

# Polynôme d'Euler et groupe des classes des corps quadratiques imaginaires

Q.BRAMAS (quentin@bramas.fr)

3 juin 2010

Dirigé par M. Thierry LAMBRE

# Table des matières

<b>1</b>	<b>Préliminaires</b>	<b>5</b>
<b>2</b>	<b>Décomposition des nombres premiers dans un corps quadratique</b>	<b>5</b>
2.1	Symbole de Legendre . . . . .	5
2.2	Générateurs des idéaux premiers de la décomposition de $Ap$ . . . . .	7
<b>3</b>	<b>Finitude du groupe des classes d'idéaux</b>	<b>9</b>
3.1	Théorème de Minkowski . . . . .	9
3.2	Plongement canonique d'un corps quadratique . . . . .	11
3.3	Théorème de Dirichlet . . . . .	13
<b>4</b>	<b>Calcul du nombre de classes</b>	<b>16</b>
4.1	Idéaux primitifs du groupe des classes . . . . .	16
4.2	Premiers calculs . . . . .	17
<b>5</b>	<b>Théorème Final</b>	<b>18</b>

Je remercie M. Thierry LAMBRE pour son aide, son soutiens et sa patience.

## Introduction

Ce dossier est le résultat d'un travail encadré de recherche au cours de ma première année de master recherche à Clermont-Ferrand. Mon intérêt pour l'algèbre et l'arithmétique m'ont très vite conduits vers ce sujet qui interpelle par l'éloignement entre la simplicité du résultat et les outils nécessaires à sa démonstration.

Le sujet commence par l'observation intrigante d'un polynôme et des questions qui s'en suivent. Prenons l'exemple du polynôme d'Euler  $f(X) = X^2 + X + 41$  qui est tel que  $f(n)$  est un nombre premier pour  $n = 0, 1, 2, \dots, 39$  ( $f(n) = 41, 43, 47, \dots, 1523, 1601$ ).

Existe-t-il d'autres polynômes comme celui là ? En faite on peut trouver d'autres polynôme de la forme  $X^2 + X + q$  avec  $q$  un nombre premier avec la même propriété, c'est à dire générant des nombres premiers pour  $X = 0, 1, \dots, q - 2$ . Par exemple pour  $q = 2, 3, 5, 11, 17, 41$  la propriété est vraie. Cependant pour  $q = 7, 13, 19, 23, 29$ , elle est fausse.

Peut-on trouver un nombre premier  $q > 41$  ayant cette propriété ? Les nombres premiers vérifiant cette propriété sont-ils en nombre fini ? Si oui quel est le plus grand ?

C'est à ces questions que va répondre mon projet.

Ce n'est qu'à la dernière section qu'on démontre que le résultat dépend du nombre de classe des corps quadratiques imaginaires, expliquant ainsi le cheminement du dossier.

# 1 Préliminaires

Soit l'extension  $K = \mathbb{Q}[\sqrt{d}]$  avec  $d$  un entier relatif sans facteurs carrés. L'anneau des entiers  $A$  de  $K$  est l'ensemble des éléments de  $K$  qui sont racines d'un polynôme unitaire de  $\mathbb{Z}$ . On rappelle que si  $d \equiv 2$  ou  $3[4]$ , alors  $(1, \sqrt{d})$  est une  $\mathbb{Z}$ -base de  $A$  et le discriminant de  $K$  est  $\delta = 4d$ . Dans le cas où  $d \equiv 1[4]$ , alors  $(1, \frac{1+\sqrt{d}}{2})$  est une  $\mathbb{Z}$ -base de  $A$  et le discriminant de  $K$  est  $\delta = d$ .

**Théorème 1.** *Soit l'extension quadratique  $K = \mathbb{Q}[\sqrt{d}]$  avec  $d$  un entier relatif sans facteurs carrés. Soit  $A$  l'anneau des entiers de  $K$ . Soit  $I$  un idéal fractionnaire de  $A$ . On a alors la décomposition unique de  $I$  en facteur d'idéaux premiers :*

$$I = \prod_{i=1}^r P_i^{e_i}$$

avec si  $I = Ap$ , pour  $p$  un nombre premier :

$$2 = \sum_{i=1}^r e_i f_i$$

Où  $f_i$  est un entier correspondant à la dimension de  $A/P_i$  vu comme espace vectoriel sur  $\mathbb{Z}/p\mathbb{Z}$ .

**Théorème 2.** *Soit  $I$  un idéal d'un anneau  $A$ .  $I$  est le produit de deux idéaux premiers si et seulement si  $A/I$  est le produit de deux corps.*

**Théorème 3.** *Soit  $I$  un idéal d'un anneau  $A$ .  $I$  est le carré d'un idéal premier si et seulement si  $A/I$  a des éléments nilpotents.*

## 2 Décomposition des nombres premiers dans un corps quadratique

### 2.1 Symbole de Legendre

Soit l'extension quadratique  $K = \mathbb{Q}[\sqrt{d}]$  avec  $d$  un entier relatif sans facteurs carrés. Soit  $A$  l'anneau des entiers de  $K$ . Soit  $p$  un nombre premier impair de  $\mathbb{Z}$ . Étudions la décomposition de l'idéal principal  $Ap$  en facteurs d'idéaux premiers.

On a déjà :

$$Ap = \prod_{i=1}^q P_i^{e_i} \quad \text{avec } P_i \text{ des idéaux premiers de } A$$

Avec :

$$\sum_{i=1}^q e_i f_i = 2$$

On a donc 3 cas possibles :

1.  $q = 1, e_1 = 1, f_1 = 2$  :

$$Ap = P \quad \text{on dit que } p \text{ est inerte} \quad (1)$$

2.  $q = 1, e_1 = 2, f_1 = 1$  :

$$Ap = P^2 \quad \text{on dit que } p \text{ est ramifié} \quad (2)$$

3.  $q = 2, e_1 = 1, f_1 = 1$  :

$$Ap = P_1 P_2 \quad P_1 \neq P_2, \text{ on dit que } p \text{ est décomposé} \quad (3)$$

Étudions la forme de  $A/Ap$  en fonction de  $p$  un nombre premier impair. Prenons  $d \equiv 1[4]$ , on a  $A = \mathbb{Z} + \mathbb{Z} \frac{1+\sqrt{d}}{2}$ , soit  $\alpha \in A$ ,  $\alpha = a + b \frac{1+\sqrt{d}}{2}$ ,  $a, b \in \mathbb{Z}$ .

Si  $b$  est pair,  $\alpha = a + \frac{b}{2} + \frac{b}{2} \sqrt{d} \in \mathbb{Z} + \mathbb{Z} \sqrt{d}$

sinon  $\alpha = a + (b+p) \frac{1+\sqrt{d}}{2} = a + \frac{b+p}{2} + \frac{b+p}{2} \sqrt{d}$  modulo  $Ap$ .

D'où :  $A/Ap \cong \mathbb{Z} + \mathbb{Z} \sqrt{d}/Ap$ .

Pour  $d \equiv 2[4]$  ou  $d \equiv 3[4]$ , on a directement :  $A/Ap \cong \mathbb{Z} + \mathbb{Z} \sqrt{d}/Ap$ .

Ainsi on obtient :  $A/Ap \cong \mathbb{Z} + \mathbb{Z} \sqrt{d}/Ap$  pour toutes valeur de  $d$ .

Or  $\mathbb{Z} + \mathbb{Z} \sqrt{d} \cong \mathbb{Z}[X]/(X^2 - d)$ , ce qui nous donne :

$$A/Ap \cong (\mathbb{Z}[X]/(X^2 - d))/Ap \cong (\mathbb{Z}[X]/(p))/(X^2 - \bar{d}) \cong (\mathbb{F}_p[X])/(X^2 - \bar{d})$$

On a donc :

$$\begin{cases} \bar{d} \text{ est un carré non-nul} \\ \bar{d} \text{ est nul} \\ \bar{d} \text{ n'est pas nul et n'est pas un carré} \end{cases} \Rightarrow \begin{cases} X^2 - \bar{d} \text{ se décompose en } (X + \sqrt{\bar{d}})(X - \sqrt{\bar{d}}) \\ X^2 - \bar{d} \text{ devient } X^2 \\ X^2 - \bar{d} \text{ est irréductible} \end{cases}$$

$$\Rightarrow \begin{cases} X^2 - \bar{d} \text{ se décompose en } (X + \sqrt{\bar{d}})(X - \sqrt{\bar{d}}) \\ X^2 - \bar{d} \text{ devient } X^2 \\ X^2 - \bar{d} \text{ est irréductible} \end{cases} \Rightarrow \begin{cases} A/Ap \text{ est le produit de deux corps} \\ A/Ap \text{ a des éléments nilpotents} \\ A/Ap \text{ est un corps} \end{cases}$$

$$\Rightarrow \begin{cases} p \text{ est décomposé} \\ p \text{ est ramifié} \\ p \text{ est inerte} \end{cases} \quad (4)$$

Pour plus de clarté, on introduit le symbole de Legendre définie par :

- $\left(\frac{d}{p}\right) = 1$  si  $d$  est un carré non-nul modulo  $p$
- $\left(\frac{d}{p}\right) = 0$  si  $p$  divise  $d$
- $\left(\frac{d}{p}\right) = -1$  sinon

**Théorème 4.** Soit  $K = \mathbb{Q}[\sqrt{d}]$  une extension quadratique, soit  $p$  un nombre premier impair de  $\mathbb{Z}$  alors :

1.  $\left(\frac{d}{p}\right) = 1 \Leftrightarrow p$  est décomposé
2.  $\left(\frac{d}{p}\right) = -1 \Leftrightarrow p$  est inerte
3.  $\left(\frac{d}{p}\right) = 0 \Leftrightarrow p$  est ramifié

*Démonstration.* D'après (4) On a déjà les implications ( $\Rightarrow$ ). Soit  $\mathcal{P} \Rightarrow \mathcal{Q}$  une des implications du théorème. Si  $\mathcal{P}$  n'est pas vérifiées, c'est forcément une des deux autres qui l'est, ce qui implique par le théorème la négation de  $\mathcal{Q}$ . Donc  $\lceil \mathcal{P} \Rightarrow \rceil \mathcal{Q}$ .

Ce qui donne par contraposé :  $\mathcal{Q} \Rightarrow \mathcal{P}$ . □

On admettra les resultats suivant :

- 2 est ramifié si et seulement si  $d \equiv 2$  ou  $3[4]$
- 2 est inerte si et seulement si  $d \equiv 5[8]$
- 2 est décomposé si et seulement si  $d \equiv 1[8]$

## 2.2 Générateurs des idéaux premiers de la décomposition de $A_p$

**Lemme 1.** Soit  $I = (x_1, x_2, \dots, x_n)$  un idéal de  $A$ , l'anneau des entier de  $K$ . On a :

$$\text{pgcd}(x_i, x_j) = 1 \quad \Rightarrow \quad I = A$$

*Démonstration.* En effet :

$$\text{pgcd}(x_i, x_j) = 1 \quad \Rightarrow \quad \exists a, b \in \mathbb{Z} \text{ tels que } ax_i + bx_j = 1$$

Donc  $1 \in I$  , donc  $I = A$ . □

**Pour  $p$  inerte :**  $A_p = (p, p\sqrt{d})$ .

En effet  $A = \mathbb{Z} + \mathbb{Z}\sqrt{d} = (1, \sqrt{d})$

**Pour p décomposé :**  $Ap = (p, a + \sqrt{d})(p, a - \sqrt{d})$ , avec  $d \equiv a^2[p]$  et  $1 \leq a \leq p-1$ .

En effet  $(p, a + \sqrt{d})(p, a - \sqrt{d}) = (p^2, pa + p\sqrt{d}, pa - p\sqrt{d}, a^2 - d)$ . Or :

$$d \equiv a^2[p] \Rightarrow p \mid a^2 - d \Rightarrow \frac{a^2 - d}{p} \in \mathbb{Z}$$

Donc  $(p^2, pa + p\sqrt{d}, pa - p\sqrt{d}, a^2 - d) = Ap(p, a + \sqrt{d}, a - \sqrt{d}, \frac{a^2-d}{p})$ .

Comme  $a + \sqrt{d} + a - \sqrt{d} = 2a$ , On a :  $(p, a + \sqrt{d}, a - \sqrt{d}, \frac{a^2-d}{p}) = (p, a + \sqrt{d}, a - \sqrt{d}, \frac{a^2-d}{p}, 2a)$ , mais  $\text{pgcd}(p, 2a) = 1$  car  $p \neq 2$  et  $a < p$  d'où  $(p, a + \sqrt{d}, a - \sqrt{d}, \frac{a^2-d}{p}, 2a) = A$  et  $ApA = Ap$ .

Donc on a bien  $Ap = (p, a + \sqrt{d})(p, a - \sqrt{d})$ . Si l'un des facteurs vaut  $A$  alors l'autre aussi. En effet, si  $(p, a + \sqrt{d}) = A$ , il suffit de vérifier qu'il existe  $\alpha$  et  $\beta$  de  $\mathbb{Z}$  tel que  $\alpha p + \beta(a - \sqrt{d}) = 1$ , i.e.  $\alpha p + \beta(a + \sqrt{d}) = 1 + 2\beta\sqrt{d}$ , ce qui est évident car  $(p, a + \sqrt{d}) = A$ . Donc  $Ap$  est un produit de deux idéaux différents de  $A$ , donc ils sont premiers. La décomposition en idéaux premiers étant unique, on a bien  $Ap = P_1P_2$  avec  $P_1 = (p, a + \sqrt{d})$  et  $P_2 = (p, a - \sqrt{d})$  distincts.

**Pour p ramifié :**  $Ap = (p, \sqrt{d})^2$ .

En effet soit  $P = (p, \sqrt{d})$ ,  $P^2 = (p^2, p\sqrt{d}, d)$ . Or  $p$  ramifié équivalent à  $p$  divise  $d$ . D'où  $P^2 = Ap(p, \sqrt{d}, \frac{d}{p})$ , or comme  $d$  n'a pas de facteurs carrés,  $p$  n'apparaît qu'une seule fois dans sa décomposition en facteurs premiers, et comme  $p$  est premier on a  $\text{pgcd}(p, \frac{d}{p}) = 1$ . Donc  $P^2 = Ap(p, \sqrt{d}, \frac{d}{p}) = ApA = Ap$

**Remarque :** Si  $d \equiv 1[4]$  et  $(\frac{d}{p}) \neq -1$  alors il existe un entier  $b$ ,  $0 \leq b < p-1$ , tel que  $p$  divise  $N(b + \frac{1+\sqrt{d}}{2})$ .

En effet si  $(\frac{d}{p}) \neq -1$ , il existe un idéal premier  $P$  qui divise  $Ap$ , où  $P = (p, a + \sqrt{d})$ , avec  $0 \leq a < p-1$  (si  $(\frac{d}{p}) = 0$  alors  $a = 0$ ).

Or  $a + \sqrt{d} = a - 1 + 2\frac{1+\sqrt{d}}{2}$ . D'où :

$$(p, a + \sqrt{d}) = (p, (a-1) + 2\frac{1+\sqrt{d}}{2}) = (p, l(a-1) + \frac{1+\sqrt{d}}{2})$$

avec  $2l \equiv 1[p]$ .

$$(p, a + \sqrt{d}) = (p, l(a-1) + \frac{1+\sqrt{d}}{2}) = (p, b + \frac{1+\sqrt{d}}{2})$$

avec  $b \equiv l(a-1)[p]$ . Ainsi  $0 \leq b < p-1$  et  $A(b + \frac{1+\sqrt{d}}{2}) \subseteq P$  donc  $N(P)$  divise  $N(b + \frac{1+\sqrt{d}}{2})$ . Comme  $p$  divise  $N(P)$ , alors  $p$  divise  $N(b + \frac{1+\sqrt{d}}{2})$ .

### 3 Finitude du groupe des classes d'idéaux

#### 3.1 Théorème de Minkowski

Commençons tout d'abord à définir quelques notions, ainsi qu'un théorème que nous ne démontrerons pas.

**Définition 1.** On appelle sous-groupe discret de  $\mathbb{R}^n$ , un sous-groupe additif  $H$  de  $\mathbb{R}^n$  qui vérifie : pour tout compact  $K \subset \mathbb{R}^n$ ,  $H \cap K$  est fini.

Un exemple simple est  $\mathbb{Z}^r$  ( $r \leq n$ ).

**Théorème 5.** Soit  $H$  un sous-groupe discret de  $\mathbb{R}^n$ , alors  $H$  est engendré (comme  $\mathbb{Z}$ -module) par  $r$  vecteurs linéairement indépendants sur  $\mathbb{R}$  ( $r \leq n$ ). On dit alors que  $H$  est de rang  $r$ .

**Définition 2.** Un sous-groupe discret de  $\mathbb{R}^n$  de rang  $n$  est appelé un réseau de  $\mathbb{R}^n$ .

Nous noterons  $\mu$  la mesure de Lebesgue dans  $\mathbb{R}^n$ . Ainsi pour toute partie intégrable  $S$  de  $\mathbb{R}^n$ ,  $\mu(S)$  désigne son volume.

Soit  $H$  un réseau de  $\mathbb{R}^n$  de base  $e = (e_1, e_2, \dots, e_n)$ , alors tout point  $x$  de  $\mathbb{R}^n$  s'écrit

$$\begin{aligned}x &= \sum_{i=1}^n \lambda_i e_i \quad \text{avec } \lambda_i \in \mathbb{R} \\ \Rightarrow x &= \sum_{i=1}^n [\lambda_i] e_i + \sum_{i=1}^n (\lambda_i - [\lambda_i]) e_i \quad \text{avec } \lambda_i \in \mathbb{R} \\ \Rightarrow x &= h + \sum_{i=1}^n \alpha_i e_i \quad \text{avec } 0 \leq \alpha_i < 1 \text{ et } h \in H\end{aligned}$$

On définit  $P_e$  le parallélotope semi-ouvert :

$$P_e = \left\{ \sum_{i=1}^n \alpha_i e_i \mid 0 \leq \alpha_i < 1 \right\}$$

Ainsi :

$$\Rightarrow x = h + x_0 \quad \text{avec } x_0 \in P_e \text{ et } h \in H$$

On dit que  $P_e$  est un domaine fondamental pour  $H$  car tout point de  $\mathbb{R}^n$  est congru modulo  $H$  à un unique point de  $P_e$ .

On en déduit :

$$\mathbb{R}^n \text{ est la réunion disjointe des } h + P_e (h \in H) \quad (5)$$

**Lemme 2.** *Le volume  $\mu(P_e)$  est indépendant de la base  $e$  choisie pour  $H$ .*

Ainsi  $\mu(P_e)$  est appelé volume du réseau  $H$ .

On rappelle que comme  $\mu$  est une mesure, pour  $I$  et  $J$  deux ensembles intégrables de  $\mathbb{R}^n$  on a :

$$I \cap J = \emptyset \quad \Rightarrow \quad \mu(I \cup J) = \mu(I) + \mu(J)$$

**Théorème 6.** (Minkowski). *Soit  $H$  un réseau de  $\mathbb{R}^n$  et  $S$  un sous-ensemble intégrable de  $\mathbb{R}^n$  tels que  $\mu(S) > v(H)$ . Alors il existe deux éléments  $x, y \in S$  distincts tels que  $x - y \in H$ .*

*Démonstration.* Soit  $e = (e_1, e_2, \dots, e_n)$  une  $\mathbb{Z}$ -Base de  $H$  et  $P_e$  le parallétope semi-ouvert défini précédemment.

On déduit de (5) que  $S$  est la réunion disjointe des  $S \cap (h + P_e)$  ( $h \in H$ )  
D'où :

$$\mu(S) = \sum_{h \in H} \mu(S \cap (h + P_e))$$

Or  $\mu$  est invariante par translation donc on a :

$$\mu(S \cap (h + P_e)) = \mu((S - h) \cap P_e)$$

Donc :

$$\mu(S) = \sum_{h \in H} \mu((S - h) \cap P_e)$$

Or chaque ensemble  $(S - h) \cap P_e$  est contenu dans  $P_e$ , donc sa réunion aussi,  
d'où :

$$\mu(\cup_{h \in H} ((S - h) \cap P_e)) \leq \mu(P_e)$$

Donc si les ensembles  $(S - h) \cap P_e$  sont deux à deux disjoints on a la contradiction suivante :

$$\mu(H) = \mu(P_e) < \mu(S) = \sum_{h \in H} \mu((S - h) \cap P_e) = \mu(\cup_{h \in H} ((S - h) \cap P_e)) \leq \mu(P_e)$$

Donc les ensembles  $(S - h) \cap P_e$  ne sont pas deux à deux disjoints, donc il existe  $h$  et  $h'$  distincts de  $H$  tels que  $(S - h) \cap (S - h') \cap P_e \neq \emptyset$ . On a donc deux éléments  $x$  et  $y$  de  $S$  tels que :

$$x - h = y - h' \Leftrightarrow x - y = h - h' \in H$$

Avec  $x \neq y$  car  $h \neq h'$  . □

**Lemme 3.** Soit  $H$  un réseau de  $\mathbb{R}^n$  et  $S$  une partie intégrable, symétrique par rapport à 0 et convexe de  $\mathbb{R}^n$  tels que  $\mu(S) > 2^n v(H)$ . Alors  $H \cap S$  contient un point autre que 0.

*Démonstration.* Soit  $S' = \frac{1}{2}S$ . On a  $\mu(S') = \frac{1}{2^n}\mu(S)$  car on se trouve dans  $\mathbb{R}^n$ .

Donc  $\mu(S') > v(H)$ . On applique donc le théorème 1 à  $S'$ . Alors il existe  $x$  et  $y$  distincts de  $S'$  tels que  $x - y \in H$ . D'où  $h = x - y = \frac{1}{2}(2x - 2y)$  est un point de  $S$ , car  $S$  est symétrique et convexe, qui réponds à la question.  $\square$

**Corollaire 1.** Soit  $H$  un réseau de  $\mathbb{R}^n$  et  $S$  une partie intégrable, compact, symétrique par rapport à 0 et convexe de  $\mathbb{R}^n$  tels que  $\mu(S) \geq 2^n v(H)$ . Alors  $H \cap S$  contient un point autre que 0.

*Démonstration.* On pose  $S_\epsilon = (1 + \epsilon)S$ . On a bien  $\mu(S_\epsilon) > \mu(S) \geq 2^n v(H)$  donc on applique le Lemme 3 à  $S_\epsilon$ .

On pose  $H' = H - \{0\}$  donc  $H' \cap S_\epsilon$  est non-vidé, compact et discret. Donc  $\cap_{\epsilon>0}(H' \cap S_\epsilon)$  est aussi non-vidé.

Soit  $h \in \cap_{\epsilon>0}(H' \cap S_\epsilon)$ ,  $h \neq 0$ ,  $h \in H$  et  $h \in \cap_{\epsilon>0}S_\epsilon = S$  car  $S$  est compact donc  $h$  réponds à la question.  $\square$

## 3.2 Plongement canonique d'un corps quadratique

Soit  $K = \mathbb{Q}[\sqrt{d}]$  ( $d$  sans facteur premier), le polynôme minimal de  $x$  dans  $K$  sur  $\mathbb{Q}$  à exactement deux racines distinctes,  $x_1$  et  $x_2$ , dans  $\mathbb{C}$ , donc on peut définir deux isomorphismes distincts  $\sigma_1$  et  $\sigma_2$  définis par  $\sigma_1(x) = x_1$  et  $\sigma_2(x) = x_2$ .

D'où :

$$\sigma_1 = \text{identité et } \sigma_2(x) = \bar{x}$$

avec pour  $x = a + b\sqrt{d}$ ,  $\bar{x} = a - \sqrt{d}$  (ce qui étend la notion de conjugué de  $\mathbb{C}$  à  $\mathbb{R}$ )

Soit  $\alpha : \mathbb{C} \rightarrow \mathbb{C}$  le passage au nombre complexe conjugué. On a :

$$\alpha \circ \sigma_i = \sigma_j \quad \text{avec } (i = j \Leftrightarrow \sigma_i \subset \mathbb{R})$$

Si  $R$  est l'ensemble des isomorphismes  $\sigma_i$  qui vérifie  $\sigma_i \subset \mathbb{R}$ , on note  $r_1$  son cardinal. Si  $r$  est le nombre d'isomorphisme  $\sigma_i$  qui ne sont pas dans  $R$  alors  $r$  est pair. En effet soit  $\sigma_i \notin R$  avec  $\alpha \circ \sigma_i = \sigma_j$ ,  $i \neq j$ , alors comme  $\alpha \circ \sigma_j = \sigma_i$  on a bien  $\sigma_j \notin R$ . On note  $r_2 = \frac{1}{2}r$ .

On a  $r_1 + 2r_2 = 2$ , ce qui donne deux cas possible : le cas d'une extension imaginaire (i.e.  $d < 0$ ), où  $r_1 = 0$  et  $r_2 = 1$ , et le cas réel (i.e.  $d > 0$ ), où  $r_1 = 2$  et  $r_2 = 0$ .

Ainsi on définit  $\sigma$  de la façon suivante :

– Dans le cas réel :

$$\sigma(x) = (\sigma_1(x), \sigma_2(x)) \in \mathbb{R}^2$$

– Dans le cas imaginaire :

$$\sigma(x) = (\sigma_1(x)) \in \mathbb{C}$$

Qu'on identifiera souvent à :

$$\sigma(x) = (\operatorname{Re}(\sigma_1(x)), \operatorname{Im}(\sigma_1(x))) \in \mathbb{R}^2$$

Où  $\operatorname{Re}$  et  $\operatorname{Im}$  désignent la partie réelle et la partie imaginaire.

Nous appellerons  $\sigma$  le plongement canonique de  $K$  dans  $\mathbb{R}^2$ .

**Proposition 1.** Soient  $\delta$  le discriminant absolu de  $K$ ,  $A$  son anneau des entiers, et  $I$  un idéal entier non nul de  $A$ . Alors  $\sigma(A)$  et  $\sigma(I)$  sont des réseaux de  $\mathbb{R}^2$  et on a :  $v(\sigma(A)) = 2^{-r_2} |\delta|^{1/2}$  et  $v(\sigma(I)) = 2^{-r_2} |\delta|^{1/2} N(I)$

*Démonstration.* Soit  $\alpha = (\alpha_1, \alpha_2)$  une base de  $A$ . La matrice dans les bases  $\alpha$  et canonique de  $\mathbb{R}^2$  a donc un déterminant :

$$D = \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) \end{pmatrix}$$

**Dans le cas réel :** On choisissant la numérotation des  $\sigma_i$  on a  $\sigma_1 = \text{Identité}$  et  $\sigma_2(x) = \bar{x}$  pour tout  $x \in K$ . on a donc :

– Pour  $d \equiv 2$  ou  $3[4]$ ,  $\alpha = (1, \sqrt{d})$  et  $\delta = 4d$  :

$$D = \pm(\sqrt{d} + \sqrt{d}) = \pm\sqrt{4d} = \pm\sqrt{\delta}$$

– Pour  $d \equiv 1[4]$ ,  $\alpha = (1, \frac{1+\sqrt{d}}{2})$  et  $\delta = d$  :

$$D = \pm \left( \frac{1 + \sqrt{d}}{2} + \frac{-1 + \sqrt{d}}{2} \right) = \pm\sqrt{d} = \pm\sqrt{\delta}$$

D'où  $v(\sigma(A)) = |D| = \sqrt{\delta}$

**Dans le cas imaginaire :** On a  $(\sigma_1(x), \sigma_2(x)) = (\operatorname{Re}(x), \operatorname{Im}(x))$ . Donc :

– Pour  $d \equiv 2$  ou  $3[4]$ ,  $\alpha = (1, \sqrt{d})$  et  $\delta = 4d$  :

$$D = 1 \times \sqrt{d} = \frac{i\sqrt{|4d|}}{2} = \frac{i\sqrt{|\delta|}}{2}$$

– Pour  $d \equiv 1[4]$ ,  $\alpha = (1, \frac{1+\sqrt{d}}{2})$  et  $\delta = d$  :

$$D = 1 \times \frac{\sqrt{d}}{2} = \frac{i\sqrt{|\delta|}}{2}$$

D'où  $v(\sigma(A)) = |D| = \frac{1}{2}\sqrt{|\delta|}$

D'où dans le cas général :  $v(\sigma(A)) = 2^{-r_2} |\delta|^{1/2}$

L'égalité  $v(\sigma(I)) = 2^{-r_2} |\delta|^{1/2} N(I)$  se déduit du fait que la norme  $N(I) = \text{card}(A/I)$  est l'indice de  $I$  dans  $A$  et que donc si  $(i_1, i_2)$  est une base de  $I$  on a :

$$\det \begin{pmatrix} \sigma_1(i_1) & \sigma_1(i_2) \\ \sigma_2(i_1) & \sigma_2(i_2) \end{pmatrix} = N(I) \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) \end{pmatrix}$$

□

### Définition de $B_t$

On définit  $B_t$  l'ensemble des

$$(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

tels que :

$$\sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t$$

Il est clair que  $B_t$  définit un ensemble convexe, compact et symétrique par rapport à 0.

Dans le cas réel  $B_t = \{(y_1, y_2) \in \mathbb{R}^2 \text{ tq. } |y_1| + |y_2| \leq t\}$ . D'où le volume de  $B_t$  est l'aire du carré de côté  $t\sqrt{2}$ . Donc :

$$\mu(B_t) = 2t^2$$

Dans le cas imaginaire  $B_t = \{z = a + ib \in \mathbb{C} \text{ tq. } \sqrt{a^2 + b^2} \leq t\}$ . D'où le volume de  $B_t$  est l'aire du disque de rayon  $t$ . Donc :

$$\mu(B_t) = \frac{\pi}{4} t^2$$

Ce qui donne dans le cas général :

$$\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{1}{2} t^2$$

## 3.3 Théorème de Dirichlet

**Proposition 2.** Soient  $K$  un corps quadratique,  $r_1$  et  $r_2$  les entiers définis au début du paragraphe 2,  $\delta$  son discriminant absolu, et  $I$  un idéal entier non nul de  $K$ . Alors  $I$  contient un élément non nul  $x$  tel que

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{1}{2} |\delta|^{1/2} N(I) \quad (6)$$

*Démonstration.* Soit  $\sigma$  le plongement canonique de  $K$  dans  $\mathbb{R}^2$  (ou  $\mathbb{C}$  identifié à  $\mathbb{R}^2$  dans le cas imaginaire).

Choisissons  $t$  tel que  $\mu(B_t) = 2^2 v(\sigma(I))$ , c'est à dire :

$$2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{1}{2} t^2 = 2^{-r_2} |\delta|^{1/2} N(I)$$

$$t^2 = 2^{1-r_2-r_1} \left(\frac{2}{\pi}\right)^{r_2} |\delta|^{1/2} N(I)$$

$$t^2 = 2 \left(\frac{4}{\pi}\right)^{r_2} |\delta|^{1/2} N(I)$$

D'après le Corollaire 1, il existe un élément  $x \in I$  non nul, tel que  $\sigma(x) \in B_t$ . Étudions la norme de  $x$

– Dans le cas réel :  $N(x) = x\bar{x} = \sigma_1(x)\sigma_2(x)$ .

Or :

$$\sigma_1(x)\sigma_2(x) = \frac{1}{4} \left( (\sigma_1(x) + \sigma_2(x))^2 - (\sigma_1(x) - \sigma_2(x))^2 \right)$$

$$\Rightarrow N(x) \leq \frac{1}{4} (\sigma_1(x) + \sigma_2(x))^2 \leq \frac{1}{4} t^2$$

car  $\sigma(x) \in B_t$

– Dans le cas imaginaire :  $N(x) = |\sigma_1(x)|^2$ . Or :

$$2 |\sigma_1(x)| \leq t$$

car  $\sigma(x) \in B_t$

$$\Rightarrow N(x) = |\sigma_1(x)|^2 \leq \frac{t^2}{4}$$

Ce qui donne dans le cas général :

$$N(x) \leq \frac{t^2}{4} = \left(\frac{4}{\pi}\right)^{r_2} \frac{1}{2} |\delta|^{1/2} N(I)$$

□

**Corollaire 2.** Avec les mêmes notations, toute classe d'idéaux de  $K$  contient un idéal entier  $J$  tel que

$$N(J) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{1}{2} |d|^{1/2}$$

*Démonstration.* Soit  $I$  un idéal entier de la classe donnée. D'après la Proposition 2, il existe  $x \in I$  vérifiant (6). De plus l'idéal  $xI^{-1}$  est entier. En effet :

$$\begin{aligned} (I^{-1})^{-1} &= \{x \in K \mid xI^{-1} \subset A\} \\ \Leftrightarrow I &= \{x \in K \mid xI^{-1} \text{ soit entier} \} \\ \Rightarrow x \in I, & \quad xI^{-1} \text{ est entier} \end{aligned}$$

On pose donc  $J = xI^{-1}$  de la même classe que  $I$ . On a bien  $N(I^{-1}) = \frac{1}{N(I)}$  (car  $N(A) = N(I)N(I^{-1})$ ).

Donc :

$$N(J) = N(x)N(I^{-1}) = \frac{N(x)}{N(I)} \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{1}{2} |d|^{1/2}$$

□

**Téorème 7.** *Pour tout corps quadratique  $K$ , le groupe des classes d'idéaux de  $K$  est fini.*

*Démonstration.* En effet, on a vu qu'il existe un entier  $\theta$  tel que chaque classe contient un idéal entier  $I$  de norme borné par  $\theta$ . Il suffit donc de montrer que le nombre d'idéaux entier de norme borné par  $\theta$  est fini, ou encore que le nombre d'idéaux entier donc la norme est un entier donnée  $q$  est fini.

Soit  $I$  un tel idéal. D'après la définition,  $q = \text{card}(A/I)$  et comme dans un groupe, l'ordre d'un élément divise l'ordre du groupe, alors  $cl(q) = cl(q \times 1) = q \times cl(1) = cl(0) = I$ , donc  $q \in I$ . Donc  $I$  contient  $Aq$  avec  $Aq = P_1^{\alpha_1} \dots P_r^{\alpha_r}$  dans la décomposition en nombre premier. Or il y a un nombre fini d'idéaux qui contiennent  $Aq$  car si  $Aq \subset I$ , alors il existe  $J$  tel que  $Aq = IJ$  avec comme décomposition possible pour  $I$  en idéaux premiers :

$$I = P_1^{\alpha'_1} \dots P_r^{\alpha'_r} \quad \text{avec} \quad \begin{array}{l} \alpha'_1 \leq \alpha_1 \\ \vdots \\ \alpha'_r \leq \alpha_r \end{array}$$

Ce qui laisse un nombre fini de possibilités.

Donc le nombre de classe est fini. □

**Définition 3.** *Un idéal  $I$  est dit normalisé si*

$$N(I) \leq [\theta]$$

avec

$$\theta = \left(\frac{4}{\pi}\right)^{r_2} \frac{1}{2} |d|^{1/2} = \begin{cases} \frac{1}{2} |d|^{1/2} & \text{pour } d > 0 \\ \frac{2}{\pi} |d|^{1/2} & \text{pour } d < 0 \end{cases}$$

On utilisera  $\theta$  ainsi définie jusqu'à la fin du dossier.

## 4 Calcul du nombre de classes

### 4.1 Idéaux primitifs du groupe des classes

**Définition 4.** Un idéal  $I$  est appelé primitif s'il n'existe pas de nombre premier  $p$  tel que  $Ap$  divise  $I$ . On note  $\mathcal{P}$  l'ensemble des idéaux normalisés primitifs.

Soit  $I \in \mathcal{P}$  on a :

$$N(I) = \prod_{r \text{ ramifié}} r \prod_{p \text{ décomposé}} p^{e(p)}$$

En effet pour tout  $p$  premier,  $Ap$  ne divise pas  $I$  donc  $I \not\subseteq Ap$  donc  $Ap$  ne doit pas apparaître dans la décomposition de  $I$  en idéaux premiers.

Donc si  $p$  est inerte alors  $Ap$  n'apparaît pas, donc  $p$  ne divise pas  $N(I)$ . Si  $p$  est ramifié,  $Ap = P^2$  n'apparaît pas donc si  $p$  divise  $N(I)$  i.e  $I \subset P$  alors comme  $I \not\subseteq Ap = P^2$  alors  $p^2$  ne divise pas  $N(I)$ . Si  $p$  est décomposé alors  $Ap = P_1P_2$  n'apparaît pas donc si  $I \subset P_1$  alors  $I \not\subseteq P_2$ , donc  $I \in P_1^{e(p)}$ .

Montrons que chaque classe d'idéaux contient un idéal normalisé primitif. En effet on sait déjà que chaque classe contient un idéal normalisé  $I$ . Or si  $I$  n'est pas primitif, il existe un idéal  $J$  dans la même classe tel que  $I = ApJ$  avec  $N(J) \leq \frac{1}{p}N(I)$  donc par récurrence on peut démontrer qu'il existe  $p_1, p_2 \dots p_r$  et un idéal  $K$  tels que  $I = Ap_1Ap_2 \dots Ap_rK$  avec  $K$  primitif,  $K$  est dans la même classe que  $I$  et  $N(K) < N(I)$  donc  $K$  est normalisé. Cela prouve une fois de plus que le nombre de classe est fini.

Dans la suite on note  $N(\mathcal{P})$  l'ensemble des  $N(I)$  avec  $I \in \mathcal{P}$  et  $h$  le nombre de classes.

**Théorème 8.** Soient  $m \in \mathbb{Z}$  et

$$\alpha = \begin{cases} u + v\sqrt{d} & \text{avec } u, v \in \mathbb{Z} & \text{si } d \equiv 2 \text{ ou } 3[4] \\ u + v\sqrt{d} & \text{avec } u, v \in \mathbb{Z}, u \equiv v[2] & \text{si } d \equiv 1[4] \end{cases}$$

Alors,  $A\alpha$  est primitif avec  $N(A\alpha) = m$  si et seulement si :

$$\begin{cases} m = |u^2 - dv^2|, \text{pgcd}(u, v) = 1 & \text{si } d \equiv 2 \text{ ou } 3[4] \\ m = \frac{|u^2 - dv^2|}{4}, \text{pgcd}(\frac{u-v}{2}, v) = 1 & \text{si } d \equiv 1[4] \end{cases}$$

On appelle cette écriture de  $m$  la représentation primitive de  $m$ .

## 4.2 Premiers calculs

On remarque que pour tout  $I \in \mathcal{P}$ ,  $N(I) = 1$ , i.e.  $N(\mathcal{P}) = \{1\}$ ,  $\mathcal{P}$  est réduit à  $A$  alors  $h = 1$ . On déduit de cela que pour  $[\theta] = 1$  alors  $h = 1$ .

Dans le cas réel  $\theta = \frac{1}{2}\sqrt{\delta}$ , d'où :

$$1 \leq \frac{1}{2}\sqrt{\delta} < 2 \quad \Leftrightarrow \quad 4 \leq \delta < 16$$

avec  $\delta \equiv 0$  ou  $1[4]$ , donc  $\delta \in \{4, 5, 8, 9, 12, 13\}$ . 4 et 9 ne correspondent pas à une extension quadratique. Pour  $\delta = 8$  on a bien  $d = 2 \equiv 2[4]$  avec donc  $\delta = 4d$ . De même pour  $\delta = 12$  où  $d = 3$ . Pour  $\delta = 5$  on a bien  $d = 5 \equiv 1[4]$  avec donc  $\delta = d$ . De même pour  $\delta = 13$  où  $d = 13$ .

Donc pour  $d \in \{2, 3, 5, 13\}$ ,  $h = 1$ .

Dans le cas imaginaire,  $\delta < 0$ ,  $\theta = \frac{2}{\pi}\sqrt{\delta}$ , d'où :

$$-\frac{\pi^2}{4} \geq \delta > -\pi^2$$

avec  $\delta \equiv 0$  ou  $1[4]$ , donc  $\delta \in \{-3, -4, -7, -8\}$ . Pour  $\delta = -4$  on a bien  $d = -1 \equiv 3[4]$  avec  $d = 4\delta$ . De même pour  $\delta = -8$  où  $d = -2$ . Pour  $\delta = -3$  on a bien  $d = -3 \equiv 1[4]$  avec  $d = \delta$ . De même pour  $d = \delta = -7$ .

Donc pour  $d \in \{-1, -2, -3, -7\}$ ,  $h = 1$ .

**Lemme 4.** *Si pour tout  $p \leq [\theta]$ ,  $p$  est inerte, alors  $h = 1$*

*Démonstration.* En effet si pour tout  $p \leq [\theta]$ ,  $p$  est inerte, alors quel que soit  $I \in \mathcal{P}$  on a :

$$N(I) < [\theta] \Rightarrow \prod_{r \text{ ramifié}} r \prod_{p \text{ décomposé}} p^{e(p)} \leq [\theta]$$

or si  $r$  ramifié ou décomposé alors  $r > [\theta]$  donc  $N(I) = 1$ , donc  $h = 1$

□

**Recherche de tout les corps quadratiques imaginaires de nombre de classe  $h = 1$ .**

Le Théorème 8 et le Lemme 4 vont nous aider pour le calcul de  $h$ . Notamment en vérifiant si les nombres premiers inférieurs à  $\theta$  sont inertes ou si les entiers inférieurs à  $\theta$  ont une écriture primitive. Étudions la méthode sur l'exemple suivant :

**Prenons**  $[\theta] = 2$

On a  $\delta < 0$  et  $\theta = \frac{2}{\pi}\sqrt{\delta}$ , soit :

$$2 \leq \frac{2}{\pi}\sqrt{\delta} < 3$$

$$-\pi^2 \geq \delta > -\frac{9}{4}\pi^2$$

avec  $\delta \equiv 0$  ou  $3[4]$ , donc  $\delta \in \{-11, -12, -15, -16, -19, -20\}$ . Pour  $\delta = -11$  on a bien  $d = -11 \equiv 1[4]$  avec donc  $\delta = d$ . De même pour  $\delta = -15$  où  $d = -15$  et  $\delta = -19$  où  $d = -19$ . Pour  $\delta = -20$  on a bien  $d = -5 \equiv 3[4]$  avec  $\delta = 4d$ .

Donc  $d \in \{-5, -11, -15, -19\}$ .

Regardons le calcul de  $h$  pour les deux cas suivants :

- Pour  $d = -11$ . Comme  $-11 \equiv 5[8]$  alors 2 est inerte et donc  $h = 1$ .
- Pour  $d = -5$ . Comme  $-5 \equiv 3[8]$  alors 2 est ramifié, donc  $A2 = P^2$ . Or 2 n'a pas d'écriture primitive. En effet sinon  $2 = |u^2 + 5v^2|$  (car  $d = -5 \equiv 3[4]$ ) d'où  $u^2 = -5v^2 + 2$ , or  $-5v^2 + 2 \equiv 2[5]$  donc  $u^2 \equiv 2[5]$  ce qui est impossible.

Donc il n'existe pas d'idéal principal primitif de norme 2. Comme  $N(A2) = 4 = N(P)^2$ , alors  $N(P) = 2$  et donc  $P$  n'est pas principal donc  $h = 2$ .

Les travaux de Gauss ajoutent un critère pour exclure certains corps quadratiques de la liste des corps quadratiques imaginaires de nombre de classe  $h = 1$ . Cela permet, en allant jusqu'à  $[\theta] = 8$ , de trouver une liste de 6 corps quadratiques imaginaires de nombre de classe  $h = 1$  (pour  $d = -7, -11, -19, -43, -67, -163$ ). Il a été démontré qu'il n'en n'existe aucun autre, notamment grâce aux travaux de Heck, Deuring, Mordell et Heilbronn.

## 5 Théorème Final

**Théorème 9.** *Soit  $q$  un nombre premier et  $f_q(X) = X^2 + X + q$ . Les conditions suivantes sont équivalentes :*

- (1)  $q = 2, 3, 5, 11, 17, 41$ .
- (2)  $f_q(n)$  est un nombre premier pour  $n = 0, 1, 2 \dots q - 2$ .
- (3)  $\mathbb{Q}(\sqrt{1 - 4q})$  a un nombre de classe  $h = 1$ .

*Démonstration.* L'implication  $1 \Rightarrow 2$  est une simple vérification.

Les équivalences entre 2 et 3 ont été démontrées pour la première fois par Rabinovitch en 1912.  $2 \Rightarrow 3$  fut démontrée une fois de plus en 1936 par

Lehmer. En 1974, Szekeres donna une nouvelle preuve de  $3 \Rightarrow 2$  ainsi que Ayoub et Chowla en 1981 qui donnèrent la preuve la plus simple.

L'implication  $3 \Rightarrow 1$  est une conséquence de la détermination de tous les corps quadratiques imaginaires de nombre de classe  $h = 1$ .

$2 \Rightarrow 3$  :

Soit  $d = 1 - 4q < 0$ , donc  $d \equiv 1[4]$ . On peut supposer que  $q \neq 2$  et  $q \neq 3$ , car dans ce cas  $d = -7$  ou  $-11$ , et on a déjà vérifié que  $h = 1$ . On suppose donc  $p \geq 5$ .

Pour prouver que  $h = 1$ , il suffit de montrer que tout nombre premier  $p \leq \frac{2}{\pi} \sqrt{|d|}$  est inerte.

$q$  est premier donc  $q = 2t - 1$  avec  $t \in \mathbb{N}$ , donc  $d = 1 - 4q = 1 - 4(2t - 1) = -8t + 5 \equiv 5[8]$ , donc  $2$  est inerte.

Soit  $p \leq \frac{2}{\pi} \sqrt{|d|} < \sqrt{|d|}$ . Supposons que  $p$  n'est pas inerte.

Alors  $\left(\frac{d}{p}\right) \neq -1$  donc il existe  $b \in \mathbb{N}$ ,  $0 \leq b \leq p - 1$  tel que  $p$  divise  $N(b + \frac{1+\sqrt{d}}{2})$  (Remarque section 2.2) d'où  $p$  divise :

$$\begin{aligned} (b + \frac{1+\sqrt{d}}{2})(b + \frac{1-\sqrt{d}}{2}) &= b^2 + b + \frac{1-d}{4} \\ &= b^2 + b + q = f_q(b) \end{aligned}$$

Notons que  $b \neq p - 1$ , en effet sinon  $p$  divise  $(p-1)^2 + p - 1 + q = p^2 + 3p + q$ , donc  $p$  divise  $q$  donc  $p = q < \sqrt{|d|} = \sqrt{|1 - 4q|}$ , donc  $q^2 < 4q - 1$ , soit  $q = 2$  ou  $3$ , ce qui contredit les hypothèses.

Donc  $f_q(b)$  est un nombre premier par hypothèse, donc comme  $p$  divise  $f_q(b)$  alors  $p = f_q(b)$ . D'où :

$$\begin{aligned} \sqrt{1 - 4q} > p = f_q(b) &\geq f_q(0) = q \\ 1 - 4q > q^2 \end{aligned}$$

Implique une fois de plus  $q = 2$  ou  $3$ , ce qui contredit les hypothèses.

Donc  $p$  est inerte et donc  $h = 1$

$3 \Rightarrow 1$  :

Avec  $d = 1 - 4q$ , si  $\mathbb{Q}(\sqrt{d})$  a un nombre de classe  $h = 1$  alors  $d = -7, -11, -19, -43, -67, -163$  équivalent à  $q = 2, 3, 5, 11, 17, 41$   $\square$

## Références

- [1] P.RIBENBOIM *Euler's famous prime generating polynomial and the class number of imaginary quadratic fields.*
- [2] P.SAMUEL *Théorie algébrique des nombres.*
- [3] L.N.STEWART and D.O.TALL *Algebraic number theory.*