Sur les polynômes d'Euler générant des nombres premiers

Écrit par

Julien MOLINA

Sous la direction de Maria CARRIZOSA

Mémoire dans le cadre de l'UE d'initiation à la recherche, à l'université Claude Bernard Lyon 1

Semestre de printemps 2018

Table des matières

Introduction

L'intérêt des nombres premiers dans toute l'histoire des mathématiques est indéniable. De nombreuses questions sont donc apparues sur eux. Cela dit, rappelons ce qu'est un nombre premier :

Définition 1
Soit A un anneau et p un élément de A non nul.
On dit que p est ***premier*** *s'il n'est pas inversible et si l'idéal engendré par p dans A, (p), est premier. Autrement dit, si p divise un produit ab, avec $a, b \in A$, alors p divise a ou p divise b.*

Une des questions qui va nous intéresser est : est-ce qu'un polynôme à coefficients entiers non constant, évalué sur $\mathbb{N}$, peut ne donner que des valeurs premières ? Cette question se révélera vaine comme le montre le théorème suivant :

Théorème 1
Soit $f \in \mathbb{Z}[X]$, avec $\deg(f) > 0$. Alors il existe une infinité d'entiers n tels que $f(n)$ n'est pas un nombre premier.

Démonstration : Supposons qu'il existe $n_0 \geqslant 1$ tel que $f(n_0) = p$ un nombre premier. Puisque $\lim_{n \to +\infty} |f(n)| = +\infty$, il existe $n_1 \geqslant 1$, tel que si $n \geqslant n_1$ alors $|f(n)| > p$. Prenons h tel que $n_0 + ph \geqslant n_1$, ce qui est possible puisque $\mathbb{R}$ est archimédien. Alors $|f(n_0 + ph)| > p$, mais $f(n_0 + ph) = f(n_0) + pk = pk', k, k' \in \mathbb{Z}$. Donc $f(n_0 + ph)$ est composé. □

Cette question étant résolue, nous allons donc réduire un peu nos attentes. Nous allons plutôt nous intéresser à la question suivante : est-ce qu'un polynôme non constant à coefficients entiers admet toujours au moins une valeur première. Cette question possède diverses réponses.

Pour les polynômes de degré 1, le résultat est déjà réglé et connu sous le nom du théorème de la progression arithmétique de Dirichlet.

Théorème 2 (Progression arithmétique de Dirichlet)
Soit $a, b \in \mathbb{N}^*$ des entiers premiers entre eux. Alors il existe une infinité de nombres premiers de la forme $a + bn$, où n parcourt $\mathbb{N}$.

Le cas où a et b ne sont pas premiers entre eux n'est pas traité puisqu'il y aura toujours des termes en commun : en effet, pour $c, d \in \mathbb{N}$, $c + nd = PGCD(c, d)(c' + nd')$ et donc $c + nd$ sera toujours composé. Intéressons-nous donc maintenant aux polynômes du second degré. Par des petites manipulations arithmétiques, il peut être assez facile de montrer qu'un polynôme de degré deux possède au moins une valeur première ou non. Mais alors, une autre question intéressante est de s'intéresser aux valeurs premières consécutives. Cette question sera l'objet principal de ce mémoire.

Euler avait trouvé que le polynôme $P_e(X) = X^2 + X + 41$, évalué en $0, 1, \cdots, 39$, n'avait que des valeurs premières. Regardons alors les polynômes de la forme $X^2 + X + q$, où q est un nombre premier. Nous aboutissons donc sur le théorème de notre mémoire :

Théorème 3
Soit q un nombre premier et soit le polynôme suivant $P_q(X) = X^2 + X + q$. Les assertions suivantes sont équivalentes :

(i) $q = 2, 3, 5, 11, 17, 41$

(ii) $P_q(n)$ *est premier pour* $n \in \{0, 1, \cdots, q - 2\}$

Pour démontrer ce théorème, nous allons devoir introduire toute une théorie plus complexe mais fondamentale en théorie des nombres et des anneaux.

Cela dit, on peut démontrer ce résultat avec des outils plus élémentaires de la théorie des anneaux. Nous allons procéder à ce cheminement pour le polynôme $P_e(X) = X^2 + X + 41$; ce qui nous permettra de mieux comprendre, implicitement, pourquoi nous allons introduire toute cette théorie.

Pour ce faire, nous allons procéder en plusieurs étapes.

(i) **Se placer dans l'anneau adéquat** : Comme souvent en arithmétique, il est utile de chercher à factoriser les expressions algébriques. Dans notre cas, P_e n'a pas de racines réelles, nous allons donc le factoriser dans $\mathbb{C}$:

$$P_e(X) = X^2 + X + 41 = (X + \frac{1}{2} + i\frac{\sqrt{163}}{2})(X + \frac{1}{2} - i\frac{\sqrt{163}}{2}) = (X + \alpha)(X + \overline{\alpha})$$

où nous posons $\alpha := \frac{1+i\sqrt{163}}{2}$. Nous sommes donc amenés à travailler dans l'anneau suivant $A := \mathbb{Z}[\alpha]$.

(ii) **De l'usage de la divisibilité** : Nous allons, ici, donner une démonstration du théorème en question : $P_e(n)$ est premier pour $n \in \{0, 1, \cdots, 39\}$. Nous verrons qu'en l'espèce, deux points seront tout à fait contestables. Mais nous corrigerons le tir dans les paragraphes à venir.

Commençons la démonstration : Supposons par l'absurde que $P_e(n)$ n'est pas premier. En vertu du crible d'Eratosthène, $P_e(n)$ admet un diviseur premier $p < \sqrt{P_e(n)}$. Précisément, pour $n < 40$, nous avons : $p^2 < n^2 + n + 41 < 40^2 + 40 + 41 = 41^2$. Donc $p < 41$. Travaillons maintenant dans $A = \mathbb{Z}[\alpha]$ comme si nous étions dans $\mathbb{Z}$, sans craintes. La factorisation faite précédemment nous montre que p divise $(n + \alpha)(n + \overline{\alpha})$. MAIS, sous les hypothèses, fortes et, à l'heure actuelle, très discutables, que p perdure premier dans A et que le lemme d'Euclide est toujours valable dans A, on a que p divise $n + \alpha$ ou p divise $n + \overline{\alpha}$ dans A. En supposant que $p \mid n + \alpha$, on a que $n + \alpha = p(x + \alpha y)$ avec $x, y \in \mathbb{Z}$. En identifiant les coefficients, nous obtenons que $1 = py$, ce qui est absurde puisque p est premier dans $\mathbb{Z}$.

(iii) **La notion d'irréductibilité** : Comme nous l'avons vu, la preuve précédente présuppose deux points peu banals : la persistance de p comme élément premier dans A et l'existence ou non du lemme d'Euclide dans cet anneau. Nous allons d'abord rappeler la définition d'un objet fondamental dans la théorie des anneaux et qui généralise la notion de primalité :

Définition 2
Soit R un anneau intègre et x un élément non-inversible de R.
*On dit que x est **irréductible** dans R si pour $z, t \in R$ tel que $x = zt$ alors z ou t est inversible dans R.*

$\longrightarrow$ Faisons un petit aparté sur la norme N : pour $z = a + \alpha b$ avec $a, b \in \mathbb{Z}$, on définit :

$$N(z) := z\overline{z} = a^2 + ab + 41b^2$$

Rapidement, nous remarquons que $N(z)$ est un entier positif et surtout que $N(zw) = N(z)N(w)$ pour $z, w \in \mathbb{Z}[\alpha]$; et si b est non nul, $N(z) \geqslant 41$. Notons deux points supplémentaires :

Proposition 1
- *Un nombre $z \in A$ est inversible si et seulement si il est de norme* 1.
- *Un nombre premier p de $\mathbb{N}$ est réductible dans A si et seulement si c'est une norme.*

Démonstration : • Si z est de norme 1, alors $N(z) = z\overline{z} = 1$. Donc z est inversible d'inverse son conjugué. Réciproquement, si z est inversible, il existe $x \in A$ tel que $zx = 1$. Ainsi $N(zx) = 1$ et $N(z)N(x) = 1$ dans $\mathbb{N}$. Ainsi $N(z) = 1$.
• En effet, si on a $p = zw, z, w \in \mathbb{Z}[\alpha]$, non inversibles. Ils sont donc de norme supérieur stricte à 1 et cela donne $N(p) = p^2 = N(z)N(w)$ donc $p = N(z) = N(w)$ par le lemme de d'Euclide qui est valable dans $\mathbb{N}$ et donc p est une norme.
Réciproquement, procédons par contraposée et supposons p irréductible. Par l'absurde supposons que p est une norme. Alors, il existe $z \in A$ tel que $p = N(z) = z\overline{z}$. Or p est irréductible, donc z ou $\overline{z}$ est inversible. Sans perte de généralité, supposons z inversible. Mais alors $\overline{z}$ est aussi inversible en passant au conjugué. Puisque l'ensemble des inversibles est un groupe, $z\overline{z}$ est aussi inversible. Donc $z\overline{z} = p$ est inversible. Ce qui est absurde puisque p est irréductible. □

Et donc si $p < 41$ comme il ne peut pas être une norme, il est irréductible. Ainsi notre première question est réglée : p reste irréductible dans A.

(iv) **Quid du lemme d'Euclide** : Rappelons rapidement ce qu'est le lemme d'Euclide : si p est irréductible et divise un produit alors il divise l'un de ses facteurs. Dans un anneau quelconque, les éléments vérifiant cette propriété sont appelés **premiers**. Grâce à Euclide, nous savons que ce lemme assure l'unicité de la décomposition en élément premiers dans $\mathbb{Z}$.

Faisons un petit détour par la factorialité, c'est-à-dire l'existence d'une décomposition unique, à permutation près des facteurs, en produit d'éléments irréductibles. Concrètement, il est relativement facile de

trouver une décomposition (en effet, si $z = wt$, on a $N(z) = N(w)N(t)$ et si w et t ne sont pas inversibles, la norme décroit, de sorte que le processus s'arrête au bout d'un nombre fini d'étapes). Cela étant dit, le point crucial est donc d'obtenir l'unicité. Et pour ce faire, il faut que nous soyons en possession du lemme d'Euclide. Le lemme suivant va, en quelque sorte, nous simplifier le lemme d'Euclide :

Lemme 1
Soit p un nombre premier de $\mathbb{Z}$ qui reste irréductible dans A, ie qui n'est pas une norme. Les assertions suivantes sont équivalentes :

1. *Si p divise zw avec $z, w \in A$, alors p divise z ou w.*
2. *Si p divise une norme $N(z)$, avec $z \in A$, alors il divise z.*

Si A vérifie une de ces deux propriétés, alors il est factoriel.

Démonstration : L'implication 1) $\implies$ 2) est immédiate. Réciproquement, si p divise zw, on a $zw = pt$, donc $p^2N(t) = N(z)N(w)$ dans $\mathbb{Z}$. Ainsi, p divise $N(z)N(w)$ et donc divise un des deux, disons $N(z)$ donc divise z. □

En vertu du lemme précédent, on doit donc s'intéresser à la divisibilité d'une norme. Nous allons encore retraduire cet énoncé :

Lemme 2
Un nombre premier p de $\mathbb{Z}$ divise une norme $N(z)$ pour $z \in A$ sans diviser z si et seulement si p est impair et si -163 est un carré modulo p, condition encore équivalente au fait que p est un carré modulo 163.

Démonstration : Supposons que p divise $N(x + \alpha y) = x^2 + xy + 41y^2$. S'il divise y, il divise aussi x donc z. Sinon, on peut diviser par y modulo p et alors le polynôme $x^2 + x + 41$ possède une racine modulo p. On voit déjà que $p \neq 2$ puisque $x^2 + x + 1$ n'a pas de racine. On peut alors calculer modulo p comme nous le ferions dans $\mathbb{R}$ et le polynôme a des racines si et seulement si son discriminant -163 est un carré modulo p. Pour ce qui est du reste, la loi de la réciprocité quadratique nous donne le résultat. □

Corollaire 1
Si l'un des nombres premiers $2, 3, 5, 7$ *divise une norme $N(z)$, $z \in A$, alors il divise z. Autrement dit, ces nombres sont irréductibles mais même premiers dans A.*

Démonstration : Pour 2 nous l'avons déjà vu. Pour les autres, il suffit donc de vérifier que -163 n'est pas un carré modulo p. En effet, $-163 \equiv -1$ [3] ; $-163 \equiv 2$ [5] et $-163 \equiv -2$ [7]. □
Nous aurions pu continuer ainsi jusqu'à $p = 37$, mais seuls ceux-ci nous suffisent.

(v) **Et la factorialité fut** : Et nous voilà donc prêts pour démontrer le résultat qu'il nous manquait pour valider entièrement la démonstration du théorème sur P_e :

Théorème 4
L'anneau $A = \mathbb{Z}[\alpha]$ vérifie la propriété 2. *du lemme* 1. *Il est donc factoriel.*

Démonstration : Reste donc à traiter le cas $p > 7$. On suppose que p divise une norme. Ainsi, il existe $K \in \mathbb{N}^*$ tel que Kp soit une norme. On montre alors (admis) en utilisant le théorème de Minkowski ou le principe des tiroirs (*cf.* [6]) ou l'algorithme de Cornacchia (*cf.* [4]) qu'il existe k avec $k \leqslant \sqrt{\frac{163}{3}}$ ou $k \leqslant \frac{2}{\pi}\sqrt{163}$ ou $k \leqslant \frac{2+\sqrt{41}+1}{\sqrt{2}}$ ie $k \leqslant 7$ ou $k \leqslant 8$ ou $k \leqslant 10$, tel que pk soit une norme $N(z)$. On en déduit alors que p est une norme. En effet, on choisit k le plus petit possible, on en prend un facteur premier q, qui sera donc inférieur ou égal à 7, il est alors premier dans A par le corollaire 1. Il divise donc z ou $\overline{z}$. Posons $k = qk'$. Si $z = qw$, on a $qk'p = q^2N(w)$ donc $k'p = qN(w)$. Comme q est premier avec p, il divise k' et on a $k' = qk''$. Donc $k''p = N(w)$, ce contredisant la minimalité de k. □

Nous avons donc démontré que $P_e(n)$ était premier pour $n \in \{0, \cdots, q-2\}$ à l'aide d'outils classiques. Commençons alors la présentation de notre nouvelle théorie.

Chapitre 1

Théorie

Tout résultat traitant des A-modules sera admis. La théorie des modules n'étant pas notre intérêt premier. Il est alors possible de se référer à [2].

1.1 Extensions Quadratiques

Définition 3
Soit $\mathbb{K}$ une extension de $\mathbb{Q}$. On dit que $\mathbb{K}$ est une ***extension quadratique*** *de $\mathbb{Q}$ si $[\mathbb{K} : \mathbb{Q}] = 2$.*

Proposition 2
Soit $\mathbb{L}/\mathbb{Q}$ une extension quadratique. Alors il existe $d \in \mathbb{Z}$ sans facteurs carrés dans sa décomposition, tel que $\mathbb{L} = \mathbb{Q}(\sqrt{d})$.

Démonstration : Soit $\mathbb{L}$ une extension quadratique de $\mathbb{Q}$. Soit $\alpha \in \mathbb{L} \setminus \mathbb{Q}$. Alors le couple $(1, \alpha)$ forme une base de $\mathbb{L}$ en tant que $\mathbb{Q}$-espace vectoriel. Il existe donc $u, v \in \mathbb{Q}$ tels que $\alpha^2 = u\alpha + v1$.
On peut donc écrire $u = \frac{m}{n}$ et $v = \frac{s}{t}$. Nous les mettons sur le même dénominateur : $u = \frac{b}{a}$ et $v = \frac{c}{a}$. On peut donc dire que α est racine du polynôme $P(X) = aX^2 - bX - c \in \mathbb{Z}[X]$.
On affirme que $\Delta := b^2 - 4ac$ n'est pas un carré parfait sinon α appartiendrait à $\mathbb{Q}$ puisque les racines de P sont de la forme $x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a}$.
Soit Δ_1 le plus grand carré diviseur de Δ. On peut alors écrire : $\Delta = \Delta_1 d$ et $\alpha = \frac{1}{2a}(b + \Delta_1 \delta)$ où δ est l'une des racines carrées complexes de d.
Alors $\delta \in \mathbb{L}$ puisque $\alpha, a, b, \Delta_1 \in \mathbb{L}$ et $\delta \notin \mathbb{Q}$ sinon $\alpha \in \mathbb{Q}$. Ainsi $\mathbb{Q}(\delta)$ est de degré 2 sur $\mathbb{Q}$ avec $\mathbb{Q}(\delta) \subset \mathbb{L}$, d'où l'égalité par le degré. □

$\longrightarrow$ On distingue deux cas : Si $d > 0$ alors $\mathbb{L} = \mathbb{Q}(\sqrt{d})$ est un sous-corps de $\mathbb{R}$; on dira que $\mathbb{L}$ est un sous-corps réel quadratique.
Si $d < 0$, alors $\mathbb{L} = \mathbb{Q}(\sqrt{d})$ est un sous-corps de $\mathbb{C}$ qui n'est pas un sous-corps de $\mathbb{R}$; on dira que $\mathbb{L}$ est un sous-corps quadratique imaginaire.
Par définition, tout élément $\alpha \in \mathbb{Q}(\sqrt{d})$ est de la forme $\alpha = a + b\sqrt{d}$, où $a, b \in \mathbb{Q}$. On appelle alors **élément conjugué** de α le nombre $\alpha' = a - b\sqrt{d}$.

Définition 4
Soit $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.

1. *On appelle* ***norme*** *de α le nombre : $N(\alpha) = \alpha\alpha' = a^2 - db^2 \in \mathbb{Q}$*
2. *On appelle* ***trace*** *de α le nombre : $Tr(\alpha) = \alpha + \alpha' = 2a \in \mathbb{Q}$.*

.

On remarque aussi rapidement que pour $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, $N(\alpha\beta) = N(\alpha)N(\beta)$ et $Tr(\alpha+\beta) = Tr(\alpha)+Tr(\beta)$
De plus, on constate que α et α' sont les racines du polynôme $P(X) = X^2 - Tr(\alpha)X + N(\alpha)$.

Une définition plus générale de la norme et de la trace d'un élément sera plus utile :

Définition 5
Soit B un anneau et A un sous-anneau de B tel que B soit un A-module de rang fini.
Pour $x \in B$, on définit l'endomorphisme de B : $m_x : y \longmapsto xy$
On appelle ***trace*** *(resp.* ***norme****) de $x \in B$ la trace (resp. le déterminant) de l'endomorphisme m_x.*

Ceci nous permet de voir rapidement que si $a \in A$ alors $N(a) = a^n$ où n est le rang de A sur B.

1.2 Anneau des entiers, nombres algébriques

Définition 6
On considère une extension quadratique $\mathbb{L}/\mathbb{Q}$. Soit $\alpha \in \mathbb{L}$.
*On dit que α est un **entier algébrique** s'il existe des entiers $m, n \in \mathbb{Z}$ tel que α soit racine du polynôme $P(X) = X^2 + mX + n$.*

Définition 7
*On appelle **anneau des entiers** de $\mathbb{L}$ l'ensemble des entiers algébriques que nous noterons $\mathcal{O}_{\mathbb{L}}$.*

Faisons tout de suite quelques petites remarques :

1. Comme son nom l'indique l'anneau des entiers possède bien une structure d'anneau... Ce que nous admettrons.
2. On note Frac($\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$) le corps des fractions de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Alors $\mathbb{Q}(\sqrt{d}) = Frac(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$.
   En effet, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \subset \mathbb{Q}(\sqrt{d})$ par définition. Puisque $\mathbb{Q}(\sqrt{d})$ est un corps, par définition de Frac(X) qui est le plus petit sous-corps contenant X, on obtient que Frac($\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$) $\subset \mathbb{Q}(\sqrt{d})$.
   Réciproquement, si $\alpha \in \mathbb{Q}(\sqrt{d})$, alors il existe $a_0, a_1, b_0, b_1 \in \mathbb{Z}$ tels que $\frac{a_0}{b_0} + \frac{a_1}{b_1}\alpha + \alpha^2 = 0$. D'où $a_0 b_0 b_1^2 + a_1 b_1 b_0^2 \alpha + b_0^2 b_1^2 \alpha^2 = 0$. En posant $\beta := b_0 b_1 \alpha$, on a que β est racine d'un polynôme à coefficients dans $\mathbb{Z}$, ie $\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. De plus $b_0 b_1 \in \mathbb{Z} \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Ainsi, $\alpha = \frac{\beta}{b_0 b_1} \in Frac(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$. D'où l'égalité.
3. On a aussi que $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z}$. L'inclusion droite-gauche est évidente. L'autre se fait en utilisant le fait que $\mathbb{Z}$ est intégralement clos.

Proposition 3
Soit $\alpha \in \mathbb{Q}(\sqrt{d})$. Alors α est entier sur $\mathbb{Z}$ si et seulement si $Tr(\alpha)$ et $N(\alpha)$ sont des entiers (relatifs).

<u>*Démonstration*</u> : Il est clair que si la trace et la norme sont entières, alors α est entier puisqu'il est racine de $X^2 - Tr(\alpha)X + N(\alpha)$.
Réciproquement, supposons α entier. S'il est dans $\mathbb{Q}$, comme $\mathbb{Z}$ est factoriel donc intégralement clos, α est dans $\mathbb{Z}$ et sa trace et sa norme aussi. Sinon, α est racine d'un polynôme P à coefficients entiers. Quitte à remplacer ce polynôme par un de ses facteurs irréductibles (puisque $\mathbb{Z}[X]$ est factoriel),on peut supposer P irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$. C'est donc le polynôme minimal de α, qui est $X^2 - Tr(\alpha)X + N(\alpha)$ puisque $\alpha \notin \mathbb{Q}$, et on en déduit que sa norme et sa trace dont des entiers. □

On peut alors avoir la proposition suivante sur la structure de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Proposition 4
L'ensemble des entiers $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ a pour structure :

1. $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$ *si* $d \equiv 2, 3$ [4]
2. $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ *si* $d \equiv 1$ [4]

<u>*Démonstration*</u> : Soit $z = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Par la proposition précédente sa trace, $2a$, et sa norme, $a^2 - db^2$ sont entières. Deux cas se présentent à nous :

1. Si a est entier, db^2 aussi. On pose alors $b = \frac{r}{s}$ avec $r \in \mathbb{Z}$ et $s \in \mathbb{N}^*$ et $PGCD(r, s) = 1$. Comme db^2 est dans $\mathbb{Z}$, on voit que s^2 divise dr^2 et, comme il est premier avec r^2, le lemme de Gauss nous donne qu'il divise d. Comme d est supposé sans facteurs carrés c'est qu'on a $s = 1$. En définitive, a et b sont entiers et z est dans $\mathbb{Z}[\sqrt{d}]$.
2. Sinon, on a $2a \in \mathbb{Z}$, mais $a \notin \mathbb{Z}$, donc $a = \frac{a'}{2}$ avec $a' \in 2\mathbb{Z} + 1$. On pose encore $b = \frac{r}{s}$ comme précédemment et on a $N(z) = \frac{a'^2}{4} - d\frac{r^2}{s^2} = n \in \mathbb{Z}$, soit encore $4s^2 n = a'^2 s^2 - 4dr^2$. Comme 4 divise $a'^2 s^2$ et que a' est impaire, s est pair, $s = 2s'$ et l'équation devient $4s'^2 n = a'^2 s'^2 - dr^2$. On voit alors que s'^2 divise dr^2 et, par Gauss, qu'il divise d et cela impose $s' = 1$. Il reste $4n = a'^2 - dr^2$. Comme s vaut 2 et qu'il est premier avec r, cela montre que r est impair, comme a', et leurs carrés sont congrus à 1 modulo 4. On en déduit qu'on a $d \equiv 1$ [4]
   Cela montre donc que le deuxième cas ne peut se produire si $d \equiv 2, 3$ [4] et le théorème est prouvé dans ces deux cas. Maintenant, si $d \equiv 1$ [4], les calculs précédents montre que ou bien $z \in \mathbb{Z}[\sqrt{d}]$ ou bien $z \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ et z s'écrit : $z = \frac{a'}{2} + \frac{r}{2}\sqrt{d}$ avec r et a' impairs donc $z = \frac{1+\sqrt{d}}{2} + \frac{a'-1}{2} + \frac{r-1}{2}\sqrt{d}$ et puisque $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, on a que $z \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. □

On a donc que :

1. Si $d \equiv 2,3$ [4], le couple $(1, \sqrt{d})$ forme une $\mathbb{Z}$-base de l'anneau $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.
2. Si $d \equiv 1$ [4], le couple $(1, \frac{1+\sqrt{d}}{2})$ est une $\mathbb{Z}$-base de l'anneau $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

1.3 Discriminant

Définition 8
Soit $\mathbb{L}/\mathbb{K}$ une extension de degré n. Soit $(x_1, ..., x_n) \in \mathbb{L}^n$.
*On appelle **discriminant** de $(x_1, ..., x_n)$ l'élément de $\mathbb{K}$ défini par : $D_{\mathbb{L}/\mathbb{K}}(x_1, ..., x_n) := \det((Tr(x_i x_j))_{i,j})$, où nous voyons la trace comme une application $\mathbb{K}-$bilinéaire de $\mathbb{L} \times \mathbb{L} \longrightarrow \mathbb{K}$, $(x, y) \longmapsto Tr(xy)$.*

Définition 9
On appelle discriminant de l'anneau des entiers $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ d'un corps $\mathbb{K}$, le discriminant d'une $\mathbb{Z}-$base.

Remarquons tout de suite que le discriminant de l'anneau des entiers ne dépend pas de la $\mathbb{Z}-$base choisie. En effet, le déterminant dans un changement de base d'une application bilinéaire est modifié par un carré. Or ce carré est le déterminant d'une application inversible, donc le déterminant est lui aussi un inversible. Or dans $\mathbb{Z}$, les seuls inversibles sont 1 et -1. Donc le discriminant n'est finalement pas changé.
$\longrightarrow$ Faisons alors les calculs du discriminant pour les corps qui nous intéressent.

1. Si $d \equiv 2,3$ [4] alors une $\mathbb{Z}-$base est $(1, \sqrt{d})$.
   On calcule alors $D_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}} = \det \begin{pmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$
2. Si $d \equiv 1$ [4] alors une $\mathbb{Z}-$base est $(1, \frac{1+\sqrt{d}}{2})$.
   On calcule alors $D_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}} = \det \begin{pmatrix} Tr(1) & Tr(\frac{1+\sqrt{d}}{2}) \\ Tr(\frac{1+\sqrt{d}}{2}) & Tr(\left(\frac{1+\sqrt{d}}{2}\right)^2) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d$

On remarque que dans tous les cas, le discriminant $D_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}$ est congru à 0 ou 1 modulo 4.

1.4 Idéaux et décomposition en idéaux premiers

1.4.1 Norme d'un idéal

Dans ce paragraphe, nous noterons par $\mathbb{K}$ un corps de nombres, ie une extension de $\mathbb{Q}$ de degré n, et $\mathcal{O}_{\mathbb{K}}$ son anneau des entiers.

Proposition 5
Soit x un élément non nul de $\mathcal{O}_{\mathbb{K}}$. On a $|N(x)| = Card\,(\mathcal{O}_{\mathbb{K}}/x\mathcal{O}_{\mathbb{K}})$.

<u>*Démonstration*</u> : On sait que $\mathcal{O}_{\mathbb{K}}$ est un $\mathbb{Z}-$module libre de rang n (admis) et donc $x\mathcal{O}_{\mathbb{K}}$ est un sous-$\mathbb{Z}-$module de $\mathcal{O}_{\mathbb{K}}$. il est donc aussi de rang n car la multiplication est une bijection de $\mathcal{O}_{\mathbb{K}} \longrightarrow x\mathcal{O}_{\mathbb{K}}$. Il existe alors une base $(e_1, ..., e_n)$ de $\mathcal{O}_{\mathbb{K}}$ et des éléments $c_i \in \mathbb{N}$ tels que $(c_1 e_1, ..., c_n e_n)$ soit une $\mathbb{Z}-$base de $x\mathcal{O}_{\mathbb{K}}$ (admis). Ainsi $\mathcal{O}_{\mathbb{K}}/x\mathcal{O}_{\mathbb{K}}$ est isomorphe à $\prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$ et son cardinal est alors $c_1 c_2 \cdots c_n$.
Notons l'application $\mathbb{Z}-$linéaire $u : \begin{cases} \mathcal{O}_{\mathbb{K}} \longrightarrow \mathcal{O}_{\mathbb{K}} \\ e_i \longmapsto c_i e_i \end{cases}$, pour $i \in \{1, ..., n\}$: on a donc $\det(u) = c_1 c_2 \cdots c_n$.
Mais encore, $(xe_1, \cdots, xe_n)$ est aussi une base de $\mathcal{O}_{\mathbb{K}}$. On a donc l'existence d'un automorphisme v de $x\mathcal{O}_{\mathbb{K}}$ tel que $v(c_i e_i) = xe_i, \forall i \in \{1, ..., n\}$. Donc $\det(v)$ est inversible dans $\mathbb{Z}$ et vaut donc ± 1. Mais nous remarquons aussi que $v \circ u$ est la multiplication par x et son determinant est, par définition, $N(x)$. Et comme $\det(v \circ u) = \det(v)\det(u)$, on en déduit que : $N(x) = \pm c_1 c_2 \cdots c_n = \pm Card\,(\mathcal{O}_{\mathbb{K}}/x\mathcal{O}_{\mathbb{K}})$. □

Définition 10
Soit I un idéal de $\mathcal{O}_{\mathbb{K}}$. On appelle norme de I, noté $N(I)$, le nombre $Card\,(\mathcal{O}_{\mathbb{K}}/I)$.

Remarquons de suite que $N(I)$ est fini. En effet, si x est un élément non nul de I, on a $x\mathcal{O}_{\mathbb{K}} \subset I$ et $\mathcal{O}_{\mathbb{K}}/I$ s'identifie alors à un quotient de $\mathcal{O}_{\mathbb{K}}/x\mathcal{O}_{\mathbb{K}}$. Ainsi, $Card\,(\mathcal{O}_{\mathbb{K}}/I) \leqslant Card\,(\mathcal{O}_{\mathbb{K}}/x\mathcal{O}_{\mathbb{K}})$, ce dernier étant fini par la proposition 4.
Nous avons aussi démontré que pour un idéal principal, $N((x)) = |N(x)|$.

Définition 11 (Produit d'idéaux)
Soient I et J deux idéaux.
*On appelle **idéal produit de I et J**, noté IJ, l'idéal $IJ := \{\sum_{k\in K} x_k y_k \ ; \ x_k \in I, y_k \in J\}$ où K est un ensemble d'indexation fini.*

Proposition 6
Soient I_1, I_2 deux idéaux non nuls de $\mathcal{O}_\mathbb{K}$. On a alors $N(I_1 I_2) = N(I_1)N(I_2)$.

Démonstration : ADMISE. (*cf.* [2]) □

Donnons un petit lemme utile qui nous servira dans nos démonstrations :

Lemme 3
Soit A un anneau et I un idéal de A.
Si $N(I)$ est un nombre premier alors I est premier.

Démonstration : Notons $N(I) = p$, où p est un nombre premier. Alors par définition, $\text{Card}(A/I) = p$. Prenons maintenant J, un idéal A/I. Alors puisque J est un sous-groupe de A, $Card(J)$ divise $Card(A/I)$. Forcément, $Card(J) = 1$ ou p. Donc, par cardinalité, les seuls idéaux de A/I sont les idéaux triviaux : $\{0\}$ et A. Ainsi, A/I est un corps, et donc I est maximal et donc premier. □

1.4.2 Décomposition en idéaux premiers

Définition 12 (Idéaux fractionnaires)
Soit A un anneau et Frac(A) son corps de fraction.
*On appelle **idéal fractionnaire** de A tout sous-A-module I de Frac(A) pour lequel il existe $d \in A$, $d \neq 0$ tel que $dI \subset A$.*

Remarquons directement que tout idéal I d'un anneau A est un idéal fractionnaire. En effet, en notant 1_A le neutre de A, on a $1_A I \subset A$.

Définition 13 (Anneau de Dedekind)
*Un anneau A est dit **anneau de Dedekind** s'il est noethérien, intégralement clos et si tout idéal premier non nul de A est maximal.*

Théorème 5
L'anneau des entiers $\mathcal{O}_\mathbb{K}$ d'un corps de nombre $\mathbb{K}$ est de Dedekind.

Démonstration :

- Comme nous l'avons vu dans une remarque suivant la définition 7 dans la section 1.2, l'anneau $\mathcal{O}_\mathbb{K}$ est intégralement clos.
- Pour montrer que $\mathcal{O}_\mathbb{K}$ est noethérien, nous allons utiliser une autre définition : un anneau est noethérien si et seulement si tout idéal est de type fini.
  Prenons un idéal I de $\mathcal{O}_\mathbb{K}$, alors I est un sous-groupe de $\mathcal{O}_\mathbb{K}$, donc un $\mathbb{Z}$-module de type fini, et a fortiori un idéal de type fini.
- Enfin, prenons un idéal premier P non nul de $\mathcal{O}_\mathbb{K}$. Alors $\mathcal{O}_\mathbb{K}/P$ est intègre. De plus, $\mathcal{O}_\mathbb{K}/P$ est inclus dans $\mathcal{O}_\mathbb{K}/x\mathcal{O}_\mathbb{K}$ pour un $x \in P$, qui est fini en vertu des propriétés sur la norme. Ainsi $\mathcal{O}_\mathbb{K}/P$ est un anneau intègre et fini donc un corps. Ainsi P est maximal. □

Théorème 6 (Décomposition en idéaux premiers)
Soit A un anneau de Dedekind, $\mathcal{P}$ l'ensemble des idéaux premiers non nuls de A.
Tout idéal fractionnaire non nul I de A s'écrit de façon unique sous la forme

$$I = \prod_{J\in\mathcal{P}} J^{n_J(I)}$$

où $n_J(I)$ sont des entiers relatifs, presque tous nuls.

Démonstration : ADMISE. (*cf.* [2]) □

Voici un corollaire du théorème de la décomposition qui nous sera utile lors de la partie sur le nombre de classe.

Corollaire 2
L'ensemble des idéaux fractionnaires non nuls d'un anneau possède une structure de groupe.

Démonstration : ADMISE. (*cf.* [2]) □

Théorème 7
Soit $\mathbb{K}$ un corps de nombres de degré n. Soit p un nombre premier de $\mathbb{K}$. On pose $(p) = p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathcal{O}_{\mathbb{K}}$ et e_i des entiers.
Alors il existe des entiers positifs f_i tels que $N(\mathfrak{p}) = p^{f_i}$ pour tout i et nous avons aussi

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

Démonstration : Puisque la norme est multiplicative, nous avons $N((p)) = p^n = N\left(\prod_{i=1}^{r} \mathfrak{p}_i^{e_i}\right) = \prod_{i=1}^{r} N(\mathfrak{p}_i)^{e_i}$.
Donc par le lemme d'Euclide, $N(\mathfrak{p}_i) = p^{f_i}$ pour tout i. On se retrouve donc bien $\sum_{i=1}^{r} e_i f_i = n$. □

1.4.3 Classification des idéaux

Nous nous replaçons dans le cas où notre corps est $\mathbb{Q}(\sqrt{d})$, avec d un entier sans facteurs carrés et $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.
Dorénavant, nous noterons l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ par $\mathbb{A}$.

Proposition 7
Tout idéal d'un anneau de Dedekind est engendré, en tant qu'idéal, par 2 éléments.

Démonstration : Preuve utilisant la notion de réseau. (*cf.* [9]). □

Cette propriété nous sera utile pour la « classification » des idéaux que nous allons faire ci-dessous. Plus précisément, nous pouvons choisir un de ces éléments dans $\mathbb{Z}$.

Considérons maintenant le cas particulier où p est un nombre premier et regardons $(p) = p\mathbb{A}$. (p) va pouvoir s'écrire d'une des manières suivantes en vertu du théorème 7 de la sous-section 1.4.2 :

1. $(p) = P^2$, où P est un idéal premier. On dira que p est **ramifié** sur $\mathbb{Q}(\sqrt{d})$.
2. $(p) = P$, où P est un idéal premier. On dira que p est **inerte** sur $\mathbb{Q}(\sqrt{d})$.
3. $(p) = P_1P_2$, où P_1, P_2 sont deux idéaux premiers distincts. On dira que p est **décomposé** sur $\mathbb{Q}(\sqrt{d})$.

Nous allons maintenant classer les entiers premiers, ie savoir s'ils sont ramifiés, inertes ou décomposés. De plus, nous donnerons des générateurs explicites des idéaux premiers de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ au dessus de p, c'est-à-dire qui apparaissent dans la décomposition de $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ en idéaux premiers.
Avant tout, définissons un objet qui nous sera fondamental et qui est fondamental dans la théorie des corps.

Définition 14 (Symbole de Legendre)
Soit p un nombre premier et a un entier.
*On appelle **symbole de Legendre** de a et p, noté $\left(\frac{a}{p}\right)$, l'objet vérifiant :*

1. $\left(\frac{a}{p}\right) = 0$ *si p divise a.*
2. $\left(\frac{a}{p}\right) = 1$ *si a est un carré modulo p.*
3. $\left(\frac{a}{p}\right) = -1$ *si a n'est pas un carré modulo p.*

Pour formuler cette classification, nous allons distinguer deux cas : $p = 2$ et $p \neq 2$. Commençons par ce dernier.

Théorème 8
On se place dans $\mathbb{Q}(\sqrt{d})$ et on considère son anneau d'entiers $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.
Soit p un nombre premier différent de 2.
Alors nous avons :

1. *Si p divise d, alors $(p) = p\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = (p, \sqrt{d})^2$.*
2. *Si p ne divise pas d et qu'il n'existe pas un entier $a \in \mathbb{Z}$ tel que $d \equiv a^2\ [p]$, alors $(p) = p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ est un idéal premier.*
3. *Si p ne divise pas d et qu'il existe un élément $a \in \mathbb{Z}$ tel que $d \equiv a^2\ [p]$, alors $(p) = p\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = (p, a+\sqrt{d})(p, a-\sqrt{d})$.*

Autrement dit :

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

<u>*Démonstration*</u> : Pour plus de lisibilité, nous noterons $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{A}$.

1. Commençons par montrer que si $\left(\frac{d}{p}\right) = -1$ alors (p) est un idéal premier.
   Si tel n'était pas le cas, nous aurions $(p) = PP'$ ou P^2, avec $P \cap \mathbb{Z} = p\mathbb{Z}$. Soit $\alpha \in \mathbb{A}$ tel que $P = (\alpha, p) \supset (\alpha)$. Ainsi, en termes d'idéaux, $P \mid (\alpha)$ d'où $N(P) \mid N((\alpha))$. Et puisque $N((p)) = p^2$ et que p est premier, on a $N(P) = p$, d'où $p \mid N(\alpha\mathbb{A}) = |N(\alpha)|$. Si $p \mid \alpha$, alors $\frac{\alpha}{p} \in \mathbb{A}$ et on a $P = p\mathbb{A} \cdot (1, \frac{\alpha}{p}) = (p)$ ce qui serait absurde ! Donc p ne divise pas α. Ainsi :
   - Si $d \equiv 2, 3\ [4]$ alors $\alpha = a + b\sqrt{d},\ a, b \in \mathbb{Z}$, donc $N(\alpha) = a^2 - db^2$ et d'où $p \mid a^2 - db^2$.
   - Si $d \equiv 1\ [4]$ alors $\alpha = \frac{a+b\sqrt{d}}{2},\ a, b \in \mathbb{Z}$ et donc $N(\alpha) = \frac{a^2-db^2}{4}$. Ainsi, $p \mid a^2 - db^2$.

   Autrement dit, $a^2 \equiv db^2\ [p]$, et donc p ne divise pas b. En effet, sinon p diviserait a et donc diviserait α ce qui serait absurde à nouveau !
   Prenons alors b' tel que $bb' \equiv 1\ [p]$ ce qui est possible puisque nous sommes dans $\mathbb{Z}/p\mathbb{Z}$ qui est un corps. Alors $(ab')^2 \equiv d\ [p]$ et donc soit $p \mid d$ soit $\left(\frac{d}{p}\right) = 1$ ce qui est une contradiction de l'hypothèse.
2. Supposons maintenant que $\left(\frac{d}{p}\right) = 0$. Ensuite posons $P = (p, \sqrt{d})$. Ainsi :
   $$P^2 = (p^2, p\sqrt{d}, d) = p\mathbb{A} \cdot (p, \sqrt{d}, \frac{d}{p})$$
   car $\frac{d}{p} \in \mathbb{Z}$ par hypothèse. Mais comme d ne contient pas de carrés par hypothèse, forcément $PGCD(p, \frac{d}{p}) = 1$ et ainsi $P^2 = p\mathbb{A}$ puisque qu'alors $(p, \sqrt{d}, \frac{p}{d}) = (1, \sqrt{d}) = \mathbb{A}$ et que si un idéal contient un inversible, il est alors égal à tout l'anneau dont il fait parti. Ainsi, puisque P^2 est un idéal premier, P en est aussi un : en effet, $N(P^2) = p^2 \implies N(P)^2 = p^2$, donc $N(P) = p$. Ainsi comme P est un idéal de norme première, il est premier.
3. Supposons enfin $\left(\frac{d}{p}\right) = 1$ et qu'il existe un élément $a \in \mathbb{Z}$ tel que $d \equiv a^2\ [p]$. Nous avons donc :
   $$\begin{aligned}(p, a+\sqrt{d})(p, a-\sqrt{d}) &= (p^2, pa + p\sqrt{d}, pa - p\sqrt{d}, a^2 - d)\\ &= p\mathbb{A} \cdot (p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p})\\ &= p\mathbb{A} \cdot (p, a+\sqrt{d}, a-\sqrt{d}, 2a, \frac{a^2-d}{p})\\ &= p\mathbb{A}\end{aligned}$$
   puisque $PGCD(p, 2a) = 1$ et donc on démontre comme précédemment les égalités. Si un des deux idéaux $(p, a+\sqrt{d})$ et $(p, a-\sqrt{d})$ est égal à $\mathbb{A}$ alors l'autre le serait aussi, ce qui serait absurde.
   Ainsi $(p, a+\sqrt{d})$ et $(p, a-\sqrt{d})$ sont des idéaux premiers en voyant que leurs normes sont premières par l'égalité précédente. Ils sont de plus distincts ; en effet si $(p, a+\sqrt{d}) = (p, a-\sqrt{d})$, alors :
   $$(p, a+\sqrt{d}) = (p, a+\sqrt{d}, a-\sqrt{d}) = (p, a+\sqrt{d}, a-\sqrt{d}, 2a) = \mathbb{A}$$
   Ce qui est absurde ! □

$\longrightarrow$ Faisons une petite remarque qui nous sera utile pour la démonstration de notre théorème.
Si $d \equiv 1\ [4]$ et $d \equiv a^2\ [p]$ alors on peut écrire $(p, a+\sqrt{d}) = (p, l(a-1)+\omega)$, où $\omega = \frac{1+\sqrt{d}}{2}$ et $2l \equiv 1\ [p]$. De plus, si $\left(\frac{d}{p}\right) \neq 1$ alors il existe $b \in \mathbb{Z}$, $0 \leqslant b \leqslant p-1$ tel que p divise $N(b+\omega)$, et si $b = p-1$ alors $d \equiv 1\ [p]$.

En effet, $a+\sqrt{d} = a-1+2\omega$. Si $2l \equiv 1\ [p]$ alors :

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

Si $\left(\frac{d}{p}\right) \neq -1$, alors il existe un idéal premier P qui divise (p), et $P = (p, a+\sqrt{d})$ avec $0 \leqslant a \leqslant p-1$. Donc $P = (p, b+\sqrt{d})$ avec $0 \leqslant b \leqslant p-1$ et $b \equiv l(a-1)\ [p]$.
Enfin, comme $(b+\omega)\mathbb{A} \subset P$, il vient que p divise $N(P)$, cette dernière divisant $N(b+\omega)$ par inclusion. Donc $p \mid N(b+\omega)$. Et finalement, si p divise $N(p-1+\omega) = N(\frac{2p-1+\sqrt{d}}{2}) = \frac{(2p-1)^2-d}{4}$ alors p divise $\frac{1-d}{4}$ d'où $d \equiv 1\ [p]$.

Nous allons maintenant traiter le cas $p = 2$:

Théorème 9
On se place toujours dans $\mathbb{Q}(\sqrt{d})$ et on considère toujours son anneau d'entiers $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. On a :

1. *Si $d \equiv 2\ [4]$, alors $(2) = (2, \sqrt{d})^2$.*
2. *Si $d \equiv 3\ [4]$, alors $(2) = (2, 1+\sqrt{d})^2$.*
3. *Si $d \equiv 1\ [8]$, alors $(2) = (2, \frac{1+\sqrt{d}}{2})(2, \frac{1-\sqrt{d}}{2})$.*
4. *Si $d \equiv 5\ [8]$, alors (p) est un idéal premier ;*

Autrement dit :

1. *2 est ramifié si et seulement si $d \equiv 2, 3\ [4]$.*
2. *2 est inerte si et seulement si $d \equiv 5\ [8]$.*
3. *2 est décomposé si et seulement si $d \equiv 1\ [8]$.*

Démonstration : ADMISE. Les raisonnements utilisent des manipulations similaires à la preuve précédente. (*cf.* [1]) □

1.5 Nombre de classes

1.5.1 Quelques assertions

Nous allons maintenant introduire l'objet qui sera le plus important pour notre étude des polynômes d'Euler : le groupe de classe et le nombre de classe.
Nous avons vu précédemment que l'ensemble des idéaux fractionnaire de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, noté $\mathcal{IF}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$, possède une structure de groupe. De plus, il nous faut remarquer que les idéaux fractionnaires principaux forme un sous-groupe de $\mathcal{IF}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$, noté $\mathcal{IP}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$.

Définition 15
*On appelle le **groupe de classes d'idéaux** de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ le groupe quotient suivant :*

$$CL(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}) = \mathcal{IF}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})/\mathcal{IP}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$$

*Nous appellerons **nombre de classes** de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ le cardinal du groupe de classes.*

On a une autre définition du groupe de classes via une relation d'équivalence :

Définition 16
Soit A un anneau de Dedekind et $Frac(A)$ son corps de fraction. Soit I et J deux idéaux non triviaux de A.
On dit que I et J sont équivalents, noté $I \sim J$, s'il existe $\alpha \in Frac(A)$ tel que $I = \alpha J$.

Il est facile de vérifier qu'on a ici une relation d'équivalence sur l'ensemble des idéaux fractionnaires de $\mathcal{IF}(A)$. Ainsi, l'espace quotient réalisé par la relation $\sim$ sur $\mathcal{IF}(A)$, muni du produit des idéaux, obtient une structure de groupe. C'est cet espace quotient que nous appellerons le **groupe des classes d'idéaux** de A, noté toujours $CL(A)$.
Ainsi, nous pouvons dire que $CL(A)$ mesure le défaut de principalité de A.

Le théorème le plus important de cette section est le suivant :

Théorème 10
Le groupe de classes d'idéaux de tout anneau de nombre est fini.

Démonstration : ADMIS. (*cf.* [2]) □

Voici aussi la proposition qui justifiera toute notre étude à venir :

Proposition 8
Soit A un anneau de Dedekind.
Le nombre de classe de A vaut 1 si et seulement si A est principal.

Démonstration : Par la définition de $CL(A)$ et avec le fait qu'il ne contienne qu'un seul élément. □

En corollaire, nous déduisons un résultat qui sera plus proche de notre point de vue comme nous l'avons vu en introduction.

Corollaire 3
Soit $\mathbb{K}$ un corps de nombre et $\mathbb{A}$ son anneau des entiers.
Alors $\mathbb{A}$ est factoriel si et seulement si son nombre de classe vaut 1.

Démonstration : Supposons que le nombre de classe vaille 1. Par le théorème précédent, $\mathbb{A}$ est principal et donc factoriel.
Réciproquement supposons $\mathbb{A}$ factoriel. Montrons alors qu'il est principal.

- Soit $\mathcal{M}$ un idéal maximal de $\mathbb{A}$. Soit $x \in \mathcal{M}$ non nul. On décompose alors $x = p_1 \cdots p_r$ en éléments irréductibles. Comme $\mathcal{M}$ est premier car maximal, un des p_i appartient à $\mathcal{M}$. Ainsi$(0) \subset (p_i) \subset \mathcal{M}$. De plus (p_i) est premier donc maximal car nous sommes dans un anneau de Dedekind, donc par l'inclusion $\mathcal{M} = (p_i)$.
- Ensuite prenons I un idéal quelconque. alors $I = (x_1, \cdots, x_n)$ car $\mathbb{A}$ est noethérien. Montrons alors par récurrence sur n que I est principal. Il suffit de le montrer dans le cas où $I = (x, y)$. Puisque A est factoriel, on a l'existence de $d = PGCD(x, y)$ avec $(d) \supset (x, y)$. On peut alors écrire $x = dx'$, $y = dy'$ avec $PGCD(x', y') = 1$. Ainsi $(x', y') = (1) = \mathbb{A}$ et il existe donc λ, μ tels que $1 = \lambda x' + \mu y'$. Donc, $d = \lambda x + \mu y$, d'où $d \in I$ et alors $(d) \subset I$ d'où l'égalité. □

1.5.2 Calcul pratique : méthode

Dorénavant, nous revenons à l'étude de nos corps quadratiques $\mathbb{Q}(\sqrt{d})$. Nous noterons aussi $h = h(d)$ le nombre de classe de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.
Indiquons maintenant les quelques derniers outils techniques dont nous allons avoir besoin.
Définissons le nombre réel suivant :

$$\theta = \begin{cases} \frac{1}{2}\sqrt{d}, \text{ si } d > 0 \\ \frac{2}{\pi}\sqrt{-d}, \text{ si } d < 0 \end{cases}$$

Définition 17
*i) On dira qu'un idéal non vide de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ est **normalisé** si $N(I) \leqslant \lfloor \theta \rfloor$.*
*ii) Un idéal I est dit **primitif** s'il n'existe pas de nombre premier p tel que (p) divise I.*

Notons maintenant $\mathcal{N}$ l'ensemble de tous les idéaux primitifs et normalisés de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.
Nous pouvons de suite remarquer que si $I \in \mathcal{N}$, et si p est un nombre premier ramifié alors $p^2 \nmid N(I)$. Idem, si p est un nombre premier inerte alors $p \nmid N(I)$; tout ceci provenant de la définition de tels nombres premiers et du fait que I soit dans $\mathcal{N}$. Ainsi, nous obtenons la décomposition suivante :

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

en supposant avoir décomposé en idéaux premiers $I = \prod \mathcal{P}_i^{e_i}$, grâce à la multiplicativité de la norme et avec ce que nous avons dit précédemment.
Nous allons admettre les faits suivants pour notre étude du nombre de classes (*cf.* [1]) :

1. Toute classe d'idéal contient au moins un idéal primitif et normalisé.
2. Pour tout $m \in \mathbb{N}^*$, il existe au plus un nombre fini d'idéaux I de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ tel que $N(I) = m$.

De ces deux points précédents et de tout ce qui a été mis en place, nous pouvons obtenir les points suivants :

- Remarquons que si $\mathcal{N}$ consiste seulement de l'idéal neutre, $1 \cdot \mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, alors $h = 1$.
- Si chaque nombre premier p tel que $p \leqslant \lfloor \theta \rfloor$ est inerte, alors $h = 1$. En effet, si $I \in \mathcal{N}$ et vérifie la condition, alors $N(I) = 1$; donc I est l'idéal unité et donc $h = 1$.

Notons maintenant $N(\mathcal{N})$ l'ensemble des entiers de la forme $N(I)$ où I parcourt $\mathcal{N}$.
Dans le but de déterminer si deux idéaux I et J dans $\mathcal{N}$ sont équivalents, il nous sera nécessaire de déterminer quels entiers $n \in N(\mathcal{N})$ peuvent s'écrire sous la forme d'une norme d'un idéal principal primitif.

Proposition 9
Soit $m \in \mathbb{Z}$. Alors il existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tel que $N((\alpha)) = m$ et (α) est primitif si et seulement si il existe $u, v \in \mathbb{Z}$ *tels que :* $m = \begin{cases} |u^2 - dv^2|, & PGCD(u,v) = 1 \quad si\ d \equiv 2,3\ [4] \\ \frac{|u^2-dv^2|}{4}, & PGCD(\frac{u-v}{2}, v) = 1 \quad si\ d \equiv 1\ [4] \end{cases}$

Démonstration : Soit $\alpha \in \mathcal{O}_{\mathbb{K}}$ tel que (α) primitif et $m = N((\alpha))$. Puisque $\alpha \in \mathcal{O}_{\mathbb{K}}$, alors par le théorème de structure de l'anneau des entiers (proposition 3.), il existe $u, v \in \mathbb{Z}$ tels que $\alpha = \begin{cases} u + v\sqrt{d}, & \text{si } d \equiv 2,3\ [4] \\ u + v\frac{1+\sqrt{d}}{2}, & \text{si } d \equiv 1\ [4] \end{cases}$
Ainsi, nous obtenons que $m = N((\alpha)) = |N(\alpha)| = \begin{cases} |u^2 - dv^2|, & \text{si } d \equiv 2,3\ [4] \\ \frac{|u^2-dv^2|}{4}, & \text{si } d \equiv 1\ [4] \end{cases}$

Reste à montrer que $PGCD(u, v) = 1$. De la même manière nous montrerions que $PGCD(\frac{u-v}{2}, v) = 1$. Alors, soit p premier qui divise u et v. Par somme, p divise α. Autrement dit, $(p) \supset (\alpha)$. Ce qui est absurde par primitivité de (α). Ainsi $PGCD(u, v) = 1$.
Réciproquement, posons $\alpha = \begin{cases} u + v\sqrt{d}, & \text{si } d \equiv 2,3\ [4] \\ u + v\frac{1+\sqrt{d}}{2}, & \text{si } d \equiv 1\ [4] \end{cases}$
On a clairement que $N((\alpha)) = m$. Et du fait que u, v sont premiers entre eux, (α) est bien primitif. □

1.5.3 Calcul du nombre de classes

Dans ce chapitre nous allons étudier comment calculer le nombre de classes « à la main ». Bien sûr notre étude ne sera pas exhaustive dans la mesure où nous ne pouvons étudier chaque discriminant... Enfin dans la partie suivante, nous expliciterons presque tous les corps quadratiques ayant un nombre de classe valant 1. Nous allons considérer deux cas en fonction du signe de d.

• Prenons $\mathbf{d>0}$ et donc $\theta = \frac{1}{2}\sqrt{D}$**.**

∗ $\lfloor \theta \rfloor = 1$.
Puisque $1 \leqslant \frac{1}{2}\sqrt{D} < 2$, il vient que $4 \leqslant D < 16$. Donc $D \in \{4, 5, 8, 9, 12, 13\}$ car $D \equiv 0, 1\ [4]$ (*cf. partie* 1.3). En gardant à l'esprit que d n'a pas de facteurs carrés, il vient que $d \in \{5, 2, 3, 13\}$. Ce cas va être conclu rapidement puisque $\lfloor \theta \rfloor = 1$, donc forcément $N(\mathcal{N}) = \{1\}$ et alors $\mathcal{N}$ consiste uniquement de l'idéal unité ; et comme dans chaque classe d'idéaux il y a au moins un idéal primitif normalisé *(cf.sous-partie* 1.5.2*)*, et bien $h = 1$, puisque tous les idéaux sont équivalents à un idéal principal et donc sont tous dans la même classe.

∗ $\lfloor \theta \rfloor = 2$.
De même, puisque $2 \leqslant \frac{1}{2}\sqrt{D} < 3$, il vient que $16 \leqslant D < 36$ et comme $D \equiv 0, 1\ [4]$ nous avons que $D \in \{16, 17, 20, 21, 24, 25, 28, 29, 32, 33\}$. Et enfin comme d n'a pas de facteurs carrés, nous nous retrouvons avec $d \in \{17, 21, 6, 7, 29, 33\}$. Maintenant nous avons donc $N(\mathcal{N}) = \{1, 2\}$ par définition d'un idéal normalisé. Nous éliminons le cas égal à 1 puisqu'il nous mène à l'idéal unité. Et nous allons regarder pour 2.

— Par exemple prenons $d = 17$. Puisque $17 \equiv 1$ [8] alors il vient que $(2) = 2\mathbb{A} = P \cdot P'$. Et comme $N(2\mathbb{A}) = 4 = N(P)N(P')$ (car extension de degré 2), nous trouvons que $N(P) = N(P') = 2$. Nous allons de suite exploiter la proposition 8 de la sous-partie précédente : $2 = \frac{1}{4}|3^2 - 17 \times 1|$ et $PGCD(\frac{3-17}{2}, 17) = 1$, ainsi $P = \alpha\mathbb{A}$,avec $\alpha = \frac{3+\sqrt{17}}{2}$, et $P' = \alpha'\mathbb{A}$ où $\alpha' = \frac{3-\sqrt{17}}{2}$. Nous trouvons qu'il ne peut y avoir que des idéaux principaux et donc ils sont tous équivalents, donc il n'y a qu'un élément dans $CL(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$, ie $h = 1$.

— Ensuite $d = 21$. Puisque $21 \equiv 5$ [8], alors $(2) = 2\mathbb{A}$ est un idéal premier, donc 2 est inerte. Et donc par le deuxième point de la sous-partie précédente, $h = 1$.

— Et un dernier exemple $d = 6$. Alors 2 divise $24 = D$, donc 2 est ramifié, ie $(2) = P^2$. Enfin par la proposition 8, $2 = |2^2 - 6 \times 1^2|$ et $PGCD(2, 1) = 1$. D'où $P = \alpha\mathbb{A}$, avec $\alpha = 2 + \sqrt{6}$. Et donc, comme précédemment $h = 1$.

∗ $\lfloor\theta\rfloor = 3$.

Toujours comme précédemment : $3 \leqslant \frac{1}{2}\sqrt{D} < 4$ et $36 \leqslant D < 64$ toujours avec $D \equiv 0, 1$ [4]. Alors $D \in \{36, 37, 40, 41, 44, 45, 48, 49, 52, 53, 56, 57, 60, 61\}$ et donc $d \in \{37, 10, 41, 11, 53, 14, 57, 15, 61\}$. Et nous sommes donc dans le cas où $N(\mathcal{N}) = \{1, 2, 3\}$.

— Prenons par exemple $d = 10$. Il nous faut considérer les cas où la norme vaut $2, 3$ car le cas 1 mène à l'idéal unitaire. Ensuite, puisque 2 divise $40 = D$, alors 2 est ramifié, ie $(2) = 2\mathbb{A} = R^2$. Ensuite puisque $\left(\frac{10}{3}\right) = \left(\frac{1}{3}\right) = 1$, 3 est alors décomposé, c'est-à-dire $(3) = 3\mathbb{A} = P \cdot P'$. Ainsi, nous avons que P, P' et R sont des idéaux primitifs. Mais, 2 n'a pas de représentation primitive ; en effet si $2 = |u^2 - 10v^2|$ alors $u^2 = 10v^2 \pm 2 \equiv \pm 2$ [10], mais ceci est impossible en regardant tous les carrés modulo 10. De même, 3 n'a pas de représentation primitive ; en effet si $3 = |u^2 - 10v^2|$ alors $u^2 = 10v^2 \pm 3 \equiv \pm 3$ [10], ce qui est aussi absurde en regardant tous les carrés modulo 10. Donc nous obtenons, toujours via la même proposition, que P, P' et R ne sont pas principaux. Donc nous avons au plus 4 classes d'idéaux dans $CL(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$: $\overline{1}, \overline{P}, \overline{P'}$ et $\overline{R}$. Remarquons deux petits points :

— Puisque $2\mathbb{A} = R^2$, $\overline{1} = \overline{R}^2$ ie $\overline{R} = \overline{R}^{-1}$.

— De même, puisque $3\mathbb{A} = P \cdot P'$ alors $\overline{1} = \overline{P} \cdot \overline{P'}$ et donc $\overline{P} = \overline{P'}^{-1}$.

Regardons maintenant les idéaux produits RP et RP'. Ces derniers sont toujours primitifs. De plus, $N(RP) = N(RP') = 2 \times 3 = 6$. Et donc toujours par la proposition 8, nous avons que RP et RP' sont principaux puisque $-2 \times 3 = -6 = 2^2 - 10 \times 1^2$ et $PGCD(2, 1) = 1$. Et donc par ce que nous avons remarqué précédemment, nous obtenons :

$$\begin{cases} \overline{R} \cdot \overline{P} = \overline{1} \\ \overline{R} \cdot \overline{P'} = \overline{1} \end{cases} \iff \begin{cases} \overline{P} = \overline{R}^{-1} = \overline{R} \\ \overline{P'} = \overline{R}^{-1} = \overline{R} \end{cases}$$

Donc nous nous retrouvons avec 2 classes d'idéaux distinctes et donc $h = 2$.

• Prenons maintenant $\mathbf{d<0}$ et ainsi $\theta = \frac{2}{\pi}\sqrt{-D}$.

∗ $\lfloor\theta\rfloor = 1$.

Comme toujours, puisque $1 \leqslant \frac{2}{\pi}\sqrt{-D} < 2$ et donc $\frac{\pi^2}{4} \leqslant |D|\pi^2$. Et comme $|D| \equiv 0, 3$ [4], nous obtenons $D \in \{3, 4, 7, 8\}$, et donc $d \in \{-3, -1, -7, -2\}$. Nous nous retrouvons forcément avec $N(\mathcal{N}) = \{1\}$, ce qui implique que $\mathcal{N}$ ne contient que l'idéal unité, et puisque que toute classe contient un idéal primitif et normalisé, tous les idéaux d'une classe sont équivalents à l'idéal unité, donc nous nous retrouvons qu'avec une classe et $h = 1$.

∗ $\lfloor\theta\rfloor = 2$.

Puisque $2 \leqslant \frac{2}{\pi}\sqrt{-D} < 3$, alors $\pi^2 \leqslant |D| < \frac{9}{4}\pi^2$. Et toujours comme $|D| \equiv 0, 3$ [4], nous trouvons $|D| \in \{11, 12, 15, 16, 19, 20\}$ et donc $d \in \{-11, -15, -19, -5\}$.

— Prenons $d = -11$. Puisque $-11 \equiv 5$ [8], alors 2 est inerte. Et par le point 4 de la sous-partie précédente, nous avons $h = 1$.

— Prenons ensuite $d = -15$. Puisque $-15 \equiv 1$ [8], alors $(2) = 2\mathbb{A} = P \cdot P'$. Remarquons de suite que 2 n'a pas de représentation primitive : Si $2 = \frac{|u^2+15v^2|}{4}$, alors $u^2 + 15v^2 = 8$ et donc $u^2 \equiv 3$ [5]. Ce qui est absurde en regardant tous les carrés modulo 5. Reste donc à déterminer si les classes de P et P' sont les mêmes. Considérons alors $R = \left(\frac{1+\sqrt{-15}}{2}\right)$ (*cf.* [8]). Ainsi $N(R) = N(\frac{1+\sqrt{-15}}{2}) = 4$. Puisque R n'est pas premier, il se décompose donc forcément comme P'^2 ou P^2 ou $P \cdot P'$ grâce à la norme. Clairement, $R \neq P \cdot P'$. Donc $R = P^2$ ou P'^2. Mais dans les deux cas, nous avons $\overline{P}^2 = \overline{1}$ et $\overline{P'}^2 = \overline{1}$. Sans perte de généralité, on a que $\overline{P} = \overline{P}^{-1}$. Et donc $\overline{P} = \overline{P}^{-1} = \overline{P'}$. Il n'y a donc que 2 classes différentes, et ainsi $h = 2$.

$*$ $\lfloor\theta\rfloor = 3$.
Puisque $3 \leqslant \frac{2}{\pi}\sqrt{-D} < 4$, comme précédemment nous obtenons $|D| \in \{23, 24, 27, 28, 31, 32, 35, 36, 39\}$ et donc $d \in \{-23, -6, -31, -35, -39\}$.

— Prenons ici $d = -31$. Puisque $-31 \equiv 1$ [8], alors $(2) = P \cdot P'$. Et aussi comme $\left(\frac{-31}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{1}{3}\right) = -1$, il vient que $(3) = 3\mathbb{A} = R$ est un idéal premier.

(a) Voyons d'abord pour 2 : On a que 2 n'a pas de représentation primitive. En effet, si $2 = \frac{|u^2+31v^2|}{4}$, ainsi $8 = u^2 + 31v^2$, ce qui est impossible. Donc P et P' ne sont pas des idéaux principaux. Ainsi $\overline{P} = \overline{P'}^{-1}$. Regardons maintenant l'élément $\frac{1+\sqrt{-31}}{2}$. On a $N\left(\frac{1+\sqrt{-31}}{2}\right) = 8 = 2^3$. L'idéal engendré par cet élément se décompose en produit d'idéaux parmi P et P'. Supposons que PP' divise $\left(\frac{1+\sqrt{-31}}{2}\right)$. Alors (2) divise $\left(\frac{1+\sqrt{-31}}{2}\right)$ dans $\mathbb{A}$. Ce qui n'est pas possible. Donc forcément $\left(\frac{1+\sqrt{-31}}{2}\right) = P^3$ ou P'^3. Supposons sans perte de généralité que $\left(\frac{1+\sqrt{-31}}{2}\right) = P^3$ et alors $\overline{P^3} = \overline{1} = \overline{P}^3$. Si jamais $\overline{P}^2 = 1$ alors $\overline{P}^3 = \overline{P}$ mais $\overline{P} \neq \overline{1}$ donc c'est impossible. Et alors $\overline{P}^2\overline{P'} \neq \overline{P'}$ et $\overline{P} \neq \overline{P'}$.

(b) On a que $(3) = R$, d'où $\overline{R} = \overline{1}$.

Finalement, on a trouvé trois classes différentes : $\overline{1}, \overline{P}$ et $\overline{P'}$ Donc $h = 3$.

1.5.4 Détermination des corps quadratiques ayant pour nombre de classe 1

Nous allons distinguer deux cas en fonction du signe de d, pour $\mathbb{Q}(\sqrt{d})$.

• **d>0** : Dans ce cas là, nous sommes seulement en présence d'une conjecture : il existe une infinité de $d > 0$ tels que $\mathbb{Q}(\sqrt{d})$ a un nombre de classe étant égal à 1. Nous sommes plutôt en faveur d'une réponse positive à cette conjecture ; mais elle est toujours à démontrer. Par exemple, il existe 142 corps $\mathbb{Q}(\sqrt{d})$, où $2 \in \{2, \cdots, 500\}$, avec un nombre de classe 1.

• **d<0** : Nous avons déjà vu que si $\mathcal{N}$, l'ensemble idéaux primitifs et normalisés de $\mathbb{A}$, où A est l'anneau des entiers, est constitué uniquement de l'idéal unité, alors $h = 1$, avec h le nombre de classe.

Mais dans le cas $d < 0$, nous avons la condition nécessaire et suffisante : $h = 1$ si et seulement si $\mathcal{N} = \{\mathbb{A}\}$
En effet, tout d'abord comme cous l'avons vu dans la section précédente, si $|D| \leqslant 7$, le résultat est vrai (où D est le discriminant). Supposons maintenant $|D| > 7$, et soit $I \in \mathcal{N}$, et $I \neq \mathbb{A}$. Alors il existe un idéal premier P qui divise I. Ainsi $N(p) = p$ oup^2, où p est un nombre premier. Si $N(P) = p^2$, alors p est inerte et $p\mathbb{A} = P$ divise I, donc I ne serait pas primitif, ce qui est absurde. Ensuite, si $N(P) = p$, puisque P divise I, alors $p \leqslant N(I) \leqslant \lfloor\theta\rfloor \leqslant \frac{2}{\pi}\sqrt{|D|}$. Supposons que p a une représentation primitive :

— Si $d \equiv 2, 3$ [4], alors $d = \frac{|D|}{4}$ et $p = u^2 - dv^2$. Mais $v \neq 0$, ainsi $\frac{2}{\pi}\sqrt{|D|} \geqslant p \geqslant |d| = \frac{|D|}{4}$ et donc $7 \geqslant \frac{64}{\pi^2} \geqslant |D|$, ce qui est absurde.

— Si $d \equiv 1$ [4], alors $d = D$, d'où $p = \frac{u^2-dv^2}{4}$. Mais $v \neq 0$, ainsi $\frac{2}{\pi}\sqrt{|D|} \geqslant p \geqslant \frac{|d|}{4} = \frac{|D|}{4}$ et nous trouvons encore $7 \geqslant D$, ce qui est absurde.

Ainsi, P n'est pas un idéal principal par la proposition 8, et donc $h \neq 1$, ce qui contredit l'hypothèse. □

Pour déterminer les corps quadratiques imaginaires qui nous intéressent, nous allons utiliser (et admettre) un critère que Gauss avait développé : Si $d < 0$, et si nous notons par t le nombre de facteurs premiers distincts dans la décomposition de D, alors 2^{t-1} divise le nombre de classe de $\mathbb{Q}(\sqrt{d})$.
Ainsi si $h = 1$ alors $D = -4, -8$ ou $-p$, puisque d n'a pas de termes carrés, où p est un nombre premier p tel que $p \equiv 3$ [4], et alors $d = -1, -2$ ou$-p$. Donc de la sous-partie précédente, et du calcul précédent, on a que : si $D = -3, -4, -7, -8$ alors $h = 1$. Sinon, si $D \neq -3, -4, -7, -8$ et $D = -p$, avec $p \equiv 3$ [4], alors $h = 1$ si et seulement si $\mathcal{N} = \{\mathbb{A}\}$. Et cette dernière condition est équivalente aux assertions suivantes : 2 est inerte dans $\mathbb{Q}(\sqrt{-p})$ et si q est n'importe quel nombre premier impair tel que $q \leqslant \lfloor\theta\rfloor$ alors $\left(\frac{-p}{q}\right) = -1$, ie q est inerte dans $\mathbb{Q}(\sqrt{-p})$.
Ce critère va nous être utile pour déterminer tous les $D < 0$, $|D| \leqslant 200$, ayant un nombre de classes valant 1.

- $\lfloor\theta\rfloor = 1$: Ceci mène aux discriminants $D = -3, -4, -7, -8$.
- $\lfloor\theta\rfloor = 2$: Nous trouvons que $-20 \leqslant D \leqslant -11$, avec $D = p$ où $p \equiv 3$ [4], donc $D = -11, -19$. Puisque $-11 \equiv 5$ [8], alors 2 est inerte, donc si $D = -11$ alors $h = -1$. De même, puisque $-19 \equiv 5$ [8], alors 2 est inerte et donc si $D = -19$, alors $h = 1$.

- $\lfloor\theta\rfloor = 3$: Ici nous nous retrouvons avec $-39 \leqslant D \leqslant -23$ et $D = -p$, avec $p \equiv 3$ [4]. Ainsi, nous trouvons $D = -23$ ou -31. Mais, comme $-21 \not\equiv 5$ [8] et $-31 \not\equiv 5$ [8], le nombre de classe de $\mathbb{Q}(\sqrt{-23})$ et de $\mathbb{Q}(\sqrt{-31})$ ne vaut pas 1.
- $\lfloor\theta\rfloor = 4$: Nous avons $-59 \leqslant D \leqslant -40$, toujours avec $D = -p$ et $p \equiv 3$ [4]. Ainsi $D = -43, -47, -59$. Puisque $-43 \equiv 5$ [8] et $\left(\frac{-43}{3}\right) = -1$, on a que $\mathbb{Q}(\sqrt{-43})$ a un nombre de classe de 1. Mais puisque $-47 \not\equiv 5$ [8] et $\left(\frac{-59}{3}\right) = 1$, donc 3 n'est pas inerte. Ainsi comme précédemment, les extensions de corps $\mathbb{Q}(\sqrt{-47})$ et $\mathbb{Q}(\sqrt{-59})$ ont un nombre de classes différent de 1.

En répétant des raisonnements similaires, nous obtenons les résultats suivants :

- $\lfloor\theta\rfloor = 5$: On trouve $D = -67$ ayant pour nombre de classes 1.
- $\lfloor\theta\rfloor = 6$: Il n'y pas de discriminant D ayant un nombre de classes valant 1.
- $\lfloor\theta\rfloor = 7$: Aucun discriminant ne donne de corps avec un nombre de classes de 1.
- $\lfloor\theta\rfloor = 8$: $D = -163$ donne un corps quadratique imaginaire ayant un nombre de classes valant 1.

Ce processus peut être continué jusqu'à 200. Cela dit, il ne mènera à aucun autre discriminant pour lequel le nombre de classe vaut 1. Mais cela ne nous permet pas encore de conclure quant à la détermination complète des extensions quadratiques imaginaires ayant un nombre de classe valant 1.
Historiquement, il a d'abord été montré en 1934, par Heilbronn et Linfoot qu'il existait au plus une autre valeur de $d < 0$ pour laquelle $\mathbb{Q}(\sqrt{d})$ a un nombre de classe de 1. Plus tard, Lehmer montra qu'un tel discriminant d vérifiait $|d| > 5 \times 10^9$. Enfin en 1952, Heegner prouva d'un manière peu claire qu'aucun autre $d < 0$ vérifiait la condition. Ce n'est que quelques temps plus tard que Baker et ensuite Stark prouvèrent avec différents outils, mais clairement, le résultat. Indiquons rapidement un résultat intéressant qui fut démontré par les travaux de Hecke, Deuring, Mordell et Heilbronn et qui était à l'origine une conjecture de Gauss : Si $d < 0$ alors $h(d) \xrightarrow[|d|\to+\infty]{} +\infty$.

Nous pouvons donc conclure sur le fait que nous avons déterminé tous les corps quadratiques imaginaires qui ont un nombre de classes valant 1.

Chapitre 2

Le théorème

Voici maintenant le théorème principal de ce mémoire qui va mélanger toute la théorie mise en place appliquée aux polynômes d'Euler.

Théorème 11
Soit q un nombre premiers et posons $f_q(X) = X^2 + X + q$. Les assertions suivantes sont équivalentes :

(i) $q = 2, 3, 5, 11, 17, 41$

(ii) $f_q(n)$ *est premier pour* $n \in \{0, 1, ..., q-2\}$.

(iii) $\mathbb{Q}(\sqrt{1-4q})$ *a un nombre de classe valant* 1.

Démonstration :

- L'implication $(i) \implies (ii)$ est une simple (fastidieuse) vérification.
- L'implication $(iii) \implies (i)$ est justifiée par la détermination de tous les corps quadratiques imaginaires avec un nombre de classes valant 1 que nous fîmes dans la sous-partie 1.5.4. En effet, si $\mathbb{Q}(\sqrt{1-4q})$ a un nombre de classes valant 1 alors $d = 1 - 4q = -7, -11, -19, -43, -67, -163$. Autrement dit, $q = 2, 3, 5, 7, 11, 17, 41$.
- Montrons alors l'implication $(ii) \implies (iii)$.
  Soit $d = 1 - 4q < 0$. Alors $d \equiv 1$ [4] Si $q = 2, 3$ alors $d = -7, -11$ et alors $\mathbb{Q}(\sqrt{d})$ a un nombre de classes de 1, comme nous l'avons vu. Supposons maintenant que $q \geqslant 5$. Il suffit alors de montrer que chaque nombre premier $p \leqslant \frac{2}{\pi}\sqrt{|d|}$ est inerte dans $\mathbb{Q}(\sqrt{d})$, comme nous l'avons vu dans la partie 1.5.2.
  Tout d'abord, prenons $p = 2$. Puisque nous pouvons écrire $q = 2t - 1$ et que $d = 1 - 4q = 1 - 4(2t-1) \equiv 5$ [8], alors 2 est inerte dans $\mathbb{Q}(\sqrt{d})$ par le théorème 9 de la partie 1.4.3.
  Maintenant, prenons $p \neq 2$ et $p \leqslant \frac{2}{\pi}\sqrt{d} < \sqrt{d}$ et supposons que p n'est pas inerte. Alors, nous avons que $\left(\frac{d}{p}\right) \neq -1$ et comme nous l'avons remarqué juste après le théorème 8 de la sous-partie 1.4.3, il existe $b \in \mathbb{Z}$, $0 \leqslant b \leqslant p-1$ tel que p divise $N(b+\omega)$, où $\omega = \frac{1+\sqrt{d}}{2}$. Ceci donne que p divise la quantité suivante :

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

  Remarquons de ce pas que $b \neq p-1$, sinon nous aurions, toujours grâce à la remarque qui suit le théorème 8, p divise $1 - d = 4q$, d'où $p = q < \sqrt{|d|} = \sqrt{|1-4q|}$ et donc $q^2 < 4q - 1$ *ie* $q = 2, 3$ ce qui est absurde.
  Ensuite, par hypothèse $f_q(b)$ est un nombre premier, du coup $\sqrt{4q-1} > p = f_q(b) \geqslant f_q(0) = q$ et encore $q = 2, 3$, ce qui contredit l'hypothèse. Ainsi, nous avons bien montré par l'absurde que tout nombre premier inférieur à $\frac{2}{\pi}\sqrt{|d|}$ est inerte et donc le nombre de classe de l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est 1.
- La démonstration est dorénavant terminée puisque nous avons démontré les implications circulaires. Mais par intérêt, nous démontrerons aussi l'implication $(iii) \implies (ii)$.
  Supposons donc que $d = 1 - 4q$ et que le nombre de classe h de $\mathbb{Q}(\sqrt{-d}$ est $h = 1$. Alors soit $d = -1, -2, -1, -7$ soit $d < -7$ et donc $d \equiv -p$ avec $p \equiv 3$ [4] et $q > 2$, ce que nous avons vu dans

la sous-partie 1.5.4. Toujours dans cette même sous-partie, nous avons noté que 2 était inerte dans $\mathbb{Q}(\sqrt{-p}))$, donc $p \equiv 3$ [8].
Ensuite nous allons montrer que si l est un nombre premier impair vérifiant $l < q$, alors $\left(\frac{l}{p}\right) = -1$. En effet, si $\left(\frac{l}{p}\right) = 1$, alors l se décompose dans $\mathbb{Q}(\sqrt{-p})$. Mais nous avons $h = 1$, donc il existe un entier algébrique $\alpha = \frac{a+b\sqrt{-p}}{2}$ tel que $(l) = l\mathbb{A} = \alpha\mathbb{A} \cdot \alpha'\mathbb{A}$, où $\mathbb{A}$ est l'anneau des entiers. Alors :

$$l^2 = N(l\mathbb{A}) = N(\alpha\mathbb{A})N(\alpha'\mathbb{A}) = N(\alpha\mathbb{A})^2 = N(\alpha)^2$$

Donc $l = N(\alpha) = \frac{a^2+b^2p}{4}$. Ainsi, $p+1 = 4q > 4l = a^2+b^2p$, d'où $1 > a^2+(b^2-1)p$ et nécessairement $a^2 = 0$ et $b^2 = 1$. Ceci donne que $4l = p$ qui est absurde.
Supposons alors maintenant qu'il existe un entier m, $m \in \{0, \cdots, q-2\}$ tel que $f_q(m)$ n'est pas premier. Alors il existe un nombre premier l tel que $l^2 \leqslant m^2 + m + q$ et $m^2 + m + q = al$, avec $a \geqslant 1$. Puisque $f_q(m)$ est impair (car q premier et > 2), on a que $l \neq 2$ et

$$l^2 \leqslant m^2 + m + q \iff 4l^2 \leqslant 4m^2 + 4m + 4q$$

Or $4m^2 + 4m + 4q = 4m^2 + 4m + 1 - d = 4m^2 + 4m + 1 + p = (2m+1)^2 + p$, nous obtenons :

$$4l^2 \leqslant 4m^2 + 4m + 4q \iff 4 \leqslant (2m+1)^2 + p$$

Mais comme par hypothèse $m \leqslant q + 2$, on a :

$$\begin{aligned} m < q - 1 &\implies m + 1 < q \\ &\implies 2m + 2 < 2q \\ &\implies 2m + 1 < 2q - 1 \end{aligned}$$

Or, nous remarquons que $\frac{p-1}{2} = \frac{-d-1}{2} = \frac{-1+4q-1}{2} = \frac{-2+4q}{2} = -1 + 2q$ et ainsi obtenons que :

$$4l^2 < \left(\frac{p-1}{2}\right)^2 + p = \left(\frac{p+1}{2}\right)^2$$

D'où $l < \frac{p+1}{4} = q$.
Comme nous l'avons montré précédemment, $\left(\frac{l}{p}\right) = -1$. Cependant, par des calculs similaires aux précédents, nous avons :

$$4al = (2m+1)^2 + 4q - 1 = (2m+1)^2 + p$$

D'où, $-p$ est un carré modulo l. Ainsi par la loi de la réciprocité quadratique, nous avons :

$$1 = \left(\frac{-p}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}}\left(\frac{l}{p}\right)(-1)^{\frac{l-1}{2}\frac{p-1}{2}} = \left(\frac{l}{p}\right)$$

Ce qui est absurde. Donc il n'existe pas de nombre m, $m \in \{0, \cdots, q-2\}$ tel que $f_q(m)$ n'est pas premier. □

Bibliographie

[1] RIBENBOIM Paulo. *My Numbers, My Friends : Popular Lectures on Number Theory.* Springer, 2000

[2] SAMUEL Pierre. *Théorie algébrique des nombres.* Éditions Hermann, 1971.

[3] PERRIN Daniel. *Cours d'algèbre.* Ellipse, 1996.

[4] PERRIN Daniel. *Pourquoi y a-t-il beaucoup de nombres premiers de la forme n^2+n+41 ?* [En ligne].
Disponible : https ://www.math.u-psud.fr/ perrin/journeedu2311/redaction2311e.pdf

[5] BAKER Matthew. *Algebraic number theory : Course note (Fall 2006), Math 8803, Georgia Tech* [En ligne]. Atlanta : School of mathematics, Georgia Institute Of Mathematics ; 2006.
Disponible : http ://people.math.gatech.edu/ mbaker/pdf/ANTBook.pdf

[6] PERRIN Daniel. *Anneaux d'entiers des corps quadratiques imaginaires* [En ligne].
Disponible : https ://www.math.u-psud.fr/ perrin/TER/anneauxd'entiers.pdf

[7] EDIXHOVEN Bas, MORET-BAILLY Laurent. *Cours de maîtrise de mathématiques : Théorie algébriques des nombres.* [En ligne]. Université de Rennes 1 : Septembre 2004.
Disponible : https ://perso.univ-rennes1.fr/laurent.moret-bailly/docpedag/polys/tano04.pdf

[8] CONRAD Keith. *Class group calculations* [En ligne].
Disponible : http ://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/classgpex.pdf

[9] CHENEVIER Gaëtan. *Arithmétiques des entiers quadratiques imaginaires.* [En ligne].
Disponible : http ://gaetan.chenevier.perso.math.cnrs.fr/MAT552/cours4.pdf