idéal fractionnaire, alors il existe $A \in \mathrm{GL}_2(\mathbb{Z})$ telle que $e' = eA$. Pour prouver le lemme, il suffit de voir que si e est orientée positivement, alors $\det(A) = 1$ si et seulement si e' est orientée positivement.
Pour montrer cette équivalence il suffit de combiner le fait que si la base $e = (\alpha, \beta)$ est orientée positivement alors $\Im(-\frac{\beta}{\alpha}) > 0$, c'est-à-dire $-\frac{\beta}{\alpha} \in \mathbb{H}$ avec la remarque 3.26. □

Il est également possible de définir une autre action sur $\mathcal{I}_F$. En effet, $F^\times$ agit sur $\mathbb{I}_F$ et $\mathcal{I}_F$ par homothétie [1].
Soit $\gamma \in F^\times$ et $(\mathcal{I}, e) \in \mathcal{I}_F$ avec $e = (\alpha, \beta)$, alors $\gamma\mathcal{I} \in \mathbb{I}_F$ et $\gamma e = (\gamma\alpha, \gamma\beta)$ est une base orientée positivement de $\gamma\mathcal{I}$ puisque $-\frac{\gamma\beta}{\gamma\alpha} = -\frac{\beta}{\alpha}$.
Nous avons $N(\gamma\mathcal{I}) = N(\gamma)N(\mathcal{I})$, donc

$$\varphi_{\gamma\mathcal{I},\gamma e}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = \frac{N(\gamma\alpha X + \gamma\beta Y)}{N(\gamma)N(\mathcal{I})} = \frac{N(\alpha X + \beta Y)}{N(\mathcal{I})} = \varphi_{\mathcal{I},e}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right).$$

Dès lors, nous pouvons écrire le quotient $\mathcal{I}_F / F^\times$ et l'application $\varphi \colon \mathcal{I}_F \to \mathcal{Q}$ qui envoie $(\mathcal{I}, e)$ sur $\varphi_{\mathcal{I},e}$ est constante sur les classes d'homothétie et induit une application $\overline{\varphi} \colon \mathcal{I}_F / F^\times \to \mathcal{Q}$.

Nous avons donc deux groupes, $\mathrm{SL}_2(\mathbb{Z})$ et $F^\times$ qui agissent sur un même ensemble $\mathcal{I}_F$. Nous pouvons observer que les deux actions commutent.
En effet, soient $\gamma \in F^\times$ et $A \in \mathrm{SL}_2(\mathbb{Z})$, par définition nous avons que

$$\begin{aligned} \gamma((\mathcal{I}, e)^A) &= \gamma(\mathcal{I}, eA) \\ &= (\gamma\mathcal{I}, \gamma(\alpha a_{11} + \beta a_{21}), \gamma(\alpha a_{12} + \beta a_{22})) \\ &= (\gamma\mathcal{I}, \gamma\alpha a_{11} + \gamma\beta a_{21}, \gamma\alpha a_{12} + \gamma\beta a_{22}) \\ &= (\gamma\mathcal{I}, (\gamma e)A) \\ &= (\gamma(\mathcal{I}, e))^A. \end{aligned}$$

Cela implique l'existence de la bijection

$$(\mathcal{I}_F / \mathrm{SL}_2(\mathbb{Z}))/F^\times \cong (\mathcal{I}_F / F^\times)/\mathrm{SL}_2(\mathbb{Z}). \tag{3.1}$$

Une autre chose remarquable est que la bijection $\phi : \mathcal{I}_F \to \mathbb{I}_F$ d'oubli de la base est $F^\times$-équivariante. En effet, soient $(\mathcal{I}, e) \in \mathcal{I}_F$ et $\gamma \in F^\times$, nous

1. Cela peut être mis en lien avec le développement suivant la définition 3.35 et sa remarque.

avons que

$$\begin{aligned}\phi(\gamma(\mathcal{I},e)) &= \phi((\gamma\mathcal{I},\gamma e))\\ &= \gamma\mathcal{I}\\ &= \gamma(\phi((\mathcal{I},e))).\end{aligned}$$

Nous pouvons alors passer au quotient et avoir la bijection $\mathcal{I}_F/F^\times \cong \mathbb{I}_F/F^\times$.

En combinant ce résultat avec la bijection 3.1 nous obtenons que

$$(\mathcal{I}_F/\operatorname{SL}_2(\mathbb{Z}))/F^\times \cong \mathbb{I}_F/F^\times.$$

Rappelons que $\mathrm{Cl}(F)$ est le quotient $\mathbb{I}_F/F^\times$. Nous en déduisons que

$$(\mathcal{I}_F/\operatorname{SL}_2(\mathbb{Z}))/F^\times \cong \mathrm{Cl}(F) \text{ et donc } \mathrm{Cl}(F) \cong (\mathcal{I}_F/F^\times)/\operatorname{SL}_2(\mathbb{Z}). \tag{3.2}$$

De ce que nous avons vu jusqu'à présent nous pouvons déduire la proposition ci-dessous qui met en bijection les classes d'idéaux orientés sous l'action de $F^\times$ avec les formes quadratiques de $\mathcal{Q}_F$ et les paramètres qui leur sont associés.

PROPOSITION 3.44. *Soit $(\mathcal{I},e) \in \mathcal{I}_F$ alors $\varphi_{\mathcal{I},e} \in \mathcal{Q}_F$ et le paramètre de la forme $\varphi_{\mathcal{I},e}$ est $-\frac{\beta}{\alpha}$ si $e=(\alpha,\beta)$.*
De plus, l'application $\varphi\colon \mathcal{I}_F \to \mathcal{Q}_F$ qui envoie $(\mathcal{I},e)$ sur $\varphi_{\mathcal{I},e}$ est $\operatorname{SL}_2(\mathbb{Z})$-équivariante.

DÉMONSTRATION. Commençons par vérifier que nous avons bien que $\eta_{\varphi_{\mathcal{I},e}} = -\frac{\beta}{\alpha}$. Comme par hypothèse $(\mathcal{I},e) \in \mathcal{I}_F$, la base $e=(\alpha,\beta)$ est orientée positivement et nous en déduisons que $\Im(-\frac{\beta}{\alpha}) > 0$. De plus, sur base de la définition 3.37 nous calculons que $\varphi_{\mathcal{I},e}\left(\begin{smallmatrix}-\beta/\alpha\\1\end{smallmatrix}\right) = 0$. Donc $-\frac{\beta}{\alpha}$ est bien le paramètre de la forme $\varphi_{\mathcal{I},e}$.

De plus, $-\frac{\beta}{\alpha} \in F \setminus \mathbb{Q}$ donc le discriminant de la forme $\varphi_{I,e}$ est D_F et nous avons bien $\varphi_{\mathcal{I},e} \in \mathcal{Q}_F$.

Vérifions enfin que φ est équivariante sous l'action de $\operatorname{SL}_2(\mathbb{Z})$. Cela découle de la définition de l'action de $\operatorname{SL}_2(\mathbb{Z})$ sur $\mathcal{Q}_F$ puisque nous avons $\varphi^A_{\mathcal{I},e} = \varphi_{\mathcal{I},eA}$ pour $A \in \operatorname{SL}_2(\mathbb{Z})$. Donc nous obtenons les égalités suivantes

$$\begin{aligned}\varphi((\mathcal{I},e)^A) &= \varphi(\mathcal{I},eA)\\ &= \varphi_{\mathcal{I},eA}\\ &= \varphi^A_{\mathcal{I},e}\end{aligned}$$

et l'application φ est $\operatorname{SL}_2(\mathbb{Z})$-équivariante. □

Cette proposition montre que $\overline{\varphi}$ est une application $\mathcal{I}_F/F^\times \to \mathcal{Q}_F$. En fait, il se fait même que c'est une bijection comme nous allons le voir. Pour définir l'inverse de cette application nous énonçons d'abord la proposition suivante.

PROPOSITION 3.45. *Soient $q \in \mathcal{Q}_F$ et $\eta_q \in \mathcal{H}_F$ son paramètre. Le $\mathbb{Z}$-module $\mathcal{I}_q = \mathbb{Z} + \mathbb{Z}\eta_q$ est un idéal fractionnaire de F et $e_q = (-1, \eta_q)$ est une base orientée positivement de $\mathcal{I}_q$. De plus, $\varphi_{\mathcal{I}_q, e_q} = q$.*

DÉMONSTRATION. Par définition, si $q\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = aX^2 + bXY + cY^2 \in \mathcal{Q}_F$, son paramètre s'écrit $\eta_q = \frac{-b+\sqrt{D_F}}{2a}$ où $D_F = b^2 - 4ac$. Pour voir que $\mathcal{I}_q$ est un idéal fractionnaire, il suffit de vérifier que $\delta\mathcal{I}_q \subset \mathcal{I}_q$ pour $\delta = \frac{1+\sqrt{D_F}}{2}$ si $D_F \equiv 1 \pmod 4$ et $\delta = \frac{\sqrt{D_F}}{2}$ si $D_F \equiv 0 \pmod 4$. Étant donné que $\mathcal{I}_q$ est engendré par 1 et η_q, il suit que $\delta\mathcal{I}_q$ est engendré par δ et $\delta\eta_q$, donc prouver que $\delta\mathcal{I}_q \subset \mathcal{I}_q$ revient à prouver $\delta \in \mathcal{I}_q$ et $\delta\eta_q \in \mathcal{I}_q$.

Supposons d'abord $D_F \equiv 1 \bmod 4$, ce qui entraîne $b \equiv 1 \pmod 2$. Soit $b = -1 + 2b_0$ avec $b_0 \in \mathbb{Z}$. Alors nous calculons

$$\delta = \frac{1+\sqrt{D_F}}{2} = b_0 + \frac{-b+\sqrt{D_F}}{2} = b_0 + a\eta_q \in \mathcal{I}_q$$

et

$$\delta\eta_q = (b_0 + a\eta_q)\eta_q = b_0\eta_q - b\eta_q - c = -c + (b_0 - b)\eta_q \in \mathcal{I}_q.$$

Supposons ensuite $D_F \equiv 0 \bmod 4$, donc $b \equiv 0 \pmod 2$. Soit cette fois-ci $b = 2b_0$ avec $b_0 \in \mathbb{Z}$. Alors $\delta = \sqrt{b_0^2 - ac}$ et $\eta_q = \frac{-b_0+\delta}{a}$. Cela entraine que

$$\delta = b_0 + a\eta_q \in \mathcal{I}_q \quad \text{et} \quad \delta\eta_q = b_0\eta_q - b\eta_q - c = -c + (b_0 - b)\eta_q \in \mathcal{I}_q.$$

Nous voyons ainsi que $\mathcal{I}_q$ est un idéal fractionnaire de F comme annoncé.

Étant donné que $\Im(\eta_q) > 0$, la base $e_q = (-1, \eta_q)$ de $\mathcal{I}_q$ est orientée positivement.

Enfin, il reste à vérifier que $\varphi_{\mathcal{I}_q, e_q} = q$. La définition 3.37 nous donne $\varphi_{\mathcal{I}_q, e_q}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = \varphi_{\mathcal{I}_q}(-X + \eta_q Y) = \frac{\mathrm{N}(-X+\eta_q Y)}{\mathrm{N}(\mathcal{I}_q)}$. Nous calculons ensuite que

$$\begin{aligned} \mathrm{N}(-X + \eta_q Y) &= \left((-X - \tfrac{b}{2a}Y) + \tfrac{Y}{2a}\sqrt{D_F}\right)\left((-X - \tfrac{b}{2a}Y) - \tfrac{Y}{2a}\sqrt{D_F}\right) \\ &= X^2 + \tfrac{b}{a}XY + \tfrac{c}{a}Y^2 \end{aligned}$$

Intéressons nous maintenant au dénominateur. Nous savons par le commentaire sous la remarque 3.36 que pour $\mathcal{I}$ un idéal entier $\mathrm{N}(\mathcal{I})$ est le plus grand commun diviseur des $\mathrm{N}(\lambda)$ pour λ dans $\mathcal{I}$ donc c'est en fait le contenu de l'application quadratique N. Dans notre cas, l'idéal $\mathcal{I}_q$ est fractionnaire, mais nous savons par une discussion réalisée au début de cette section, que $a\mathcal{I}_q$ est entier, et la norme sur $a\mathcal{I}_q$ est $a^2X^2 + abXY + acY^2$. Comme q est primitive par hypothèse, a, b, c sont premiers entre eux et le contenu de la norme sur $a\mathcal{I}_q$ est a, par conséquent $\mathrm{N}(\mathcal{I}_q) = \frac{1}{a}$. Nous en

déduisons que

$$\varphi_{\mathcal{I}_q,e_q}\left(\begin{smallmatrix}X\\Y\end{smallmatrix}\right) = \frac{X^2 + \frac{b}{a}XY + \frac{c}{a}Y^2}{\frac{1}{a}} = aX^2 + bXY + cY^2 = q\left(\begin{smallmatrix}X\\Y\end{smallmatrix}\right)$$

ce qui conclut la preuve. □

Nous sommes maintenant en mesure de prouver la bijection souhaitée.

PROPOSITION 3.46. *L'application $\overline{\varphi}\colon \mathcal{I}_F/F^\times \to \mathcal{Q}_F$ est une bijection dont l'inverse est l'application $\psi\colon \mathcal{Q}_F \to \mathcal{I}_F/F^\times$ définie par $\psi(q) = F^\times(\mathcal{I}_q, e_q)$.*

DÉMONSTRATION. Dans un sens, la proposition 3.45 montre que $\overline{\varphi}\circ\psi$ est l'identité sur $\mathcal{Q}_F$. En effet, soit $q \in \mathcal{Q}_F$,

$$\overline{\varphi}(\psi(q)) = \overline{\varphi}(F^\times(\mathcal{I}_q, e_q)) = \varphi_{\mathcal{I}_q,e_q} = q.$$

Dans l'autre sens maintenant, soit $(\mathcal{I}, e) \in \mathcal{I}_F$. Si $e = (\alpha, \beta)$, la proposition 3.44 montre que le paramètre de la forme $\varphi_{\mathcal{I},e}$ est $-\frac{\beta}{\alpha}$ et donc $\psi(\varphi_{\mathcal{I},e}) = F^\times(\mathcal{I}_{\varphi_{\mathcal{I},e}}, e_{\varphi_{\mathcal{I},e}}) = F^\times\left(\mathbb{Z} + \mathbb{Z}(-\frac{\beta}{\alpha}), (-1, -\frac{\beta}{\alpha})\right)$.
Or, $(-\alpha)\cdot\left(\mathbb{Z} + \mathbb{Z}(-\frac{\beta}{\alpha}), (-1, -\frac{\beta}{\alpha})\right) = \mathbb{Z}\alpha + \mathbb{Z}\beta, (\alpha, \beta)) = (\mathcal{I}, e)$. Cela montre que $\psi(\varphi_{\mathcal{I},e}) = F^\times(\mathcal{I}, e)$. □

La théorie développée ci-dessus et les proposition précédentes nous permettent de démontrer le théorème suivant qui est en fait une des deux bijections du théorème 3.41.

THÉORÈME 3.47. *L'application qui à tout idéal fractionnaire $\mathcal{I}$ de F associe la classe d'équivalence propre de la forme quadratique $\varphi_{\mathcal{I},e}$, où e est une base quelconque de $\mathcal{I}$ orientée positivement, induit une bijection*

$$\Phi\colon \mathrm{Cl}(F) \xrightarrow{\sim} \mathcal{Q}_F/\mathrm{SL}_2(\mathbb{Z}).$$

DÉMONSTRATION. D'après la proposition 3.46, $\overline{\varphi}$ est une bijection donc $\mathcal{I}_F/F^\times \cong \mathcal{Q}_F$. Or, l'équation 3.2 nous donne $\mathrm{Cl}(F) \cong (\mathcal{I}_F/F^\times)/\mathrm{SL}_2(\mathbb{Z})$. Nous en déduisons que $\mathrm{Cl}(F) \cong (\mathcal{I}_F/F^\times)/\mathrm{SL}_2(\mathbb{Z}) \cong (\mathcal{Q}_F)/\mathrm{SL}_2(\mathbb{Z})$ comme souhaité. □

Pour démontrer le théorème 3.41 il nous suffit simplement d'assembler des résultats déjà démontrés.

DÉMONSTRATION. QLa première bijection $\mathrm{Cl}(F) \cong \mathcal{Q}_F/\mathrm{SL}_2(\mathbb{Z})$ c'est tout simplement le théorème 3.47.
Quant à la deuxième bijection, elle est rapide à démontrer car nous n'avons plus qu'à assembler certains résultats obtenus. En effet, nous avons établi

que $\iota_{\mathcal{Q}_F\mathcal{H}_F}$ est une bijection qui de plus, par la proposition 3.27, est $\mathrm{SL}_2(\mathbb{Z})$-équivariante. Nous pouvons alors passer au quotient et cela induit une bijection $\mathcal{Q}_F/\mathrm{SL}_2(\mathbb{Z}) \cong \mathcal{H}_F/\mathrm{SL}_2(\mathbb{Z})$. □

Idéal et son conjugué correspondant à la même forme quadratique. La discussion ci-dessous va nous montrer que même si l'équivalence propre entre les formes quadratiques associées aux idéaux fractionnaires permet généralement de distinguer les idéaux fractionnaires orientés de leur conjugué, il arrive qu'un idéal et son conjugué correspondent à la même forme quadratique associée. [2]

De façon tout à fait naturelle, nous aimerions pouvoir associer à un idéal fractionnaire orienté $(\mathcal{I}, \alpha, \beta)$ son conjugué. Il est évident par la définition 3.38 et la remarque 3.39 que $(\bar{\alpha}, \bar{\beta})$ n'est pas orientée si (α, β) l'est, nous ne pouvons donc pas prendre $\overline{(\mathcal{I}, \alpha, \beta)} = (\bar{\mathcal{I}}, \bar{\alpha}, \bar{\beta})$. Par contre, toujours par la même remarque, nous observons que si $(\bar{\alpha}, \bar{\beta})$ n'est pas orientée, $(\bar{\beta}, \bar{\alpha})$ l'est. Nous pouvons donc prendre $\overline{(\mathcal{I}, \alpha, \beta)} = (\bar{\mathcal{I}}, \bar{\beta}, \bar{\alpha})$.

Au niveau des applications quadratiques nous calculons

$$\varphi_{\bar{\mathcal{I}}}(\overline{\lambda}) = \frac{\mathrm{N}(\overline{\lambda})}{\mathrm{N}(\bar{\mathcal{I}})} = \frac{\mathrm{N}(\overline{\lambda})}{\mathrm{N}(\mathcal{I})} = \varphi_{\mathcal{I}}(\overline{\lambda})$$

Par la définition 3.37, cela donne pour les formes quadratiques, si $e = (\alpha, \beta)$ et $e' = (\bar{\beta}, \bar{\alpha})$,

$$\varphi_{\bar{\mathcal{I}},e'}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = \frac{\mathrm{N}(\bar{\beta}X + \bar{\alpha}Y)}{\mathrm{N}(\bar{\mathcal{I}})} = \frac{\mathrm{N}(\beta X + \alpha Y)}{\mathrm{N}(\mathcal{I})} = \varphi_{\mathcal{I},e}\left(\begin{smallmatrix} Y \\ X \end{smallmatrix}\right). \tag{3.3}$$

Puisque les variables ont juste été échangées, nous en déduisons que

$$\varphi_{\bar{\mathcal{I}},e'}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = \varphi^{A}_{\mathcal{I},e}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) \text{ où } A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{SL}_2(\mathbb{Z}).$$

Cela nous montre que la forme quadratique associée à $(\mathcal{I}, e)$ et celle associée à son conjugué $(\bar{\mathcal{I}}, e')$ sont reliées par l'action d'une matrice ne se trouvant pas dans $\mathrm{SL}_2(\mathbb{Z})$ (même si ça peut parfois être le cas) et donc $\varphi^{\mathrm{SL}_2(\mathbb{Z})}_{\mathcal{I},e} \neq \varphi^{\mathrm{SL}_2(\mathbb{Z})}_{\bar{\mathcal{I}},e'}$ sauf dans certains cas particuliers. En effet, il arrive que la forme quadratique associée à $(\mathcal{I}, e)$ et celle associée à $(\bar{\mathcal{I}}, e')$ puissent être reliées par une matrice $A \in \mathrm{SL}_2(\mathbb{Z})$ et soient donc dans la même orbite.

2. Cela sera utile au chapitre suivant pour identifier les idéaux qui sont de 2-torsion.

Cela signifie simplement que la classe $[\mathcal{I}]$ est de 2-torsion dans $\mathrm{Cl}(F)$ [3].

Voyons ce que ça implique pour une classe d'être de 2-torsion au niveau des formes quadratiques réduites.
Nous remarquons que l'équation 3.3 nous indique que si

$$\varphi_{\mathcal{I},e}\left(\begin{smallmatrix} Y \\ X \end{smallmatrix}\right) = aX^2 + bXY + cY^2 \text{ alors } \varphi_{\bar{\mathcal{I}},e'}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = cX^2 + bXY + aY^2.$$

Notons $\Phi([\mathcal{I}])$ la classe d'équivalence propre de $aX^2 + bXY + cY^2$, alors $\Phi([\overline{\mathcal{I}}])$ est la classe d'équivalence propre de $cX^2 + bXY + aY^2$.

De ces observations nous obtenons le corollaire ci-dessous qui nous sera utile dans la section 2 du chapitre 4.

COROLLAIRE 3.48. *Soit $\mathcal{I} \in \mathbb{I}_F$ un idéal fractionnaire. Si $aX^2 + bXY + cY^2$ est la forme quadratique réduite qui représente la classe d'équivalence $\Phi([\mathcal{I}])$, alors $[\mathcal{I}] = [\overline{\mathcal{I}}]$ si et seulement si $b = 0$ ou $a = b$ ou $a = c$.*

DÉMONSTRATION. Puisque Φ est une bijection et comme $\Phi([\overline{\mathcal{I}}])$ est la classe d'équivalence propre de $cX^2 + bXY + aY^2$, il est clair que $[\mathcal{I}] = [\overline{\mathcal{I}}]$ si et seulement si

(3.4) $cX^2 + bXY + aY^2$ est proprement équivalente à $aX^2 + bXY + cY^2$.

Or nous savons également que $cX^2 + bXY + aY^2$ est proprement équivalente, sous l'action de S [4], à la forme $aX^2 - bXY + cY^2$. La condition 3.4 devient alors que $[\mathcal{I}] = [\overline{\mathcal{I}}]$ si et seulement si

(3.5) $aX^2 - bXY + cY^2$ est proprement équivalente à $aX^2 + bXY + cY^2$.

Nous distinguons alors plusieurs cas.

- Si $a \neq |b|$ et $a \neq c$, alors la forme $aX^2 - bXY + cY^2$ est réduite. De plus, elle est différente de $aX^2 + bXY + cY^2$ si $b \neq 0$, elles ne sont donc pas proprement équivalentes. Dans ce cas nous en déduisons que $[\mathcal{I}] = [\overline{\mathcal{I}}]$ si et seulement si $b = 0$.
- Si $a = |b|$, alors comme $aX^2 + bXY + cY^2$ est réduite il faut par définition que $b \geq 0$, donc $b = a$. Comme $aX^2 - aXY + cY^2$ est proprement équivalente sous l'action de T [4] à la forme $aX^2 + aXY + cY^2$,

3. En effet, nous savons que $\mathrm{Cl}(F) \cong \mathcal{Q}_F / \mathrm{SL}_2(\mathbb{Z})$. Si les formes quadratiques sont proprement équivalentes nous avons alors que dans $\mathrm{Cl}(F)$, $[\mathcal{I}] = [\bar{\mathcal{I}}]$. Or, nous savons que $[\mathcal{O}] = [\mathcal{I}][\bar{\mathcal{I}}]$. Cette égalité devient donc $[\mathcal{O}] = [\mathcal{I}]^2$ ce qui montre bien que $[\mathcal{I}]$ est de 2-torsion.

4. Définies sous la définition 3.12.

la condition 3.5 est vérifiée et nous avons que $[\mathcal{I}] = [\overline{\mathcal{I}}]$ dans ce cas.

— Si $a = c$, les formes $aX^2 + bXY + cY^2$ et $cX^2 + bXY + aY^2$ sont identiques, donc $[\mathcal{I}] = [\overline{\mathcal{I}}]$.

□

Puisque $\mathcal{I}\overline{\mathcal{I}} = \mathcal{O}\,\mathrm{N}(\mathcal{I})$, nous avons toujours que $[\mathcal{I}][\overline{\mathcal{I}}] = [\mathcal{O}]$, donc $[\mathcal{I}] = [\overline{\mathcal{I}}]$ si et seulement si $[\mathcal{I}]$ est de 2-torsion dans le groupe des classes d'idéaux, c'est pourquoi le corollaire nous donne une caractérisation des éléments de 2-torsion.

Chapitre 4

Calcul des groupes de classes d'idéaux

Dans ce dernier chapitre nous allons voir plus en détails les techniques permettant de calculer le groupe de classes d'idéaux.

1. Approche en lien avec la borne de Minkowski

Dans cette première section nous allons aborder une approche utilisant des outils que nous avons vus au chapitre 2 tels que la factorisation unique des idéaux, la borne de Minkowski, etc. Nous alternerons entre méthodes générales théoriques et exemples illustratifs.

La première chose à faire, lorsque nous nous retrouvons face à un corps quadratique imaginaire $F = \mathbb{Q}[\sqrt{D}]$ et que nous souhaitons calculer son groupe de classes d'idéaux $\mathrm{Cl}(\mathbb{Q}[\sqrt{D}])$ est d'identifier l'anneau d'entiers $\mathcal{O}$ correspondant. Pour cela, il suffit de regarder la valeur de D modulo 4 et d'en déduire δ, nous pouvons nous aider du tableau récapitulatif ci-dessous.

$D \pmod 4$	δ, où $\mathcal{O} = \mathbb{Z}[\delta]$	$D_F = \operatorname{disc} \mathcal{O}$
$2, 3$	$\sqrt{D}$	$4D$
1	$\frac{1+\sqrt{D}}{2}$	D

Une fois que nous connaissons l'anneau des entiers concerné, une étape très importante est de calculer la borne de Minkowski qui est, rappelons le, $\mathfrak{M}_F = \sqrt{|D_F|} \cdot \frac{2}{\pi}$ dans le cas des corps quadratiques imaginaires.

Ensuite, grâce à cette borne nous pouvons utiliser la proposition 2.28 qui nous permet de voir quels éléments au maximum sont dans $\mathrm{Cl}(F)$.

Une fois que nous avons des informations sur les éléments qui sont dans le groupe de classes d'idéaux, il est important de voir quels sont ses générateurs. Pour cela nous pouvons faire appel à la proposition 2.29 qui encore une fois utilise la borne de Minkowski.

Notons P_p pour désigner un idéal de $\mathcal{O}$ ayant pour norme le nombre premier p. Nous savons que l'ensemble des générateurs que nous venons d'obtenir est peut-être redondant et une première façon de possiblement le réduire est de voir, pour chaque P_p et $\bar{P}_p$, si nous avons $P_p = \bar{P}_p$ ou $P_p \neq \bar{P}_p$. C'est le théorème suivant qui permet de répondre à cette question.

THÉORÈME 4.1. *Soit $p \in \mathbb{N}$ un nombre premier.*

— *Si $\left(\frac{D_F}{p}\right) = -1$, $\mathcal{O}p$ est un idéal premier dans $\mathcal{O}$ (et p est inerte);*

— $\left(\frac{D_F}{p}\right) = 0$ *si et seulement si $P_p = \bar{P}_p$ (et p est ramifié);*

— $\left(\frac{D_F}{p}\right) = 1$ *si et seulement si $P_p \neq \bar{P}_p$ (et p est décomposé).*

Remarquons que puisque D_F est le discriminant du polynôme minimal de δ, ce théorème peut tout à fait être mis en lien avec la remarque 2.19.

REMARQUE 4.2. Lorsque $p \neq 2$, le symbole employé dans le théorème fait référence au symbole de Legendre bien connu. Mais lorsque $p = 2$, il fait alors référence au symbole de Kronecker pour lequel

$$\left(\frac{a}{2}\right) = \begin{cases} 0 \text{ si } 2|a \\ 1 \text{ si } a \equiv \pm 1 \pmod 8 \\ -1 \text{ si } a \equiv \pm 3 \pmod 8 \end{cases}$$

Une autre manière de supprimer des générateurs potentiellement redondants est de voir si les générateurs sont principaux ou non, c'est-à-dire si $[P_p] = [\mathcal{O}]$ ou non. Le lemme suivant est alors très intéressant.

LEMME 4.3. *Soit F un corps quadratique avec $\mathcal{O}$ comme anneau d'entiers. Soit P un idéal de $\mathcal{O}$ avec pour norme un nombre premier. Alors P est principal si et seulement si il existe un élément $\alpha \in \mathcal{O}$ tel que $\mathrm{N}(\alpha) = \pm \mathrm{N}(P)$.*

Concrètement, pour un corps quadratique imaginaire, cela signifie que P_p est principal si et seulement si il existe $\alpha \in \mathcal{O}$ tel que $\mathrm{N}(\alpha) = p$, c'est-à-dire si et seulement si il existe $x, y \in \mathbb{Z}$ tels que

$$\begin{cases} x^2 - Dy^2 = p \text{ si } D \equiv 2, 3 \pmod 4 \\ \left(x + \frac{y}{2}\right)^2 + \frac{-D}{4}y^2 = p \text{ si } D \equiv 1 \pmod 4 \end{cases}$$

Une fois que nous en sommes à ce stade, nous avons généralement une idée du nombre maximal d'éléments dans $\mathrm{Cl}(F)$ et nous avons une liste de générateurs que nous avons déjà partiellement réduite (elle pourrait peut-être l'être encore s'il existe des relations entre eux). Dans certains cas, les différentes étapes que nous avons effectuées nous permettent déjà d'y voir plus clair et d'avoir des bornes pour l'ordre du groupe de classes d'idéaux. Une autre manière d'obtenir des informations sur cet ordre est de calculer l'ordre de certains générateurs.

Pour cela, une première chose à remarquer que tous les idéaux P_p pour lesquels $P_p = \bar{P}_p$ sont tels que $[P_p]$ est de 2-torsion. En effet, puisque nous

avons l'égalité $[\mathcal{O}] = [P_p][\bar{P}_p]$, nous en déduisons que sous la condition $P_p = \bar{P}_p$, $[\mathcal{O}] = [P_p]^2$. Si de plus P_p n'est pas principal alors nous en déduisons que $[P_p]$ est d'ordre 2.
Une autre façon plus générale de trouver l'ordre d'un générateur d'utiliser la proposition suivante.

PROPOSITION 4.4. *Soit p un nombre premier rationnel qui se décompose dans un corps quadratique F et soit P_p un idéal de $\mathcal{O}$ qui divise $\mathcal{O}p$. Si $[P_p]^n = [\mathcal{O}]$ alors il existe $\alpha \in \mathcal{O} \setminus \mathbb{Z}$ tel que $\mathrm{N}(\alpha) = \pm p^n$.*

DÉMONSTRATION. L'hypothèse $[P_p]^n = [\mathcal{O}]$ indique que P_p^n est principal, il existe donc $\alpha \in \mathcal{O}$ tel que $P_p^n = \mathcal{O}\alpha$. Par hypothèse également nous avons que p est décomposé ce qui par définition nous donne $\mathcal{O}p = P_p\bar{P}_p$ avec $N(P_p) = p$. L'égalité $P_p^n = \mathcal{O}\alpha$ entraîne donc $N(\alpha) = \pm p^n$.

Voyons maintenant pourquoi $\alpha \in \mathcal{O} \setminus \mathbb{Z}$. Cela est en fait imposé par le fait que p est décomposé. En effet, si $\alpha \in \mathbb{Z}$ alors $N(\alpha) = \alpha^2$, donc $\alpha^2 = \pm p^n$ et par conséquent $\alpha = \pm p^{\frac{n}{2}}$. Mais alors

$$P_p^n = \mathcal{O}\alpha = \mathcal{O}p^{\frac{n}{2}} = P_p^{\frac{n}{2}}\bar{P}_p^{\frac{n}{2}}.$$

Par la factorisation unique des idéaux cela entraîne $P_p = \bar{P}_p$. C'est une contradiction avec l'hypothèse que p est décomposé dans F. Nous concluons donc que $\alpha \in \mathcal{O} \setminus \mathbb{Z}$. □

Il en découle le corollaire suivant.

COROLLAIRE 4.5. *Sous les même hypothèses, l'ordre de P_p est le plus petit entier $n > 0$ pour lequel il existe $\alpha \in \mathcal{O} \setminus \mathbb{Z}$ tel que $\mathrm{N}(\alpha) = \pm p^n$.*

Dans le cas des corps quadratiques imaginaires il nous faut donc voir s'il existe $\alpha \in \mathcal{O} \setminus \mathbb{Z}$ tel que $\mathrm{N}(\alpha) = p^n$ mais $\mathrm{N}(\beta) \neq p^r$ pour $r < n$ et tout $\beta \in \mathcal{O} \setminus \mathbb{Z}$, c'est-à-dire voir quelle est la première puissance n de p pour laquelle il existe $x, y \in \mathbb{Z}$ tels que

$$\begin{cases} x^2 - Dy^2 = p^n \text{ si } D \equiv 2,3 \pmod 4 \\ \left(x + \frac{y}{2}\right)^2 + \frac{-D}{4}y^2 = p^n \text{ si } D \equiv 1 \pmod 4 \end{cases}$$

En calculant l'ordre d'un certain $[P_p]$ il faut tout de même faire attention au fait que, si $P_p \neq \bar{P}_p$, le y dans l'expression ci-dessus doit être non nul comme justifié dans la démonstration de la proposition 4.4.

Lorsque nous avons effectué toutes ces étapes nous en savons parfois déjà assez pour pouvoir conclure. En effet, dans certains cas nous aurons une borne sur l'ordre de $\mathrm{Cl}(F)$ ainsi que son nombre de générateurs et

l'ordre d'au moins une partie de ceux-ci, nous en déduisons donc un isomorphisme entre le groupe de classes d'idéaux et un certain groupe abélien.
Nous verrons dans la suite qu'il y aura des cas pour lesquels ce ne sera pas suffisant. Il faudra alors effectuer des étapes supplémentaires.

Avant de passer à la suite illustrons avec un exemple les différentes étapes théoriques décrites ci-dessus et voyons comment cela s'applique concrètement.

EXEMPLE 4.6.
Nous allons calculer le groupe de classes d'idéaux de $F = \mathbb{Q}[\sqrt{-23}]$. Pour cela nous allons suivre les étapes mentionnées ci-dessus.

Nous commençons donc par identifier l'anneau d'entier $\mathcal{O}$ correspondant à $\mathbb{Q}[\sqrt{-23}]$. Puisque $D = -23$ et comme $-23 \equiv 1 \pmod 4$, nous avons que $\delta = \frac{1+\sqrt{D}}{2} = \frac{1+\sqrt{-23}}{2}$ et donc $\mathcal{O} = \mathbb{Z}[\delta] = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$.

Nous calculons ensuite la borne de Minkowski qui est

$$\mathfrak{M}_F = \sqrt{|D_F|} \cdot \frac{2}{\pi} = \sqrt{23} \cdot \frac{2}{\pi} \simeq 3.05.$$

Grâce à cette borne et à la proposition 2.28, nous savons que toute classe de $\mathrm{Cl}(F)$ contient un idéal de norme au plus $\mathfrak{M}_F \simeq 3.05$. Nous avons donc pour l'instant que $\mathrm{Cl}(F)$ contient au plus les éléments suivants $\mathrm{Cl}(\mathbb{Q}\sqrt{-23}) = \{[\mathcal{O}], [P_2], [\bar{P}_2], [P_3], [\bar{P}_3]\}$.

Nous savons ensuite, grâce à la proposition 2.29, qu'un ensemble de générateurs possiblement redondant pour $\mathrm{Cl}(F)$ est donné par tous les idéaux P ayant pour norme p premier tel que $p \leq \mathfrak{M}_F \simeq 3.05$. Les différents p possibles sont donc 2 et 3 et les générateurs correspondants sont $[P_2], [\bar{P}_2], [P_3]$ et $[\bar{P}_3]$.

Essayons de réduire une première fois cet ensemble de générateurs à l'aide du théorème 4.1. Nous calculons que

— $\left(\frac{D_F}{2}\right) = \left(\frac{-23}{2}\right) = 1$ donc $P_2 \neq \bar{P}_2$;

— $\left(\frac{D_F}{3}\right) = \left(\frac{-23}{3}\right) = 1$ donc $P_3 \neq \bar{P}_3$.

Cette fois ça n'a donc pas permis de réduire le nombre de générateurs.

Testons alors la deuxième manière qui consistait à voir si les générateurs $[P_2]$ et $[P_3]$ sont principaux ou non. Le lemme 4.3 nous dit qu'ils le sont si et seulement si il existe $\alpha \in \mathcal{O}$ tel que $\mathrm{N}(\alpha) = \pm \mathrm{N}(P_p) = \pm p$. Dans notre cas, nous devons donc vérifier

— si $\exists x, y \in \mathbb{Z}$ tels que $\left(x + \frac{y}{2}\right)^2 + \frac{23}{4}y^2 = \pm 2$?
Clairement non. Donc P_2 n'est pas principal et $[P_2] \neq [\mathcal{O}]$;

— si $\exists x, y \in \mathbb{Z}$ tels que $\left(x + \frac{y}{2}\right)^2 + \frac{23}{4}y^2 = \pm 3$?
Clairement non. Donc P_3 n'est pas principal et $[P_3] \neq [\mathcal{O}]$.

Nous n'avons donc toujours pas pu réduire notre ensemble de générateurs.

Les étapes déjà effectuées nous permettent pour le moment de savoir que le groupe de classes d'idéaux contient au plus 5 éléments, $|\mathrm{Cl}(F)| \leq 5$, et qu'il possède au plus 4 générateurs. Nous pourrions maintenant calculer l'ordre de certains d'entre eux.
Calculons par exemple l'ordre de $[P_2]$. Pour voir s'il est d'ordre 2, il faut regarder s'il existe $x, y \in \mathbb{Z}$ tels que $\left(x + \frac{y}{2}\right)^2 + \frac{23}{4}y^2 = 2^2$ et $y \neq 0$. Clairement ce n'est pas le cas. Voyons maintenant s'il est d'ordre 3, c'est-à-dire s'il existe $x, y \in \mathbb{Z}$ tels que $\left(x + \frac{y}{2}\right)^2 + \frac{23}{4}y^2 = 2^3$ et $y \neq 0$ et nous voyons que nous avons la solution $x = y = 1$.

Finalement, nous avons que le groupe de classes d'idéaux a au plus 5 éléments et qu'un de ses générateurs est d'ordre 3. Nous en déduisons que $|\mathrm{Cl}(F)| = 3$ et que $\mathrm{Cl}(F)$ est engendré par $[P_2]$. Nous obtenons donc que $\mathrm{Cl}(\mathbb{Q}\sqrt{-23}) \cong \mathbb{Z}/3\mathbb{Z}$.

Comme annoncé, il est parfois nécessaire de rajouter certaines étapes à celles déjà citées.

Par exemple, si la borne de Minkowski est supérieure à 4, la proposition 2.28 va inclure dans les classes d'idéaux possibles de $\mathrm{Cl}(F)$ des classes représentées par des idéaux de norme non première. Il est alors nécessaire de voir ce qu'il en est au cas par cas pour chacune de ces classes d'idéaux. La méthode est alors de factoriser la norme de l'idéal concerné en nombres premiers pour ainsi voir comment il se décompose et obtenir la classe de cet idéal en terme de produit de générateurs. En fonction des informations que nous aurons obtenues sur les générateurs nous pourrons alors dans certains cas simplifier ces produits. D'une situation à l'autre il se pourrait que nous arrivions même à réduire ces classes d'idéaux à des classes déjà connues (comme $[\mathcal{O}]$ par exemple). Mais de toutes façons le principal est que nous saurons de cette manière voir quels sont les différents cas possibles pour les classes d'idéaux de norme non première et ainsi obtenir une borne maximale pour l'ordre de $\mathrm{Cl}(F)$.

En plus de tout cela, il est parfois utile de trouver des relations entre les différents générateurs. Nous pouvons de cette manière nous rendre

compte qu'effectivement certain générateurs sont redondants et ainsi avoir une idée plus précise desquels il possible de retirer de l'ensemble des générateurs.
Pour trouver de telles relations, l'idée est de trouver des $\alpha \in \mathcal{O}$ tels que $\mathrm{N}(\alpha)$ peut se factoriser en un produit intéressant de premiers qui correspondent au normes des idéaux P_p pour lesquels nous souhaitions avoir une relation entre les $[P_p]$.

Tout cela est très théorique, voyons un exemple pour nous éclairer.

EXEMPLE 4.7.
Nous allons calculer le groupe de classes d'idéaux de $F = \mathbb{Q}[\sqrt{-21}]$. Pour cela nous allons suivre le modèle de l'exemple précédent en mettant en plus en application les deux étapes qui viennent d'être expliquées ci-dessus.

Nous commençons par identifier l'anneau des entiers $\mathcal{O}$ correspondant à $\mathbb{Q}[\sqrt{-21}]$. Puisque $D = -21$ et comme $-21 \equiv 3 \pmod 4$, nous avons que $\delta = \sqrt{D} = \sqrt{-21}$ et donc $\mathcal{O} = \mathbb{Z}[\delta] = \mathbb{Z}[\sqrt{-21}]$ De plus, $D_F = -84$.

Nous calculons ensuite la borne de Minkowski qui est

$$\mathfrak{M}_F = \sqrt{|D_F|} \cdot \frac{2}{\pi} = \sqrt{84} \cdot \frac{2}{\pi} \simeq 5.83.$$

Grâce à cette borne et à la proposition 2.28, nous savons que toute classe de $\mathrm{Cl}(F)$ contient un idéal de norme au plus $\mathfrak{M}_F \simeq 5.83$. Nous avons donc pour l'instant que $\mathrm{Cl}(F)$ contient au plus les éléments suivants $\mathrm{Cl}(\mathbb{Q}[\sqrt{-21}]) = \{[\mathcal{O}], [P_2], [\bar{P}_2], [P_3], [\bar{P}_3], [I_4], [P_5], [\bar{P}_5]\}$ où $\mathrm{N}(I_4) = 4$ et nous ne savons a priori pas combien il y a de classes avec comme représentant un idéal de norme 4.

Nous savons ensuite, grâce à la proposition 2.29, qu'un ensemble de générateurs possiblement redondant pour $\mathrm{Cl}(F)$ est donné par tous les idéaux P ayant pour norme p premier tel que $p \leq \mathfrak{M}_F \simeq 5.83$. Les différents p possibles sont donc 2, 3 et 5 et les générateurs correspondants sont $[P_2], [\bar{P}_2], [P_3], [\bar{P}_3], [P_5]$ et $[\bar{P}_5]$.

Essayons de réduire une première fois cet ensemble de générateurs à l'aide du théorème 4.1. Nous calculons que

— $\left(\frac{D_F}{2}\right) = \left(\frac{-84}{2}\right) = 0$ donc $P_2 = \bar{P}_2$;
— $\left(\frac{D_F}{3}\right) = \left(\frac{-84}{3}\right) = 0$ donc $P_3 = \bar{P}_3$;
— $\left(\frac{D_F}{5}\right) = \left(\frac{-84}{5}\right) = 1$ donc $P_5 \neq \bar{P}_5$.

Nous avons donc réduit le nombre de générateurs puisque nous n'avons plus que $[P_2], [P_3], [P_5]$ et $[\bar{P}_5]$.

La deuxième manière pour réduire le nombre de générateurs est de voir si $[P_2]$, $[P_3]$ et $[P_5]$ sont principaux ou non. Le lemme 4.3 nous dit qu'ils le sont si et seulement si il existe $\alpha \in \mathcal{O}$ tel que $\mathrm{N}(\alpha) = \pm\mathrm{N}(P_p) = \pm p$. Dans notre cas, nous devons donc vérifier

— si $\exists x, y \in \mathbb{Z}$ tels que $x^2 + 21y^2 = \pm 2$?
Clairement non. Donc P_2 n'est pas principal et $[P_2] \neq [\mathcal{O}]$;

— si $\exists x, y \in \mathbb{Z}$ tels que $x^2 + 21y^2 = \pm 3$?
Clairement non. Donc P_3 n'est pas principal et $[P_3] \neq [\mathcal{O}]$;

— si $\exists x, y \in \mathbb{Z}$ tels que $x^2 + 21y^2 = \pm 5$?
Clairement non. Donc P_5 n'est pas principal et $[P_5] \neq [\mathcal{O}]$.

Cette fois nous ne pouvons donc pas réduire notre ensemble de générateurs.
Par contre nous déduisons de ces informations sur les générateurs que $[P_2]$ est d'ordre 2 (comme justifié dans la théorie au début de cette section) et donc $[P_2]^2 = [\mathcal{O}]$. De même $[P_3]$ est d'ordre 2 et $[P_3]^2 = [\mathcal{O}]$.

Pour obtenir une borne sur l'ordre de $\mathrm{Cl}(F)$ il nous faudrait maintenant obtenir plus d'informations sur les potentielles classes représentées par un idéal de norme 4. Nous remarquons que si il existe $I_4 \in F$ tel que $\mathrm{N}(I) = 4$, alors I_4 doit se factoriser en deux idéaux de norme 2 [1], $I_4 = P \cdot Q$, $\mathrm{N}(P) = 2 = \mathrm{N}(Q)$. [2] Mais alors, puisque nous avons vu que $P_2 = \bar{P}_2$ et que ce sont les seuls idéaux de norme 2, nous avons que $[P] = [Q] = [P_2]$ et donc $[I_4] = [P_2]^2 = [\mathcal{O}]$.
Dans ce cas nous obtenons que maintenant le groupe de classes d'idéaux contient au plus les éléments suivants $\mathrm{Cl}(\mathbb{Q}\sqrt{-21}) = \{[\mathcal{O}], [P_2], [P_3], [P_5], [\bar{P}_5]\}$.

Les étapes déjà effectuées nous permettent pour le moment de savoir que le groupe de classes d'idéaux contient au plus 5 éléments, $|\mathrm{Cl}(F)| \leq 5$, et qu'il possède au plus 4 générateurs. Nous savons également que deux d'entre eux sont d'ordre 2.

Il est maintenant intéressant de voir s'il existe des relations entre les différents générateurs.
Nous observons que

$$3 + \sqrt{-21} \in \mathcal{O} \text{ avec } \mathrm{N}(3 + \sqrt{-21}) = 30 = 2 \cdot 3 \cdot 5.$$

1. En fait, il se pourrait qu'un idéal de norme 4 ne se factorise pas nécessairement en produit de deux idéaux de norme 2. En effet, si 2 est inerte, il engendre un idéal premier de norme 4. Mais dans ce cas on ne le considère pas dans le groupe de classes d'idéaux puisqu'il est alors principal.

2. Voir la note au bas de la page suivante.

Nous en déduisons, en utilisant le fait que $P_2 = \bar{P}_2$ et $P_3 = \bar{P}_3$, que[3]

$$\mathcal{O}(3+\sqrt{-21}) = P_2 \cdot P_3 \cdot P_5 \text{ (ou } P_2 \cdot P_3 \cdot \bar{P}_5).$$

Dans ce cas, nous avons que

$$[P_2] \cdot [P_3] \cdot [P_5] = [\mathcal{O}] \text{ (ou } [P_2] \cdot [P_3] \cdot [\bar{P}_5] = [\mathcal{O}]).$$

En mettant cette égalité au carré nous obtenons

$$[P_2]^2 \cdot [P_3]^2 \cdot [P_5]^2 = [\mathcal{O}] \text{ (ou } [P_2]^2 \cdot [P_3]^2 \cdot [\bar{P}_5]^2 = [\mathcal{O}]).$$

Mais puisque $[P_2]$ et $[P_3]$ sont d'ordre 2 cela est équivalent à $[P_5]^2 = [\mathcal{O}]$ (ou $[\bar{P}_5]^2 = [\mathcal{O}]$). En combinant cela avec le fait que $[\mathcal{O}] = [P_5][\bar{P}_5]$, nous obtenons que $[P_5] = [\bar{P}_5]$ et par la même occasion que $[P_5]$ est d'ordre 2.
Nous sommes donc parvenus à réduire de un le nombre de générateurs qui ne sont plus que 3, $[P_2]$, $[P_3]$ et $[P_5]$.

À ce stade, nous savons que le groupe de classes d'idéaux contient au plus 4 éléments $\mathrm{Cl}(\mathbb{Q}[\sqrt{-21}]) = \{[\mathcal{O}], [P_2], [P_3], [P_5]\}$, $|\mathrm{Cl}(\mathbb{Q}[\sqrt{-21}])| \leq 4$, et qu'il possède au plus 3 générateurs qui sont tous les trois d'ordre 2.

Mais sur base de la relation $[P_2] \cdot [P_3] \cdot [P_5] = [\mathcal{O}]$, nous remarquons qu'il suffit d'en choisir 2 (le troisième pouvant être exprimé en fonction des deux autres).

Il nous reste à vérifier une seule chose, c'est si $[P_2] \cdot [P_3] = [\mathcal{O}]$ ou non. Ce serait le cas s'il existait $x, y \in \mathbb{Z}$ tels que $x^2 + 21y^2 = 6$. Or nous voyons clairement que ce n'est pas le cas donc $[P_2] \cdot [P_3] \neq [\mathcal{O}]$.

Finalement, nous obtenons que $\mathrm{Cl}(\mathbb{Q}[\sqrt{-21}])$ est engendré par 2 éléments d'ordre 2 et nous en déduisons que $\mathrm{Cl}(\mathbb{Q}[\sqrt{-21}]) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Il est intéressant de remarquer qu'en plus de nous apporter une manière de calculer le groupe de classes d'idéaux, la théorie du chapitre 2 nous permet de répondre à des questions comme par exemple de savoir si pour un certain n donné, il est possible ou non de trouver un corps quadratique tel que son groupe de classes d'idéaux contienne une classe d'idéaux

3. De telles factorisations sont obtenues en combinant le fait que la norme est un homomorphisme et la factorisation unique des idéaux en idéaux premiers.
De manière générale, soit I_k un idéal de norme disons $k \in \mathbb{N}$ dont la factorisation en entiers premiers est $k = \prod_{i=1}^{n} p_i^{\alpha_i}$. Il faut que $\prod_{i=1}^{n} p_i^{\alpha_i} = \mathrm{N}(I_k) = \prod_{j=1}^{m} \mathrm{N}(Q_j)^{\beta_j}$ si $\prod_{j=1}^{m} Q_j^{\beta_j}$ est la factorisation de I_k. Nous remarquons alors que la factorisation $I_k = \prod_{i=1}^{n} P_{p_i}^{\alpha_i}$ convient. Nous pourrions également prendre les conjugués des idéaux P_{p_i} mais dans notre cas ci-dessus nous savons que $P_2 = \bar{P}_2$ et $P_3 = \bar{P}_3$ c'est pourquoi il n'y a plus que deux possibilités.

d'ordre n (c'est ce que nous verrons dans la propriété 4.9). Voyons quelques résultats de ce type.

LEMME 4.8. *Soit $D < 0$ sans facteur carré tel que $F = \mathbb{Q}[\sqrt{D}]$ contienne un idéal divisant 2 qui soit d'ordre $n > 2$ dans le groupe de classes d'idéaux. Alors $D \equiv 1 \pmod 8$.*

DÉMONSTRATION. Soit P un tel idéal divisant 2, c'est-à-dire $P|2$ ce qui est équivalent à $P|\mathcal{O}2$ ou encore $\mathcal{O}2 \subseteq P$. Par hypothèse P est également tel que $[P]^n = [P^n] = [\mathcal{O}]$ pour $n \geq 3$ et $[P]^a \neq [\mathcal{O}]$ pour $a < n$. Notons cet idéal P_2.
Nous avons donc que $\mathcal{O}2$ se factorise comme $\mathcal{O}2 = P_2 \cdot \bar{P}_2$ ce qui est équivalent au niveau des classes à $[\mathcal{O}] = [P_2][\bar{P}_2]$.
Nous observons alors que

- $P_2 \neq \mathcal{O}2$ (car sinon $[P_2] = [\mathcal{O}]$) donc 2 est non inerte par définition ;
- $P_2^2 \neq \mathcal{O}2$ (car sinon $[P_2]^2 = [\mathcal{O}]$) donc 2 est non ramifié par définition.

Nous avons donc que 2 doit être décomposé, c'est-à-dire par le théorème 4.1 que $\left(\frac{D_F}{2}\right) = 1$ ce qui implique que $D_F \equiv \pm 1 \pmod 8$.
Mais alors, par le tableau récapitulatif du début de cette section, nous avons que $D_F = D$ et $D \equiv 1 \pmod 4$.
Cela entraîne que $D_F \equiv -1 \pmod 8$ est impossible et donc finalement il faut que $D \equiv 1 \pmod 8$. □

PROPOSITION 4.9. *Soit $n \geq 3$ fixé. Pour $D = -2^{n+2} + 1$, le groupe de classes d'idéaux du corps quadratique $\mathbb{Q}[\sqrt{D}]$ contient un élément d'ordre n.*

DÉMONSTRATION. Nous allons montrer que cet élément est en fait la classe de P_2 qui est alors d'ordre n.

Si P_2 est d'ordre strictement supérieur à 2, le lemme précédent nous dit qu'alors D doit être congru à 1 modulo 8. Nous voyons que c'est bien le cas pour $D = -2^{n+2} + 1$ avec $n \geq 3$. Afin de voir que P_2 est bel et bien d'ordre n, par la proposition 4.4 et son corollaire, il faut vérifier qu'il existe $\alpha \in \mathcal{O} \setminus \mathbb{Z}$ tel que $\mathrm{N}(\alpha) = 2^n$ mais pas de $\beta \in \mathcal{O} \setminus \mathbb{Z}$ tel que $\mathrm{N}(\beta) = 2^r$ avec $r < n$.

Un tel α s'écrit $x + \frac{1+\sqrt{D}}{2}y$ et sa norme est $\mathrm{N}(\alpha) = (x + \frac{y}{2})^2 + \frac{2^{n+2}-1}{4}y^2$ avec $y \neq 0$. Nous calculons qu'en prenant $x = 0$ et $y = 1$ nous obtenons

$$\mathrm{N}(\alpha) = \left(\frac{1}{2}\right)^2 + \frac{2^{n+2} - 1}{4} = 2^n$$

donc $\alpha = \frac{1+\sqrt{D}}{2}$ convient.

Voyons maintenant que si nous prenons un $\beta = a + \frac{1+\sqrt{D}}{2}b \in \mathcal{O} \setminus \mathbb{Z}$ nous avons

$$\mathrm{N}(\beta) = \left(a + \frac{b}{2}\right)^2 + \frac{2^{n+2}-1}{4}b^2 \geq \frac{2^{n+2}-1}{4}.$$

L'égalité $\mathrm{N}(\beta) = 2^r$ avec $r < n$ impliquerait que $2^r \geq \frac{2^{n+2}-1}{4}$ ou encore $2^{r+2} \geq 2^{n+2} - 1$ ce qui est impossible étant donné que $r < n$. Il n'existe donc pas de tel $\beta \in \mathcal{O} \setminus \mathbb{Z}$.

Cela termine de montrer que soit $n \geq 3$ donné, $D = -2^{n+2} + 1$ est tel que $\mathrm{Cl}(\mathbb{Q}\sqrt{D})$ contient une classe d'ordre n qui est la classe de P_2. □

Ce genre de raisonnement peut se généraliser un peu pour obtenir d'autres résultats du même type dont certains sont mis ci-dessous.

LEMME 4.10. *Soit $D < 0$ sans facteur carré tel que $F = \mathbb{Q}[\sqrt{D}]$ contienne un idéal divisant 3 qui soit d'ordre $n > 2$ dans le groupe de classes d'idéaux. Alors soit $D \equiv 1 \pmod{12}$, $D \equiv -2 \pmod{12}$ ou $D \equiv -5 \pmod{12}$.*

DÉMONSTRATION. Procédons comme pour la démonstration du lemme précédant en adaptant lorsque nécessaire puisque nous ne travaillons plus avec le nombre premier 2 mais cette fois avec 3.

Soit P un tel idéal divisant 3, c'est-à-dire $P|3$ ce qui est équivalent à $P|\mathcal{O}3$ ou encore $\mathcal{O}3 \subseteq P$. Par hypothèse P est également tel que

$$[P]^n = [P^n] = [\mathcal{O}] \text{ pour } n \geq 3 \text{ et } [P]^a \neq [\mathcal{O}] \text{ pour } a < n.$$

Notons cet idéal P_3.
Nous avons donc que $\mathcal{O}3$ se factorise comme $\mathcal{O}3 = P_3 \cdot \bar{P}_3$ ce qui est équivalent au niveau des classes à $[\mathcal{O}] = [P_3][\bar{P}_3]$.
Nous observons alors que

- $P_3 \neq \mathcal{O}3$ (car sinon $[P_3] = [\mathcal{O}]$) donc 3 est non inerte par définition ;
- $P_3^2 \neq \mathcal{O}3$ (car sinon $[P_3]^2 = [\mathcal{O}]$) donc 3 est non ramifié par définition.

Nous avons donc que 3 doit être décomposé, c'est-à-dire par le théorème 4.1 que $\left(\frac{D_F}{3}\right) = 1$ ce qui implique que $1 \equiv D_F \pmod{3}$ par définition du symbole de Legendre. Nous pouvons réécrire cette condition sous la forme $D_F = 3k + 1$.
Mais alors, par le tableau récapitulatif du début de cette section, nous avons les possibilités suivantes

— $D_F = D \equiv 1 \pmod 4$ et $D_F = 3k+1$:
Dans ce cas $3k+1 \equiv 1 \pmod 4$ c'est-à-dire $3k \equiv 0 \pmod 4$ et nous avons que $k \in \mathbb{Z}$ est un multiple de 4 que nous notons $k = 4d$.
Donc $D_F = 3k+1 = 3(4d)+1 = 12d+1$.
Cela donne $D = D_F = 12d+1$.

— $\frac{D_F}{4} = D \equiv 2 \pmod 4$ et $D_F = 3k+1$:
Dans ce cas $\frac{3k+1}{4} \equiv 2 \pmod 4$ c'est-à-dire $3k+1 \equiv 8 \pmod{16}$ ce qui implique $3k \equiv 7 \pmod{16}$ ou encore $k \equiv -3 \pmod{16}$. Donc $k = 16d-3$ et $D_F = 3k+1 = 3(16d-3)+1 = 48d-8$.
Cela donne $D = \frac{D_F}{4} = 12d-2$.

— $\frac{D_F}{4} = D \equiv 3 \pmod 4$ et $D_F = 3k+1$:
Dans ce cas $\frac{3k+1}{4} \equiv 3 \pmod 4$ c'est-à-dire $3k+1 \equiv 12 \pmod{16}$ ce qui implique $3k \equiv 11 \pmod{16}$ ou encore $k \equiv -7 \pmod{16}$.
Donc $k = 16d-7$ et $D_F = 3k+1 = 3(16d-7)+1 = 48d-20$.
Cela donne $D = \frac{D_F}{4} = 12d-5$.

□

PROPOSITION 4.11. *Soit $n \geq 3$ fixé. Si n est impair Pour $D = 1-3^n$, le groupe de classes d'idéaux du corps quadratique $\mathbb{Q}[\sqrt{D}]$ contient un élément d'ordre n. Et si n est pair, l'énoncé est valable pour $D = 4-3^n$.*

DÉMONSTRATION. Nous allons montrer que dans les deux cas, cet élément est la classe de P_3 qui est alors d'ordre n.

Pour n impair, plaçons nous dans le deuxième cas de la proposition précédente, où $D \equiv 2 \pmod 4$ et $D_F = 48d-8$ ou encore $D \equiv -2 \pmod{12}$. Nous observons que $D = 1-3^n$ respecte bien ces conditions.
Nous souhaitons montrer que P_3 est d'ordre n dans le groupe de classes d'idéaux. Pour cela il faut, d'après la proposition 4.4 et son corollaire, qu'il existe $\alpha \in \mathcal{O} \setminus \mathbb{Z}$ tel que $\mathrm{N}(\alpha) = 3^n$ mais pas de $\beta \in \mathcal{O} \setminus \mathbb{Z}$ tel que $\mathrm{N}(\beta) = 3^r$ avec $r < n$. Dit autrement, nous souhaitons trouver $\alpha = x + y\sqrt{D}$ avec $y \neq 0$ qui soit qui soit solution de l'équation $\mathrm{N}(\alpha) = x^2 - Dy^2 = 3^n$ mais qu'il n'existe pas de $\beta = a + b\sqrt{D}$ avec $b \neq 0$ solution d'une équation $\mathrm{N}(\beta) = a^2 - Db^2 = 3^r$ avec $r < n$.
Nous observons facilement que si nous prenons $x = y = 1$, nous obtenons que

$$\mathrm{N}(\alpha) = 1 - D = 3^n$$

donc $\alpha = 1 + \sqrt{D}$ convient. Il faut maintenant s'assurer que l'équation $\mathrm{N}(\beta) = a^2 - Db^2 = 3^r$ avec $r < n$ n'ait pas de solution pour $b \neq 0$. Cela découle simplement du fait que dans ce cas $-D = 3^n - 1 > 3^r$.
Tout ceci nous montre que P_3 est d'ordre n.

Pour n pair, plaçons nous cette fois dans le troisième cas de la propriété précédente, pour lequel $D \equiv 3 \pmod 4$ et $D_F = 48d - 20$ ou encore $D \equiv -5 \pmod{12}$. Nous observons que $D = 4 - 3^n$ respecte bien ces conditions.
A nouveau nous voulons montrer que P_3 est d'ordre n dans ces nouvelles conditions. Nous pouvons pour cela suivre un raisonnement tout à fait similaire à celui ci-dessus. Nous ne réécrivons donc pas tous les détails et observons simplement les résultats importants ci-dessous

— Soit $\alpha = x + y\sqrt{D} \in \mathcal{O} \setminus \mathbb{Z}$, si nous prenons $x = 2$ et $y = 1$ nous calculons que $\mathrm{N}(\alpha) = 4 - D = 3^n$.

— Soit $\beta = a + b\sqrt{D} \in \mathcal{O} \setminus \mathbb{Z}$, si $r < n$ il n'y a pas de solution à l'équation $\mathrm{N}(\beta) = a^2 - Db^2 = 3^r$ puisque $-D = 3^n - 4 > 3^r$.

Ces deux observations permettent de conclure que P_3 est d'ordre n.

Cela termine de montrer que soit $n \geq 3$ donné, $D = 1 - 3^n$ est tel que $\mathrm{Cl}(\mathbb{Q}\sqrt{D})$ contient une classe d'ordre n qui est la classe de P_3 si n est impair et la classe de P_3 est d'ordre n dans $\mathrm{Cl}(\mathbb{Q}\sqrt{D})$ si n est pair et $D = 4 - 3^n$. □

Pour conclure cette partie, mentionnons que, même si les exemples traités ici étaient d'une longueur raisonnable, certains corps quadratiques peuvent mener à des calculs beaucoup plus longs et fastidieux. C'est pourquoi les outils développés au chapitre 3 sont, comme nous allons le voir très bientôt, particulièrement utiles pour le calcul des groupes de classes d'idéaux.

Corps quadratiques réels. Le lecteur attentif a probablement noté que les exemples traités ci-dessus ne concernaient que les corps quadratiques imaginaires sur lesquels nous concentrons notre attention dans ce document. Il est tout de même intéressant de faire remarquer qu'en ce qui concerne les méthodes développées au chapitre 2 et illustrées dans cette section, elles s'appliquent également pour les corps quadratiques imaginaires. D'un point de vue théorique il n'y a pas d'obstacle à utiliser cette approche. La

différence entre corps quadratiques imaginaires et réels réside ici uniquement dans le fait que l'application des techniques est moins aisée dans le cas réel. En effet, l'existence de solutions aux équations quadratiques que nous sommes amenés à considérer, par exemple lorsque nous souhaitons voir si un idéal est principal ou non, est plus compliquée à tester puisque les formes quadratiques sont indéfinies.

Il est donc possible de calculer le groupe de classes d'idéaux de certains corps quadratiques réels en utilisant la théorie du chapitre 2 et en procédant de manière tout à fait similaire à ce que nous avons fait dans cette section. Pour illustrer cela nous pouvons voir l'exemple suivant.

EXEMPLE 4.12.
Nous allons calculer le groupe de classes d'idéaux de $F = \mathrm{Cl}(\mathbb{Q}[\sqrt{10}])$. Pour cela nous allons suivre les mêmes étapes que lors des exemples de corps quadratiques imaginaires précédents.

Nous commençons par identifier l'anneau des entiers $\mathcal{O}$ correspondant à $\mathbb{Q}[\sqrt{10}]$. Puisque $D = 10$ et comme $10 \equiv 2 \pmod 4$, nous avons que $\delta = \sqrt{D} = \sqrt{10}$ et donc $\mathcal{O} = \mathbb{Z}[\delta] = \mathbb{Z}[\sqrt{10}]$. De plus, $D_F = 40$.

Comme F est réel, pour calculer la borne de Minkowski, il faut prendre l'autre formule et nous obtenons

$$\mathfrak{M}_F = \sqrt{|D_F|} \cdot \frac{1}{2} = \sqrt{40} \cdot \frac{1}{2} \simeq 3.16.$$

Par la proposition 2.28, nous savons que toute classe de $\mathrm{Cl}(F)$ contient un idéal de norme au plus $\mathfrak{M}_F \simeq 3.16$. Nous avons donc pour l'instant que $\mathrm{Cl}(F)$ contient au plus les éléments suivants

$$\mathrm{Cl}(\mathbb{Q}[\sqrt{10}]) = \{[\mathcal{O}], [P_2], [\bar{P}_2], [P_3], [\bar{P}_3]\}.$$

Ensuite, par la proposition 52.29, nous avons qu'un ensemble de générateurs possiblement redondant pour $\mathrm{Cl}(F)$ est donné par tous les idéaux P ayant pour norme p premier tel que $p \leq \mathfrak{M}_F \simeq 3.16$. Les différents p possibles sont donc 2 et 3 et les générateurs correspondants $[P_2]$, $[\bar{P}_2]$, $[P_3]$ et $[\bar{P}_3]$.

Essayons de réduire une première fois cet ensemble de générateurs à l'aide du théorème 4.1. Nous calculons que

— $\left(\frac{D_F}{2}\right) = \left(\frac{40}{2}\right) = 0$ donc $P_2 = \bar{P}_2$;

— $\left(\frac{D_F}{3}\right) = \left(\frac{40}{3}\right) = 1$ donc $P_3 \neq \bar{P}_3$.

Nous avons donc réduit le nombre de générateurs puisque nous n'avons plus que $[P_2]$, $[P_3]$ et $[\bar{P}_3]$.

La deuxième manière de les réduire est de voir si $[P_2]$ et $[P_3]$ sont principaux ou non. Le lemme 4.3 nous dit qu'ils le sont si et seulement si il existe $\alpha \in \mathcal{O}$ tel que $\mathrm{N}(\alpha) = \pm \mathrm{N}(P_p) = \pm p$. Dans notre cas, nous devons donc vérifier

— si $\exists x, y \in \mathbb{Z}$ tels que $x^2 - 10y^2 = \pm 2$?
Si nous réduisons modulo 5, c'est équivalent à trouver une solution de $x^2 \equiv \pm 2 \pmod 5$, ce qui n'a pas de solution car $\left(\frac{\pm 2}{5}\right) = -1$. Donc P_2 n'est pas principal et $[P_2] \neq [\mathcal{O}]$;

— si $\exists x, y \in \mathbb{Z}$ tels que $x^2 - 10y^2 = \pm 3$?
Même raisonnement avec $\left(\frac{\pm 3}{5}\right) = -1$ et donc $[P_3] \neq [\mathcal{O}]$.

Cette fois nous ne pouvons donc pas réduire notre ensemble de générateurs.

Par contre nous déduisons de ces informations que $[P_2]$ est d'ordre 2 et donc $[P_2]^2 = [\mathcal{O}]$.

Les étapes déjà effectuées nous permettent pour le moment de savoir que le groupe de classes d'idéaux contient au plus 4 éléments, $|\mathrm{Cl}(F)| \leq 4$, et qu'il possède au plus 3 générateurs dont l'un d'entre eux est d'ordre 2.

Il est maintenant intéressant de voir s'il existe des relations entre les différents générateurs.
Nous observons que $2 + \sqrt{10} \in \mathcal{O}$ et que $\mathrm{N}(2 + \sqrt{10}) = -6 = -2 \cdot 3$. Nous en déduisons, en utilisant le fait que $P_2 = \bar{P}_2$, que $\mathcal{O}(2 + \sqrt{10}) = P_2 \cdot P_3$ (ou $P_2 \cdot \bar{P}_3$). Dans ce cas, nous avons que $[P_2] \cdot [P_3] = [\mathcal{O}]$ (ou $[P_2] \cdot [\bar{P}_3] = [\mathcal{O}]$) et donc $[P_2] = [\bar{P}_3]$ (ou $[P_2] = [P_3]$). Remarquons que si $[P_2] = [\bar{P}_3]$ alors $[\bar{P}_2] = [P_3]$ et comme $[\bar{P}_2] = [P_2]$ nous retombons sur $[P_2] = [P_3]$.
Cela nous montre que $[P_2] = [\bar{P}_2] = [P_3] = [\bar{P}_3]$.

Finalement, nous obtenons que $\mathrm{Cl}(\mathbb{Q}[\sqrt{10}]) = \{[\mathcal{O}], [P_2]\}$ est d'ordre 2 et est engendré par un élément d'ordre 2, nous en déduisons que $\mathrm{Cl}(\mathbb{Q}[\sqrt{10}]) \cong \mathbb{Z}/2\mathbb{Z}$.

Cet exemple nous montre bien que nous pouvons suivre les même étapes que lorsque nous travaillons avec des corps quadratiques imaginaires mais que les normes d'éléments peuvent être plus difficiles à traiter. En effet, comme annoncé, pour voir si les idéaux étaient principaux il a été moins évident de déterminer si oui ou non une solution aux équations considérées existait et il a fallu faire appel à un argument supplémentaire qui est

celui des modulos. Calculer le groupe de classes d'idéaux avec cette approche pour le cas de corps quadratiques réels, bien que possible, peut devenir assez vite fastidieux c'est pourquoi il vaut mieux développer d'autres méthodes.

2. Approche des formes quadratiques

Dans cette deuxième section nous allons nous servir de la théorie du chapitre 3 sur les formes quadratiques pour obtenir d'autres méthodes de calcul du groupe de classes d'idéaux qui dans certains cas nous permettront de simplifier grandement des calculs que nous aurions déjà pu réaliser dans la section précédente.

Avant d'entrer dans le calcul du groupe de classes d'idéaux à proprement parler, il est intéressant de mentionner que les formes quadratiques peuvent nous permettre, de modifier (ou ajouter) certaines des étapes vues dans la section précédente.

En plus de ces adaptations, la correspondance entre les formes quadratiques et les idéaux, nous permet, comme mentionné au chapitre précédent, de calculer l'ordre du groupe de classes d'idéaux d'un corps quadratique F imaginaire en recensant uniquement les formes quadratiques réduites de discriminant D_F dont le nombre nous donnera l'ordre du groupe de classes d'idéaux et ensuite de voir les informations obtenues par la même occasion sur les éléments de 2-torsion. Voyons concrètement sur l'exemple suivant ce que ça donne.

EXEMPLE 4.13. Soit $F = \mathbb{Q}[\sqrt{-14}]$. Si nous souhaitons calculer son groupe de classes d'idéaux $\mathrm{Cl}(F)$, il nous suffit, dans certains cas [4], de calculer le nombre de classes $h(\mathbb{Q}[\sqrt{-14}])$ et de voir combien d'éléments de 2-torsion sont contenus dans $\mathrm{Cl}(F)$.

Commençons par voir que comme $D = -14$ et que $-14 \equiv 2 \pmod 4$, le discriminant est $D_F = -56$.

4. Bien que dans des cas comme celui traité ici, ces informations sur l'ordre et les éléments de 2-torsion nous permettent parfois de déterminer totalement la structure du groupe de classes d'idéaux du corps quadratique imaginaire, il faut garder à l'esprit que ce n'est pas toujours le cas.

Listons maintenant toutes les formes quadratiques réduites définies positives. Par la proposition 3.32 nous avons que

$$|b| \leq \sqrt{\frac{|D_F|}{3}} = \sqrt{\frac{56}{3}} \simeq 4.32 \text{ et } \begin{array}{lll} b \equiv D_F \pmod 2 & \Leftrightarrow & b \equiv -56 \pmod 2 \\ & \Leftrightarrow & b \equiv 0 \pmod 2. \end{array}$$

Nous pouvons alors nous baser toujours sur la même proposition afin d'obtenir des informations sur les coefficients a et c et inscrire dans un tableau récapitulatif tous les cas possibles.

$\lvert b\rvert = a_{\min}$	$ac = \frac{b^2 - D_F}{4} = \frac{b^2+56}{4}$	$\lfloor \sqrt{ac} \rfloor = a_{\max}$	(a,c)
0	$14 = 2 \cdot 7$	3	$(1,14)^+, (2,7)^+$
2	$15 = 3 \cdot 5$	3	$(3,5)$
4	$18 = 2 \cdot 3^2$	4	

Les paires marquées d'un $+$ représentent celles auxquelles correspond une seule valeur de $b \geq 0$ (soit car $b = 0$ soit car la condition de bord $a = |b|$ ou $a = c$ est satisfaite), nous observons que le nombre total de formes réduites définies positives est $2 + 2 \cdot 1 = 4$.
Le groupe des classes d'idéaux est donc un groupe abélien d'ordre 4.
De plus, par le corollaire 3.48, les classes d'idéaux de 2-torsion correspondent précisément aux formes quadratiques marquées d'un $+$, il y en a donc 2.

Nous en concluons que $\mathrm{Cl}(\mathbb{Q}[\sqrt{-14}]) \cong \mathbb{Z}/4\mathbb{Z}$.

L'exemple que nous venons de voir illustre bien le fait que le calcul du groupe de classes d'idéaux, grâce aux formes quadratiques, est devenu beaucoup plus simple et plus rapide.

Un autre exemple intéressant à remarquer pour sa particularité est le suivant.

EXEMPLE 4.14. Soit $F = \mathbb{Q}[\sqrt{-163}]$. Si nous souhaitons calculer son groupe de classes d'idéaux $\mathrm{Cl}(F)$, il nous suffit de procéder comme dans l'exemple précédent.

Cette fois, $D = -163$ et $-163 \equiv 1 \pmod 4$ donc le discriminant est $D_F = -163$.

Nous avons donc, par la proposition 3.32

$$|b| \leq \sqrt{\frac{|D_F|}{3}} = \sqrt{\frac{163}{3}} \simeq 7.37 \text{ et } \begin{array}{lll} b \equiv D_F \pmod 2 & \Leftrightarrow & b \equiv -163 \pmod 2 \\ & \Leftrightarrow & b \equiv 1 \pmod 2. \end{array}$$

Le tableau récapitulatif est

$\lvert b\rvert = a_{\min}$	$ac = \frac{b^2 - D_F}{4} = \frac{b^2+163}{4}$	$\lfloor \sqrt{ac} \rfloor = a_{\max}$	(a,c)
1	$41 = 1 \cdot 41$	6	$(1,41)^+$
3	$43 = 1 \cdot 43$	6	
5	$47 = 1 \cdot 47$	6	
7	$53 = 1 \cdot 53$	7	

Nous observons qu'ici il n'y a qu'une forme quadratique réduite définie positive. Elle est de 2-torsion puisque le neutre est toujours de 2-torsion. Nous nous retrouvons donc avec $\mathrm{Cl}(F)$ qui est un groupe abélien d'ordre 1.

Nous concluons que $\mathrm{Cl}(\mathbb{Q}[\sqrt{-163}]) = [\mathcal{O}]$.

La particularité de cet exemple est que, comme nous pouvons le remarquer, le groupe de classes d'idéaux est trivial. Nous en déduisons que la factorisation en irréductibles est unique dans l'anneau des entiers du corps quadratique $\mathbb{Q}[\sqrt{-163}]$.

Corps quadratiques réels. Contrairement à la section précédente, nous ne pouvons cette fois pas utiliser la même approche que celle ci-dessus avec des corps quadratiques réels. En effet, une bonne partie de la théorie du chapitre 3 était valable uniquement pour les formes quadratiques définies, c'est-à-dire pour les corps quadratiques imaginaires, c'est pourquoi tout au long de ce chapitre nous avions fait l'hypothèse que le discriminant était strictement négatif. Les corps quadratiques réels nécessitent d'autres notions qui ne sont pas traitées dans ce document consacré principalement aux corps quadratiques imaginaires.

Conclusion

Pour conclure ce travail, rappelons que le groupe de classes d'idéaux est un outil puissant permettant de déterminer si la factorisation en irréductibles est unique ou non dans l'anneau des entiers d'un corps quadratique donné. Différentes approches ont été abordées en se focalisant principalement sur les corps quadratiques imaginaires. Dans le cas des corps quadratiques réels, des modifications sont souvent nécessaires et pour le cas de l'approche avec les formes quadratiques il faut même faire appel à des notions supplémentaires telles que par exemple les *fractions continues* ou encore le *groupe de classes restreint*. Si le lecteur est intéressé par ces théories il est vivement encouragé à continuer son exploration passionnante de la théorie algébrique des nombres.

Terminons en mentionnant pour la curiosité que le théorème de Stark-Heegner qui fut prouvé en 1952 par le mathématicien allemand Kurt Heegner indique qu'il n'existe que 9 corps quadratiques imaginaires ayant un groupe de classes d'idéaux trivial, c'est-à-dire pour lesquels la factorisation est unique dans leur anneau d'entiers. Ce sont $\mathbb{Q}[\sqrt{-1}], \mathbb{Q}[\sqrt{-2}], \mathbb{Q}[\sqrt{-3}]$, $\mathbb{Q}[\sqrt{-7}], \mathbb{Q}[\sqrt{-11}], \mathbb{Q}[\sqrt{-19}], \mathbb{Q}[\sqrt{-43}], \mathbb{Q}[\sqrt{-67}]$ et $\mathbb{Q}[\sqrt{-163}]$ [5].
Pour simple information également, en ce qui concerne les corps quadratiques réels, Gauss a conjecturé qu'il en existait une infinité tels que le groupe de classes d'idéaux soit trivial. Cette conjecture n'est toujours pas démontrée [6].

5. Ce résultat avait d'abord été conjecturé par Gauss et ce n'est qu'en 1967 qu'il a été reconnu que la preuve apportée par Heegner était valide.

6. La page sur laquelle j'ai lu cette information avait été modifiée pour la dernière fois le 20 février 2020

Bibliographie

[1] M. Trifković, *Algebraic Theory of Quadratic Numbers*, Universitext, Vol.?, Springer Science+Business Media, New York, 2013. ↑1, 20, 21, 26

[2] P. Samuel, *Théorie algébrique des nombres*, Collection méthodes, Hermann, 2003. ↑2

[3] M. H. Weissman, *An illustrated theory of numbers*, American Mathematical Society, 2017. ↑6, 7

[4] D. Perrin, *Anneaux d'entiers des corps quadratiques imaginaires*, TER (Travail d'Etude et de Recherche de maîtrise), Orsay, ?. ↑2, 16, 17, 23

[5] M. Hazewinkel, N. Gubareni, and V. V. Kirichenko, *Algebras, Rings and Modules Volume 1*, Mathematics and Its Applications, Kluwer Academic Publishers, 2004. ↑5

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Faculté des sciences
Place des sciences, 2 bte L6.06.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/sc**