Théorie de Kummer appliquée à la résolution d'équations diophantiennes

Faucher Liam

Stage de recherche en L3 sous la direction de : M. Caldero Philippe

Université Claude Bernard Lyon 1
43 Boulevard du 11 novembre 1918, Villeurbanne

5 juillet 2026

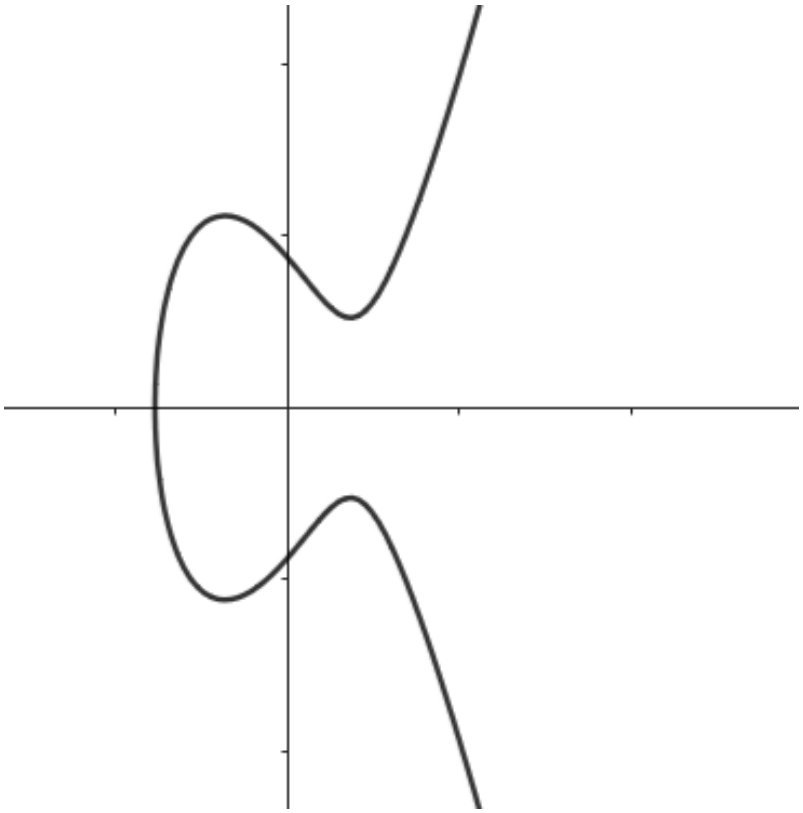

Table des matières

Notations

(a)	Idéal engendré par l'élément a
χ_f	Polynôme caractéristique de l'endomorphisme f
$\mathbb{P}$	Ensemble des nombres premiers
$\mathcal{O}_K$	Anneau des entiers du corps K
μ_f	Polynôme minimal de l'endomorphisme f
μ_z	Polynôme minimal de z sur $\mathbb{Q}$
Φ_n	n-ième polynôme cyclotomique
m_z	Morphisme multiplication par z

1 Introduction et prérequis

1.1 Présentation du cadre - Introduction historique

Les éléments de théorie présentés dans ce document sont principalement motivés par la résolution d'équations diophantiennes, c'est-à-dire la recherche de solutions entières à des équations polynomiales à coefficients entiers et à plusieurs indéterminées.

L'exemple le plus marquant est sûrement celle qui constitue la conjecture de 1637 de Pierre de Fermat. Souvent nommée Dernier théorème de Fermat, cette équation fut un obstacle majeur de la théorie des nombres pendant plus de 300 ans. En 1994, Andrew Wiles établit des liens entre la géométrie algébrique et la théorie des nombres, et prouve par la même occasion la conjecture de Fermat. Depuis le XXe siècle, cette branche, via l'étude géométrique des équations diophantiennes, est celle ayant fourni le plus de résultats en arithmétique ; jusqu'à récemment cette année 2026 où Gerd Faltings reçoit le prix Abel pour ses travaux en géométrie arithmétique.

Avant ça, le XIXe siècle est marqué par un essor de la théorie algébrique des nombres. L'approche est ici tout autre, purement algébrique. Cet angle d'attaque reposant sur la factorialité de certains anneaux, popularisé par Carl Friedrich Gauss dans ses *Disquisitiones Arithmeticae* de 1801, se révèle particulièrement fructueux pour la résolution d'équations. En 1847, Ernst Kummer résout partiellement le problème de Fermat en introduisant des outils avancés basés sur les travaux de Gauss. Ces outils vont par la suite être formalisés par Richard Dedekind, ce qui conduit notamment à la définition des idéaux.

L'objectif de ce document est, via le formalisme moderne hérité de Dedekind, de présenter une partie des travaux de Kummer.

1.2 Exemple de résolution par la factorialité

Avant de voir sa généralisation par Kummer, illustrons rapidement la méthode de Gauss citée plus tôt. On ne s'attardera pas sur certains détails de démonstration car nous traiterons un cas plus général dans la section 4 de ce document.

L'idée est de factoriser l'équation dans un anneau *factoriel* i.e. où tout élément non nul s'écrit de façon unique comme produit d'éléments irréductibles à multiplication près par un élément inversible. L'objectif est ainsi de diminuer le degré de l'équation et d'obtenir une paramétrisation des potentielles solutions.

On cherche les couples entiers tels que $x^3 = y^2 + 1$. Nous allons utiliser le fait que $\mathbb{Z}[i]$, appelé anneau des *Entiers de Gauss*, est factoriel.

On considère un couple de solution et on réécrit l'équation sous la forme suivante :

$$x^3 = (y + i)(y - i) = ab, \tag{1}$$

où $a := y + i$ et $b := y - i$. Supposons que l'on ait montré que a et b sont premiers entre eux dans $\mathbb{Z}[i]$. Notons alors :

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \ , \quad b = v \prod_{p \in \mathcal{P}} p^{v_p(b)} \ \text{ et } \ x = w \prod_{p \in \mathcal{P}} p^{v_p(x)}$$

où $\mathcal{P}$ est un système de représentants des irréductibles non nuls de $\mathbb{Z}[i]$, et $u, v, w \in \mathbb{Z}[i]^\times$. Alors :

$$\forall p \in \mathcal{P}, \begin{cases} 3v_p(x) = v_p(a) + v_p(b) \\ v_p(a) = 0 \text{ ou } v_p(b) = 0 \end{cases}$$

La première égalité vient de (1) et la seconde vient du fait que $a \wedge b = 1$. Il s'ensuit que :

$$\forall p \in \mathcal{P}, 3 \mid v_p(a) \text{ et } v_p(b).$$

Donc a et b sont également des cubes à multiplication par un inversible près. Ainsi il existe $\alpha, \beta \in \mathbb{Z}$ et $\omega \in \mathbb{Z}[i]^\times$ tels que :

$$a = y + i = \omega(\alpha + i\beta)^3.$$

Ceci permet d'obtenir des conditions sur y puis x, et il vient assez vite que le seul couple entier solution est $(1, 0)$.

Remarque 1.1. Cette méthode, bien que très efficace, est en pratique assez spécifique car les anneaux factoriels sont en fait assez rares. Typiquement, considérons une variante de l'équation précédente :

$$x^3 = y^2 + d \text{ avec } d \in \mathbb{N}^*.$$

On peut adapter la recette pour $d = 2$ car $\mathbb{Z}[i\sqrt{2}]$ est factoriel, et avec un peu plus d'efforts pour $d = 3$ (en effet, $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel mais $\mathbb{Z}[j]$ où $j := \frac{-1+i\sqrt{3}}{2}$ lui l'est, on l'appelle l'anneau des *Entiers d'Eisenstein*. Il est assez proche de $\mathbb{Z}[i\sqrt{3}]$ si bien qu'on arrive à s'y plonger et à remonter). Cependant, on se retrouve vite bloqué car l'anneau $\mathbb{Z}[i\sqrt{d}]$ n'est factoriel que pour $d = 1$ ou 2, et l'astuce de $d = 3$ ne se généralise pas. Ainsi, si l'on se pose la question de résoudre l'équation :

$$x^3 = y^2 + 10,$$

nous sommes pour l'heure coincés si l'on se restreint à une démarche similaire. Le principal enjeu de cette théorie va être de développer des outils pour pouvoir généraliser notre approche à une classe d'anneaux bien plus importante.

1.3 Rappels préliminaires

Terminons ce préambule en démontrant quelques résultats plus ou moins élémentaires de théorie des corps. Ces derniers sont des prérequis nécessaires pour pouvoir aborder la théorie de Kummer. D'abord, cette sous-section est dédiée à quelques rappels sur l'algébricité.

Rappel 1.2. Soit k un corps et K une extension de k. Un élément $x \in K$ est dit *algébrique sur* k si $[k(x) : k] < \infty$. Alors, il existe un unique polynôme unitaire irréductible P de $k[X]$ qui annule x. De plus, $k(x)$ est isomorphe à $k[X]/(P)$. En outre, $(1, x, \ldots, x^{d-1})$ est une base de $k(x)$, si bien que $d = [k(x) : k]$ (où $d := \deg(P)$).

Démonstration. Considérons le morphisme d'évaluation en x :

$$\begin{array}{rccc} \mathrm{ev}_x : & k[X] & \longrightarrow & k[x] \\ & P & \longmapsto & P(x) \end{array}$$

Notons I l'idéal $\mathrm{Ker}(\mathrm{ev}_x)$. Pour tout produit $TS \in I$ i.e. $(TS)(x) = T(x)S(x) = 0$, on a T ou S qui annule x par intégrité de K. D'où, T ou S est dans I. Ainsi, I est premier, non nul car x est algébrique. Il est donc engendré par un polynôme irréductible de $k[X]$, car $k[X]$ est principal. Tous les polynômes qui engendrent I sont associés, donc égaux à une constante multiplicative près. Donc, si on impose la condition P unitaire, ce polynôme est unique. C'est bien l'unique polynôme annulateur de x qui est à la fois unitaire et irréductible dans $k[X]$: en effet, si $\tilde{P}$ convient, alors $\tilde{P} \in (P)$ i.e. $P \mid \tilde{P}$; puis, comme $\tilde{P}$ est unitaire et irréductible, il vient $\tilde{P} = P$.

Par le 1er théorème d'isomorphisme, on a $k[X]/(P) \simeq k[x]$. Or (P) est un idéal premier d'un anneau principal, il est donc maximal, si bien que $k[X]/(P)$ est un corps. Il vient alors que $k[x] = k(x)$. Considérons enfin la famille $\mathcal{F} := (1, x, \ldots, x^{d-1})$. $\mathcal{F}$ est une famille libre de $k(x)$: en effet, soient $\lambda_0, \ldots \lambda_{d-1} \in k$ tels que :

$$\lambda_0 + \lambda_1 x + \cdots + \lambda_{d-1} x^{d-1} = 0$$

Le polynôme $Q := \lambda_0 + \lambda_1 X + \cdots + \lambda_{d-1} X^{d-1}$ est dans (P) et vérifie $\deg(Q) < d = \deg(P)$, c'est donc le polynôme nul. En outre, notons $\pi : k[X] \longrightarrow k[X]/(P)$ le morphisme quotient. Pour tout $T \in k[X]$, on écrit la division euclidienne de T par P, $T = PQ + R$ puis alors $\pi(T) = \pi(R)$ où $\deg(R) < d$. Cela signifie que $(1, \bar{X}, \ldots, \bar{X}^{d-1})$ est une famille génératrice de $k[X]/(P)$. Alors, $\mathcal{F}$ est génératrice de $k(x)$ par l'isomorphisme précédent, c'est donc une base de $k(x)$.

□

Définition 1.3. P est appelé le *polynôme minimal* de x sur k.

Montrons alors une propriété qui permet de prolonger des morphismes de corps. Bien qu'élémentaire, cette proposition est fondamentale car, d'une certaine manière, c'est l'idée qui conduit aux fondements de la Théorie de Galois et à la théorie des corps plus avancée.

Proposition 1.4. Soient L_1/K_1 et L_2/K_2 des extensions de corps. Soit également, pour $i = 1$ ou 2, $\alpha_i \in L_i$ algébrique sur K_i, et $P_i = \sum_{j=0}^{d_i} a_j X^j$ son polynôme minimal sur K_i. Alors, s'il existe $\sigma \in \mathrm{Hom}(K_1, K_2)$ tel que :

$$\bar{\sigma}(P_1) := \sum_{j=0}^{d_1} \sigma(a_j) X^j = P_2$$

Il existe $\tilde{\sigma} \in \mathrm{Hom}(K_1(\alpha_1), K_2(\alpha_2))$ qui prolonge σ et tel que $\tilde{\sigma}(\alpha_1) = \alpha_2$.

Démonstration. Considérons d'abord :

$$\begin{array}{rccc} \bar{\sigma} : & K_1[X] & \longrightarrow & K_2[X] \\ & \sum_{j\geq 0} a_j X^j & \longmapsto & \sum_{j\geq 0} \sigma(a_j) X^j \end{array}$$

C'est l'unique morphisme prolongeant σ et défini par $\bar{\sigma}(X) = X$. Remarquons alors que, comme $\bar{\sigma}(P_1) = P_2$, on a :

$$\forall P, Q \in K_1[X], \quad P - Q \in (P_1) \Longrightarrow \ \bar{\sigma}(P) - \bar{\sigma}(Q) = \bar{\sigma}(P - Q) \in (P_2).$$

Ainsi, le morphisme $\bar{\sigma}$ passe au quotient, c'est-à-dire que l'on peut définir un morphisme de la façon suivante :

$$\begin{array}{rccc} \phi : & K_1[X]/(P_1) & \longrightarrow & K_2[X]/(P_2) \\ & P+(P_1) & \longmapsto & \bar{\sigma}(P)+(P_2) \end{array}$$

Enfin, d'après le rappel 1.2, pour $i = 1$ ou 2, on a l'isomorphisme suivant :

$$\begin{array}{rccc} \phi_i : & K_i(\alpha_i) & \longrightarrow & K_i[X]/(P_i) \\ & \sum_{j=0}^{d_i-1} x_j \alpha_i^j & \longmapsto & \sum_{j=0}^{d_i-1} x_j \bar{X}^j \end{array}$$

Alors, on pose $\tilde{\sigma} = \phi_2^{-1} \circ \phi \circ \phi_1$ qui vérifie bien $\tilde{\sigma}(\alpha_1) = \alpha_2$, car $\phi(\overline{X}) = \overline{X}$. Et en outre, ce morphisme vérifie, pour tout $x \in K_1$:

$$\tilde{\sigma}(x) = \phi_2^{-1}(\phi(\phi_1(x))) = \phi_2^{-1}(\phi(x+(P_1))) = \phi_2^{-1}(\sigma(x)+(P_2)) = \sigma(x)$$

□

1.4 Quelques propriétés des extensions séparables

Dans cette dernière sous-section, nous allons introduire et utiliser la notion de séparabilité, dans le but d'établir des résultats sur des extensions finies de $\mathbb{Q}$ dans les sections suivantes. On notera $\bar{\mathbb{K}}$ une clôture algébrique du corps $\mathbb{K}$.

Définition 1.5. Soit K/k une extension algébrique de corps. Elle est dite *séparable* si pour tout $x \in K$, le polynôme minimal de x sur k est à racines simples dans $\bar{k}$.

Proposition 1.6. En caractéristique nulle, toute extension algébrique est séparable.

Démonstration. Soit K une extension algébrique d'un corps k de caractéristique nulle. Tout polynôme non constant T vérifie $T' \neq 0$. Notamment, soit $x \in K$ et P son polynôme minimal sur k, on a $P' \neq 0$. Alors, toute racine α de P vérifie $P'(\alpha) \neq 0$: Ceci vient du fait que P est le polynôme minimal de α sur k, et que P' est non nul et vérifie $\deg(P') < \deg(P)$. Il vient enfin que α est une racine simple de P. En effet, si on avait $P = (X-\alpha)Q$ pour un certain Q annulant α, alors on aurait :

$$P' = (X-\alpha)Q' + Q, \text{ puis } 0 \neq P'(\alpha) = Q(\alpha) = 0,$$

ce qui est faux. On vient donc de démontrer que P est à racines simples dans $\bar{k}$, donc K est bien séparable.

□

Remarque 1.7. On travaillera dans les sections suivantes avec des extensions finies de $\mathbb{Q}$. Ainsi, d'après la proposition précédente, tout élément sera tel que son polynôme minimal P sur $\mathbb{Q}$ aura $\deg(P)$ racines distinctes dans son corps de décomposition.

Montrons alors les résultats qui concernent concrètement les extensions séparables. D'après la proposition 1.6 et la remarque 1.7, les résultats seront valables pour les extensions que l'on introduira dans les sections suivantes. Commençons par le résultat préliminaire suivant.

Proposition 1.8. Soit k un corps et $x \in \bar{k}$ algébrique tel que son polynôme minimal sur k est à racines simples. Alors, pour tout $\sigma \in \mathrm{Hom}(k, \bar{k})$, il existe $[k(x) : k]$ morphismes $\tilde{\sigma} \in \mathrm{Hom}(k(x), \bar{k})$ qui prolongent σ.

Démonstration. Notons $n = [k(x) : k]$. Notons aussi $P = \sum_{j=0}^{n} \gamma_j X^j$ le polynôme minimal de x sur k. Soit alors $\sigma \in \mathrm{Hom}(k, \bar{k})$. On note à nouveau :

$$\begin{array}{rccc} \overline{\sigma} : & k[X] & \longrightarrow & \bar{k}[X] \\ & \sum_{j\geq 0} a_j X^j & \longmapsto & \sum_{j\geq 0} \sigma(a_j) X^j \end{array}$$

Pour construire les prolongements $\tilde{\sigma} \in \mathrm{Hom}(k(x), \bar{k})$, observons d'abord le polynôme $\overline{\sigma}(P)$. P est à racines simples, donc n'a pas de racine en commun avec P' par le même argument que dans la preuve de la proposition 1.6. Alors, $P \wedge P' = 1$ si bien que :

$$\exists A, B \in k[X],\ AP + BP' = 1$$

Et alors, on obtient une autre relation de Bézout :

$$\overline{\sigma}(A)\overline{\sigma}(P) + \overline{\sigma}(B)\overline{\sigma}(P') = 1 \ \text{ i.e. } \overline{\sigma}(P) \wedge (\overline{\sigma}(P))' = 1$$

car $\overline{\sigma}$ commute avec la dérivée en tant que morphisme. Alors, $\overline{\sigma}(P)$ et $(\overline{\sigma}(P))'$ n'ont pas de racine commune. On vient donc de montrer que $\overline{\sigma}(P)$ admet n racines distinctes que l'on note $x_1, \ldots, x_n$. D'après la proposition 1.4, pour tout $i \in [\![1, n]\!]$, il existe un morphisme $\tilde{\sigma}_i : k(x) \longrightarrow \bar{k}(x_i) = \bar{k}$ tel que :

$$\tilde{\sigma}_i|_k = \sigma \text{ et } \tilde{\sigma}_i(x) = x_i$$

Notamment, les x_i sont distincts donc les n prolongements définis le sont aussi. Réciproquement, pour un tel prolongement $\tilde{\sigma}$, on a :

$$\overline{\sigma}(P)(\tilde{\sigma}(x)) = \sum_{j=0}^{n} \sigma(\gamma_j)\tilde{\sigma}(x)^j = \tilde{\sigma}(\sum_{j=0}^{n} \gamma_j x^j) = \tilde{\sigma}(0) = 0$$

Il existe donc $i \in [\![1, n]\!]$ tel que $\tilde{\sigma}(x) = x_i$. Or, $(1, x, \ldots, x^{n-1})$ étant une k-base de $k(x)$ d'après le rappel 1.2, $\tilde{\sigma}$ est entièrement déterminé par $\tilde{\sigma}(x)$. Il s'ensuit que $\tilde{\sigma} = \tilde{\sigma}_i$. Il y a donc bien exactement n tels prolongements.

□

Corollaire 1.9. Soit K/k une extension séparable de degré n. Alors :

$$|\{\sigma \in \mathrm{Hom}(K, \bar{k}) \mid \forall x \in k, \sigma(x) = x\}| = n$$

Démonstration. Procédons par récurrence sur $n \in \mathbb{N}^*$, on note $\mathcal{P}_n$ cette proposition. D'abord, $\mathcal{P}_1$ est vraie car alors $K = k$ et seul le morphisme identité convient. Soit maintenant $n \geq 2$ tel que $\mathcal{P}_1, \ldots, \mathcal{P}_{n-1}$ sont vraies. Alors, si l'extension K est simple, on obtient le résultat en appliquant la proposition précédente pour $\sigma = \mathrm{Id}$. Sinon, comme K/k est de degré fini n :

$$\exists\ x_1, \ldots, x_n \in K,\ k(x_1, \ldots, x_n) = K$$

Notons de plus $L = k(x_1, \ldots, x_{n-1})$, si bien que :

$$k \subsetneq L \subsetneq K \text{ et } \left\{ \begin{array}{ll} r := [L : k] < n & (*) \\ K = L(x_n) & (**) \end{array} \right.$$

Alors, K/k est séparable donc en particulier L/k l'est aussi, et on peut appliquer l'hypothèse de récurrence d'après $(*)$. Alors, d'après $\mathcal{P}_r$, il existe exactement r morphismes $\sigma_1, \ldots, \sigma_r$ de L dans $\bar{k}$ fixant k.

Par ailleurs, pour tout $x \in K$, le polynôme minimal P de x sur k est dans $L[X]$ et annule x, donc x est algébrique sur L. D'où, son polynôme minimal sur L divise P donc est à racines simples dans $\bar{k}$ car K/k est séparable. Ceci montre que K/L est également séparable. D'après $(**)$, on peut alors appliquer la proposition 1.8, qui affirme que chaque σ_i possède exactement $s := [K : L]$ prolongements distincts. On en conclut que :

$$|\{\sigma \in \mathrm{Hom}(K, \bar{k}) \mid \forall x \in k, \sigma(x) = x\}| \geq rs = n$$

Par ailleurs, si $\sigma \in \mathrm{Hom}(K, \bar{k})$ fixe k, sa restriction à L est l'un des σ_i introduits précédemment d'après $\mathcal{P}_r$, ce qui veut dire que σ est l'un des prolongements des σ_i que l'on a déjà obtenu. Ainsi, $\mathcal{P}_n$ est vraie, ce qui conclut la récurrence et la démonstration.

□

Nous allons pour finir démontrer le théorème dit de *l'élément primitif* dans le cas qui nous intéresse, c'est-à-dire les extensions finies de $\mathbb{Q}$. Pour cela, nous allons avoir besoin d'un lemme d'algèbre linéaire.

Lemme 1.10. Soit E un espace vectoriel sur un corps infini $\mathbb{K}$, et soient $E_1, \ldots, E_n$ des sous-espaces vectoriels strictement inclus dans E. Alors $\bigcup_{i=1}^{n} E_i \neq E$.

Démonstration. On peut supposer $n \geq 2$ car le résultat est tautologique pour $n = 1$. On peut aussi supposer que pour tout $i \in [\![1, n]\!]$, $E_i \nsubseteq \bigcup_{j \neq i} E_j$, on peut en effet toujours se ramener dans ce cas quitte à retirer des ensembles E_i dans l'union. Soit alors $x_1 \in E_1 \setminus E_2 \cup \cdots \cup E_n$ et $x_2 \in E_2 \setminus E_1 \cup E_3 \cup \cdots \cup E_n$. Notons :

$$D = \{tx_1 + (1-t)x_2 \mid t \in \mathbb{K}\} \subset E$$

la droite affine passant par ces deux points. Montrons que pour tout $i \in [\![1, n]\!]$, $E_i \cap D$ est de cardinal au plus 1. Fixons i, et soit par l'absurde $s \neq t$ tels que $a := tx_1 + (1-t)x_2$ et $b := sx_1 + (1-s)x_2$ sont dans E_i. Alors, E_i étant un espace vectoriel, il vient :

$$sa - tb = (s-t)x_2 \in E_i, \text{ puis } x_2 \in E_i$$

car $s \neq t$. De la même façon, $x_1 \in E_i$, ce qui contredit les hypothèses faites sur x_1 et x_2. On en déduit que, comme D est de cardinal infini, il existe un élément dans $D \setminus \bigcup_{i=1}^{n} E_i$, ce qui conclut.

□

Théorème 1.11. Soit K une extension finie de $\mathbb{Q}$. Il existe $\theta \in K$ tel que $K = \mathbb{Q}(\theta)$.

Démonstration. Notons $d = [K : \mathbb{Q}]$, par le corollaire 1.9, il existe d morphismes $\sigma_1, \ldots, \sigma_d$ de K dans $\mathbb{C}$ qui fixent $\mathbb{Q}$. Notons alors $E_{i,j} = \{x \in K \mid \sigma_i(x) = \sigma_j(x)\}$ pour tout $i \neq j$. $E_{i,j}$ est un sous-espace vectoriel strict de K. En effet, $0 \in E_{i,j}$ et pour tout $\lambda \in \mathbb{Q}$ et $x, y \in E_{i,j}$, on a :

$$\sigma_i(\lambda x + y) = \lambda\sigma_i(x) + \sigma_i(y) = \lambda\sigma_j(x) + \sigma_j(y) = \sigma_j(\lambda x + y)$$

donc $\lambda x + y \in E_{i,j}$, et $E_{i,j} \subsetneq K$ car $\sigma_i \neq \sigma_j$. Par le lemme précédent, $\bigcup_{i \neq j} E_{i,j} \subsetneq K$. Ainsi, il existe $\theta \in K$ tel que :

$$\theta \notin \bigcup_{i \neq j} E_{i,j} \quad \text{i.e. } \forall i \neq j,\ \sigma_i(\theta) \neq \sigma_j(\theta)$$

Or, les $\sigma_k(\theta)$ sont racines de μ_θ, qui possède donc au moins d racines distinctes. Alors, d'une part :

$$\dim(\mathbb{Q}(\theta)) = \deg(\mu_\theta) \ \geq \ d = \dim(K).$$

Les égalités viennent du rappel 1.2. D'autre part, on a $\mathbb{Q}(\theta) \subseteq K$, et on obtient finalement $K = \mathbb{Q}(\theta)$.

□

2 Anneaux d'entiers d'un corps de nombres

2.1 Notion d'élément entier

Dans le reste du document, K désignera un corps de nombres c.-à-d. une extension finie du corps des nombres rationnels $\mathbb{Q}$, on notera par la suite $d = [K : \mathbb{Q}]$. Un élément de K est appelé *entier algébrique* s'il est annulé par un polynôme unitaire à coefficients dans $\mathbb{Z}$. L'ensemble des entiers algébriques de K est noté $\mathcal{O}_K$.

Définition 2.1. Un anneau intègre A est dit *intégralement clos* si $\mathcal{O}_{Frac(A)} = A$.

Remarque 2.2. $\mathcal{O}_K$ est en fait toujours un anneau, c'est l'objet du théorème suivant. Ceci offre alors deux points de vue équivalents : chercher un anneau A intégralement clos ou regarder l'anneau $\mathcal{O}_K$ d'un corps K. Le premier point de vue est ce que l'on fera naturellement en pratique. Cependant, on utilisera le second pour établir les résultats théoriques.

Théorème 2.3. *$\mathcal{O}_K$ est un sous-anneau de K.*

Démonstration. Soient $x, y \in \mathcal{O}_K$. Il existe donc $n, m \in \mathbb{N}$ tels que :

$$\begin{cases} x^m = a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \\ y^n = b_{n-1}y^{n-1} + \cdots + b_1 y + b_0 \end{cases} \tag{2}$$

où les a_i et les b_j sont dans $\mathbb{Z}$. Montrons par récurrence forte sur $k \in \mathbb{N}$ la propriété suivante :

$$\mathcal{P}_k : \exists Q \in \mathbb{Z}[X], \begin{cases} x^{m+k} = Q(x) \\ \deg(Q) < m \end{cases}$$

Premièrement, $\mathcal{P}_0$ est vraie d'après (2). Soit maintenant $k \in \mathbb{N}^*$ tel que $\mathcal{P}_0, \ldots, \mathcal{P}_{k-1}$ sont vraies. Encore d'après (2), en multipliant par x^k, on obtient :

$$x^{m+k} = a_{m-1}x^{m+k-1} + \cdots + a_1 x^{k+1} + a_0 x^k$$

Alors, pour $j \in [\![0, k-1]\!]$, il existe Q_j qui vérifie $\mathcal{P}_j$ si bien que :

$$a_{m-1}Q_{k-1}(X) + \cdots + a_1 Q_1(X) + a_0 Q_0(X)$$

est de degré $< m$, dans $\mathbb{Z}[X]$, et vaut x^{m+k} lorsqu'on l'évalue en x. D'où, $\mathcal{P}_k$ est vraie, ce qui conclut la récurrence. On obtient de même le résultat pour y en remplaçant m par n. On vient alors de montrer que $\mathbb{Z}[x, y]$ est le groupe engendré par la famille $\{x^i y^j \mid 0 \leq i \leq m-1, 0 \leq j \leq n-1\}$. Notons alors :

$$u_1 = x^0y^0, u_2 = x^1y^0, \ldots, u_m = x^{m-1}y^0, u_{m+1} = x^0y^1, u_{m+2} = x^1y^1, \ldots, u_r = x^{m-1}y^{n-1}$$

où $r := mn$. Soit de plus $z := x + y, x - y$ ou xy. Pour tout $k \in [\![1; r]\!]$, $zu_k \in \mathbb{Z}[x, y]$ et se décompose donc sous la forme $\sum_{l=1}^{r} \alpha_{lk} u_l$, on note alors :

$$M := zI_r - (\alpha_{ij})^T = \begin{pmatrix} z - \alpha_{11} & \cdots & -\alpha_{r1} \\ \vdots & \ddots & \vdots \\ -\alpha_{1r} & \cdots & z - \alpha_{rr} \end{pmatrix} \text{ et } U := \begin{pmatrix} u_1 \\ \vdots \\ u_r \end{pmatrix}$$

si bien que $MU = 0$. On multiplie à gauche par $\mathrm{Com}(M)^T$ et obtient $det(M)U = 0$ par la pseudo associativité du produit matriciel. Puis, en regardant la première ligne, $\det(M) = 0$, ce qui montre l'existence d'un polynôme unitaire de $\mathbb{Z}[X]$ qui annule z, donc $z \in \mathcal{O}_K$, et ainsi $\mathcal{O}_K$ est bien un anneau.

□

2.2 Propriétés élémentaires de l'anneau $\mathcal{O}_K$

L'anneau $\mathcal{O}_K$ est un *anneau de Dedekind*, dont l'une des propriétés importantes, que l'on montrera dans la section suivante, est l'unicité de la décomposition d'un idéal en produit d'idéaux premiers. Cette propriété généralise donc comme convenu la notion d'anneau factoriel. Dans cette sous-section, nous allons montrer des propriétés élémentaires de l'anneau $\mathcal{O}_K$.

Lemme 2.4. Pour tout $z \in \mathcal{O}_K$, on a $\mu_z \in \mathbb{Z}[X]$.

Démonstration. Par hypothèse, il existe $P \in \mathbb{Z}[X]$ unitaire qui annule z. Alors $\mu_z \mid P$ donc il existe $Q \in \mathbb{Q}[X]$ tel que $\mu_z Q = P$. On introduit $a, b, c, d \in \mathbb{Z}$ tels que :

$$\mu_z = \frac{a}{b}R \text{ et } Q = \frac{c}{d}S$$

où R et S sont des polynômes primitifs (c.-à-d. de contenu 1) dans $\mathbb{Z}[X]$. Alors :

$$acRS = bdP, \text{ puis } ac = bd$$

en passant au contenu qui est multiplicatif, d'où $RS = P$. Ensuite, R,S et P étant dans $\mathbb{Z}[X]$ et P étant unitaire, on peut supposer R et S unitaires (quitte à remplacer R par $-R$). Alors, comme R et μ_z sont proportionnels, on obtient $R = \mu_z$, ce qui conclut.

□

Remarque 2.5. On vient notamment de montrer que $\mathbb{Z}$ est intégralement clos. En effet, pour $a \in \mathbb{Z}$, $X - a$ annule a, donc $\mathbb{Z} \subseteq \mathcal{O}_{\mathbb{Q}}$. Et si $z \in \mathcal{O}_{\mathbb{Q}}$, on a $z \in \mathbb{Q}$ et $X - z = \mu_z \in \mathbb{Z}[X]$ d'après le lemme précédent, donc $z \in \mathbb{Z}$ puis $\mathcal{O}_{\mathbb{Q}} \subseteq \mathbb{Z}$. Avec la même preuve, on obtient plus généralement que tout anneau factoriel est intégralement clos.

Proposition 2.6. $K = \{\frac{z}{\alpha} \in K \mid z \in \mathcal{O}_K,\ \alpha \in \mathbb{Z}^*\}$

Démonstration. Il suffit de démontrer l'inclusion directe. Soit $u \in K$, $(1, u, \ldots, u^d)$ est une famille liée car K est un $\mathbb{Q}$-espace vectoriel de degré d. Il existe donc $a_0, \ldots, a_d$ dans $\mathbb{Z}$ (quitte à multiplier par le ppcm des dénominateurs) tels que :

$$a_k u^k + a_{k-1}u^{k-1} + \cdots + a_0 = 0,$$

où k est le plus grand élément de $[\![0, d]\!]$ tel que $a_k \neq 0$. Posons $v \in K$ tel que $u =: \frac{v}{a_k}$, il reste à montrer que $v \in \mathcal{O}_K$. Or, en multipliant par a_k^{k-1} dans la relation de liaison précédente, on obtient :

$$v^k + a_{k-1}v^{k-1} + a_k a_{k-2}v^{k-2} + \cdots + a_k^{k-1}a_0 = 0.$$

Ce polynôme est bien unitaire et dans $\mathbb{Z}[X]$, ce qui conclut.

□

Définition 2.7. La *norme* d'un élément $z \in K$ est le déterminant de la multiplication par z :

$$N(z) := \det(m_z)$$

Remarquons d'abord que pour tout $P \in \mathbb{Q}[X]$, $P(m_z) = m_{P(z)}$. Notamment, l'ensemble des polynômes annulateurs de z est égal à l'ensemble des polynômes annulateurs de m_z. On en déduit que, d'une part, d'après Cayley-Hamilton, $\chi_{m_z}(z) = 0$, et donc :

$$N(z) = zz_2 \dots z_d, \tag{3}$$

où les z_i sont les autres racines de χ_{m_z} comptées avec multiplicités ; et d'autre part, on a $\mu_{m_z} = \mu_z$.

Remarque 2.8. Si $z \in \mathcal{O}_K$, alors pour tout $i \in [\![2; d]\!]$, $z_i \in \mathcal{O}_K$. En effet, $\mu_z \in \mathbb{Z}[X]$ par le lemme 2.4, est unitaire, et $\mu_z(z_i) = \mu_{m_z}(z_i) = 0$ d'après ce qui précède.

Proposition 2.9. N est multiplicative et, pour tout $z \in \mathcal{O}_K$, $N(z) \in \mathbb{Z}$.

Démonstration. Pour $z, z' \in K$, on a :

$$N(zz') = det(m_{zz'}) = det(m_z \circ m_{z'}) = det(m_z)det(m_{z'}) = N(z)N(z')$$

Concernant le second point, si $z \in \mathcal{O}_K$, $N(z) \in \mathbb{Q}$ car $\chi_{m_z} \in \mathbb{Q}[X]$. De plus, $N(z) \in \mathcal{O}_K$ comme produit d'éléments de $\mathcal{O}_K$ par la remarque 2.8 et le théorème 2.3. Et enfin, $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ d'après la remarque 2.5.

□

Via cet outil, on obtient une caractérisation simple d'utilisation des éléments inversibles de l'anneau $\mathcal{O}_K$.

Proposition 2.10. $\mathcal{O}_K^\times = \{z \in \mathcal{O}_K \mid N(z) = \pm 1\}$

Démonstration. Soit $z \in \mathcal{O}_K^\times$, il existe $z' \in \mathcal{O}_K$ tel que $zz' = 1$. Alors $N(z)N(z') = 1$ puis $N(z) = \pm 1$, d'après la proposition précédente.
Réciproquement, soit $z \in \mathcal{O}_K$ de norme $N(z) = \pm 1$. Par la remarque 2.8 et le théorème 2.3, $Z := z_2 \dots z_d \in \mathcal{O}_K$. D'après (3), Z ou $-Z$ est alors l'inverse de z, donc $z \in \mathcal{O}_K^\times$.

□

2.3 $\mathcal{O}_K$ en tant que groupe additif

Nous allons maintenant voir que le groupe $\mathcal{O}_K$ est un groupe abélien de type fini. On va même pouvoir le situer à isomorphisme près dans la classification. Nous avons pour cela besoin d'un outil préliminaire : le *discriminant* d'une $\mathbb{Q}$-base de K. $K = \mathbb{Q}(\theta)$ pour un certain $\theta \in K$ par le théorème 1.11. Soient $\theta_2, \dots, \theta_d$ les autres racines de μ_θ, et on note $\theta_1 := \theta$. Ces racines sont toutes distinctes par la remarque 1.7. Pour tout $i \in [\![1, d]\!]$, on construit alors :

$$\begin{array}{rccc} \sigma_i : & \mathbb{Q}(\theta) & \xrightarrow{\sim} & \mathbb{C} \\ & \theta & \longmapsto & \theta_i \end{array}$$

l'isomorphisme d'anneaux qui fixe $\mathbb{Q}$ et envoie θ sur θ_i. Ce sont les d prolongements du morphisme identité de la proposition 1.8.

On définit le discriminant d'une base $e = (e_1, \dots, e_d)$ par $\Delta(e) := (\det[(\sigma_i(e_j))_{i,j}])^2$.

Nous allons démontrer un résultat préliminaire. Ce dernier utilise un semblant de théorie sur les polynômes symétriques, notamment le fait que tout polynôme symétrique $P \in \mathbb{Q}[X_1, \dots, X_d]$ peut s'écrire comme un polynôme rationnel en les polynômes symétriques élémentaires $\sigma_1, \dots, \sigma_d$. On rappelle la définition suivante :

$$\forall k \in [\![1, d]\!],\ \sigma_k(X_1, \dots, X_d) = \sum_{1 \leq i_1 < \dots < i_k \leq d} \prod_{j=1}^{k} X_{i_j}$$

On utilisera également les relations de Viète, ou autrement dit les relations coefficients-racines : pour $P = X^d + \sum_{k=0}^{d-1} a_k X^k$ un polynôme unitaire dont on note $x_1, \dots, x_d$ les racines, on a :

$$\forall k \in [\![0, d-1]\!],\ a_k = (-1)^{d-k} \sigma_{d-k}(x_1, \dots, x_d)$$

Nous admettrons ces résultats pour gagner du temps.

Proposition 2.11. Soit $e = (e_1, \dots, e_d)$ une $\mathbb{Q}$-base de K. Alors $\Delta(e) \in \mathbb{Q}^*$. De plus, si $e \subset \mathcal{O}_K$, $\Delta(e) \in \mathbb{Z}^*$.

Démonstration. Remarquons d'abord que pour la base $\mathcal{B} := (1, \theta, \dots, \theta^{d-1})$, on obtient un déterminant de Vandermonde :

$$\Delta(\mathcal{B}) = \begin{vmatrix} 1 & \theta_1 & \dots & \theta_1^{d-1} \\ 1 & \theta_2 & \dots & \theta_2^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_d & \dots & \theta_d^{d-1} \end{vmatrix}^2 = \prod_{i<j} (\theta_i - \theta_j)^2 =: P(\theta_1, \dots, \theta_d) \text{ avec } P \in \mathbb{Q}[X_1, \dots, X_d]$$

Par antisymétrie du déterminant, et comme on s'intéresse à son carré, $\Delta(\mathcal{B})$ est invariant par permutation des θ_i. Donc, P est un polynôme symétrique. Par le théorème fondamental des polynômes symétriques, il existe un polynôme $Q \in \mathbb{Q}[X_1, \dots, X_d]$ tel que :

$$P(X_1, \dots, X_d) = Q(\sigma_1(X_1, \dots, X_d), \dots, \sigma_d(X_1, \dots, X_d))$$

Or, comme les coefficients de μ_θ sont dans $\mathbb{Q}$, on a $\sigma_1(\theta_1, \dots, \theta_d), \dots, \sigma_d(\theta_1, \dots, \theta_d) \in \mathbb{Q}$ par les relations de Viète. Ainsi :

$$\Delta(\mathcal{B}) = Q(\sigma_1(\theta_1, \dots, \theta_d), \dots, \sigma_d(\theta_1, \dots, \theta_d)) \in \mathbb{Q}.$$

De plus, ce discriminant est non nul car les θ_i sont distincts.

Soit maintenant $e = (e_1, \dots, e_d)$ une $\mathbb{Q}$-base quelconque de K. Pour tout $j \in [\![1, d]\!]$, notons $e_j = \sum_{k=1}^{d} \alpha_{kj} \theta^k$ sa décomposition dans la base $\mathcal{B}$. Notons de plus $M = (\alpha_{ij})_{i,j}$ la matrice de e dans la base $\mathcal{B}$. Notons enfin :

$$A = (\sigma_i(e_j))_{i,j} \text{ et } B = (\sigma_i(\theta^j))_{i,j}\ ,$$

on vérifie alors que $A = MB$. En effet, comme les σ_i fixent $\mathbb{Q}$:

$$\forall i, j \in [\![1, d]\!],\ \sigma_i(e_j) = \sum_{k=1}^{d} \alpha_{kj} \sigma_i(\theta)^k = \sum_{k=1}^{d} \alpha_{kj} \theta_i^k\ ,$$

il vient alors :

$$\Delta(e) = \det(A)^2 = \det(M)^2 \det(B)^2 = \det(M)^2 \Delta(\mathcal{B}) \in \mathbb{Q}^*$$

En outre, si $e \subset \mathcal{O}_K$, $\sigma_i(e_j) \in \mathcal{O}_K$ pour tout $i, j \in [\![1, d]\!]$ car $e_i \in \mathcal{O}_K$ et car :

$$\forall P \in \mathbb{Z}[X],\ \sigma_j(P(e_i)) = P(\sigma_j(e_i)).$$

Ainsi, le discriminant étant polynomial en les $\sigma_j(e_i)$, il vient $\Delta(e) \in \mathcal{O}_K$, et alors $\Delta(e) \in \mathcal{O}_K \cap \mathbb{Q}^* = \mathbb{Z}^*$ par la remarque 2.5.

□

Théorème 2.12. $\mathcal{O}_K \simeq \mathbb{Z}^d$ en tant que groupe additif.

Démonstration. Soit $e = (e_1, \ldots, e_d)$ une $\mathbb{Q}$-base de K incluse dans $\mathcal{O}_K$, ce qui est possible par la proposition 2.6. On choisit e telle que $|\Delta(e)|$ soit minimale, ce qui a du sens d'après la proposition précédente. Alors, d'une part, e est $\mathbb{Z}$-libre car $\mathbb{Q}$-libre. Et, d'autre part, e est $\mathbb{Z}$-génératrice. En effet, montrons que pour tout $z \in \mathcal{O}_K$:

$$z = \lambda_1 e_1 + \cdots + \lambda_d e_d \Longrightarrow \lambda_1, \ldots, \lambda_d \in \mathbb{Z}.$$

Il suffit de montrer que $\lambda_1 \in \mathbb{Z}$ par symétrie, et même $\lambda_1 = 0$ en se restreignant à $[0, 1[$ quitte à remplacer z par $z - \lfloor \lambda_1 \rfloor e_1$.

Si par l'absurde $\lambda_1 \neq 0$, $(z, e_2, \ldots, e_d)$ s'écrit de façon triangulaire dans la base e, avec des coefficients diagonaux non nuls. C'est donc une $\mathbb{Q}$-base de K incluse dans $\mathcal{O}_K$, et en faisant des opérations sur les colonnes, il vient :

$$\begin{aligned}
\Delta(z, e_2, \ldots, e_d) &= \begin{vmatrix} \sum_{i=1}^d \lambda_i e_i & e_2 & \ldots & e_d \\ \sum_{i=1}^d \lambda_i \sigma_2(e_i) & \sigma_2(e_2) & \ldots & \sigma_2(e_d) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^d \lambda_i \sigma_d(e_i) & \sigma_d(e_2) & \ldots & \sigma_d(e_d) \end{vmatrix}^2 \\
&= \begin{vmatrix} \lambda_1 e_1 & e_2 & \ldots & e_d \\ \lambda_1 \sigma_2(e_1) & \sigma_2(e_2) & \ldots & \sigma_2(e_d) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1 \sigma_d(e_1) & \sigma_d(e_2) & \ldots & \sigma_d(e_d) \end{vmatrix}^2 \\
&= \lambda_1^2 \Delta(e)
\end{aligned}$$

si bien que :

$$|\Delta(z, e_2, \ldots, e_d)| = \lambda_1^2 |\Delta(e)| < |\Delta(e)|$$

ce qui contredit l'hypothèse de minimalité. Ceci permet alors de conclure que e est une $\mathbb{Z}$-base de $\mathcal{O}_K$, d'où l'isomorphisme voulu.

□

Remarque 2.13. Un *A-module* sur un anneau commutatif unitaire A est la généralisation de la notion d'espace vectoriel sur un corps (on adapte naïvement les axiomes). Le terme $\mathbb{Z}$-*base* utilisé dans la preuve précédente est alors naturel si l'on adopte ce point de vue : on a en fait $\mathcal{O}_K \simeq \mathbb{Z}^d$ en tant que $\mathbb{Z}$-module.

2.4 Propriétés des idéaux de $\mathcal{O}_K$

Nous allons dans cette sous-partie montrer des propriétés des idéaux de $\mathcal{O}_K$, ces dernières vont préparer le terrain pour démontrer les résultats principaux sur l'anneau $\mathcal{O}_K$.

Remarque 2.14. La proposition suivante est un résultat clef pour pouvoir travailler correctement avec les idéaux de $\mathcal{O}_K$. Il repose majoritairement sur le théorème de la base adaptée dans le cadre des $\mathbb{Z}$-modules. Ce théorème est loin d'être une généralisation évidente du résultat analogue en théorie des espaces vectoriels, et on l'admettra donc pour poursuivre. On prendra le temps en annexe d'expliciter davantage ce résultat.

Proposition 2.15. Soit $(e_1, \dots, e_d)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$. Pour tout idéal non nul I de $\mathcal{O}_K$, il existe $a_1, \dots, a_d \in \mathbb{N}^*$ tels que $(a_1e_1, ..., a_de_d)$ soit une $\mathbb{Z}$-base de I.

Démonstration. Soit $I \lhd \mathcal{O}_K$ non nul, d'après la remarque précédente et le théorème A.5 de l'annexe, il existe $k \leq d$ et $a_1, \dots, a_k \in \mathbb{Z}^*$ tels que $(a_1e_1, \dots, a_ke_k)$ soit une base de I. Complétons cette base en une famille génératrice de I $(a_1e_1, \dots, a_de_d)$, ceci est toujours faisable quitte à compléter par des zéros. Montrons alors qu'aucun des a_j n'est nul. Si $a_j = 0$, alors :

$$\lambda e_j \in I \;\Rightarrow\; \lambda = 0$$

En effet, $(a_1e_1, \dots, a_de_d)$ est génératrice donc λe_j s'écrit $\sum_{i\neq j} \lambda_i a_i e_i$ si bien que

$$\lambda e_j - \sum_{i\neq j} \lambda_i a_i e_i = 0 \ , \text{ puis } \lambda = \lambda_1 a_1 = \cdots = 0$$

par liberté de $(e_1, \dots, e_d)$. Or, pour tout $f \in I \setminus \{0\}$, il existe $z \in \mathcal{O}_K$ et $a \in \mathbb{Z}^*$ tels que :

$$\frac{e_j}{f} = \frac{z}{a}$$

par la proposition 2.6. Alors $ae_j = fz \in I$ avec $a \neq 0$. Un tel a_j nul ne peut donc pas exister. Ceci permet de montrer que $(a_1e_1, \dots, a_de_d)$ est libre. En effet, soient $\lambda_1, \dots, \lambda_d \in \mathbb{Z}$ tels que :

$$\sum_{i=1}^{d} \lambda_i a_i e_i = 0.$$

Par liberté de $(e_1, \dots, e_d)$, il vient :

$$\forall i \in [\![1, d]\!], \lambda_i a_i = 0.$$

Puis comme les a_i sont tous non nuls, les λ_i sont nécessairement tous nuls. Finalement, $(a_1e_1, \dots, a_de_d)$ est bien une base de I.

Remarquons en outre qu'on peut choisir les a_i dans $\mathbb{N}$. En effet, si $(a_1e_1, \dots, a_de_d)$ est génératrice, $(|a_1|e_1, \dots, |a_d|e_d)$ est encore une famille $\mathbb{Z}$-génératrice de I. On peut donc appliquer ce qui précède pour montrer que c'est une base.

□

Définition 2.16. On appelle alors *norme* de I l'entier suivant :

$$N(I) := |\mathcal{O}_K/I| = \prod_{i=1}^{d} a_i$$

Remarque 2.17. La principale surprise dans la définition précédente est le fait que ce cardinal est fini. Ceci provient de l'isomorphisme suivant qui découle de la proposition 2.15 :

$$\begin{array}{ccc} \mathcal{O}_K/I & \xrightarrow{\sim} & \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_d\mathbb{Z} \\ \sum_i x_i e_i & \longmapsto & (x_1 + a_1\mathbb{Z}, \ldots, x_d + a_d\mathbb{Z}) \end{array}$$

Corollaire 2.18. Tout idéal premier non nul de $\mathcal{O}_K$ est maximal.

Démonstration. Soit $I \lhd \mathcal{O}_K$ premier non nul. Alors $\mathcal{O}_K/I$ est un anneau (unitaire) intègre, et fini d'après ce qui précède. Il suffit de montrer que cet anneau A est un corps. En effet, pour tout $a \in A^*$, $m_a : A \longrightarrow A$ est une application injective par intégrité de A. Elle est donc bijective par finitude de A. Ainsi, 1_A possède en particulier un antécédent x par m_a c'est-à-dire $ax = 1$ soit encore $a \in A^\times$. A est ainsi bien un corps.

□

Remarque 2.19. Pour la preuve suivante, nous avons besoin de faire quelques observations : on peut définir, de la même façon que l'on définit les applications linéaires, la notion de morphisme de $\mathbb{Z}$-modules. Notamment, un isomorphisme ψ est uniquement déterminé par son image sur une base.

De plus, ces bases que l'on considérera seront des bases de l'espace vectoriel K, en tant que familles $\mathbb{Q}$-libres de d éléments, si bien que ψ peut être vu comme un automorphisme de $\mathbb{Q}$-espace vectoriel sur le corps K. Cela permet de considérer le déterminant de ψ.

Proposition 2.20. Pour tout $\alpha \in \mathcal{O}_K$, $|N((\alpha))| = |N(\alpha)|$.

Démonstration. Notons $I = (\alpha)$. En plus de la base $(a_1e_1, \ldots, a_de_d)$, on dispose d'une seconde base de I qui est $(\alpha e_1, \ldots, \alpha e_d)$. D'après la remarque précédente, $m_\alpha : \mathcal{O}_K \longrightarrow I$, défini par $m_\alpha(e_i) = \alpha e_i$ pour tout $i \in [\![1, d]\!]$, est bien un isomorphisme de $\mathbb{Z}$-modules. Soit de plus ϕ l'isomorphisme défini par : $\phi(e_i) = a_ie_i$ pour tout $i \in [\![1, d]\!]$. Considérons alors le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{m_\alpha} & I \\ {\scriptstyle \mathrm{Id}}\downarrow & & \downarrow{\scriptstyle \gamma} \\ \mathcal{O}_K & \xrightarrow[\phi]{} & I \end{array}$$

où $\mathcal{O}_K$ est envoyé sur lui-même via Id et où l'on s'intéresse à l'automorphisme de I noté $\gamma := \phi \circ m_\alpha^{-1}$. Notons alors M la matrice de γ dans la base $(a_1e_1, \ldots, a_de_d)$. M est inversible dans $\mathcal{M}_d(\mathbb{Z})$, il existe donc $M' \in \mathcal{M}_d(\mathbb{Z})$ tel que $MM' = I_d$. D'où, $\det(MM') = \det(M)\det(M') = 1$ si bien que, comme $\det(M)$ et $\det(M')$ sont dans $\mathbb{Z}$, il vient $\det(M) = \pm 1$. Donc $|\det(M)| = 1$ c.-à-d. $|\det(m_\alpha)| = |\det(\phi)|$. Ainsi :

$$|N(\alpha)| = |det(m_\alpha)| = |det(\phi)| = |a_1 \ldots a_d| = |N(I)|.$$

□

3 Principaux théorèmes

3.1 Remarques préliminaires

Les idéaux sont historiquement introduits par Kummer sous le titre de "nombres idéaux". Ces derniers sont construits dans le but de généraliser la factorisation unique des anneaux factoriels. L'analogie entre les nombres entiers et les idéaux, pour ce qui est de leurs propriétés arithmétiques, est alors assez logique.

Elle est assez visuelle lorsqu'on regarde les idéaux principaux. Avec l'adage "*diviser* pour les nombres, c'est *contenir* pour les idéaux", on obtient l'équivalence :

$$a \mid b \iff b \in (a)$$

Mais cet adage fonctionne bien au delà. Ainsi, en procédant à ce travail de traduction des nombres vers les idéaux, on retrouve des équivalents de résultats fondamentaux d'arithmétique élémentaire.

Exemples 3.1. Soient $A,\ B,\ C$ des idéaux de $\mathcal{O}_K$, et P un idéal premier de $\mathcal{O}_K$:

Si $A \supset BC$ et $A + B = \mathcal{O}_K$, alors, pour tout $c \in C$, $bc \in A$. Et, d'autre part, il existe $a \in A, b \in B$ tels que $a + b = 1$. Donc $c = (a + b)c = ac + bc \in A$ et ainsi $A \supset C$. On vient de montrer l'analogue du *Lemme de Gauss*.

On en déduit que si $P \supset BC$, alors soit $P + B = P$ auquel cas $P \supset B$; soit $P + B \neq P$ et alors par maximalité de P, on a $P + B = \mathcal{O}_K$ puis $P \supset C$ par le "Lemme de Gauss". C'est donc l'analogue du *Lemme d'Euclide*.

Corollaire 3.2. Dans $\mathcal{O}_K$, si un idéal premier contient un produit d'idéaux maximaux, alors il est égal à l'un d'entre eux.

Démonstration. Si $P \supset Q_1 \dots Q_s$ des idéaux maximaux, alors par le "Lemme d'Euclide", P contient l'un des Q_j, puis par maximalité de Q_j, on a $P = Q_j$.

□

3.2 Décomposition en idéaux premiers

La preuve est analogue à la preuve millénaire concernant la décomposition d'un entier en nombres premiers, au sens de l'analogie développée dans la sous-section précédente. La plus grosse difficulté consiste à simuler la notion de simplification qui existe dans un anneau intègre comme $\mathbb{Z}$. Pour cela, nous allons introduire une notion qui sert d'inverse multiplicatif aux idéaux.

Définition 3.3. On appelle *idéal fractionnaire* de $\mathcal{O}_K$ tout sous-groupe additif M de K, stable par multiplication par un élément de $\mathcal{O}_K$, et tel que : $\exists x \in \mathcal{O}_K^*,\ xM \subset \mathcal{O}_K$.

Proposition 3.4. Pour tout $P \lhd \mathcal{O}_K$ premier non nul, $P' := \{x \in K \mid xP \subset \mathcal{O}_K\}$ est un idéal fractionnaire.

Démonstration. Pour $x, y \in P', (x - y)P = xP - yP \subset \mathcal{O}_K$ donc P' est un sous-groupe additif de K. Pour $\alpha \in \mathcal{O}_K$, $\alpha xP \subset \alpha\mathcal{O}_K \subset \mathcal{O}_K$ donc $\alpha x \in P'$. Enfin, soit $z \in P$ non nul, $zP' = P'z \subset \mathcal{O}_K$ par définition de P'.

□

Ce P' va jouer le rôle d'inverse multiplicatif pour P. Pour montrer cela, nous avons besoin d'une proposition préliminaire. Cette dernière amorce en parallèle la preuve de la décomposition en idéaux premiers.

Proposition 3.5. Tout idéal non nul de $\mathcal{O}_K$ contient un produit d'idéaux maximaux.

Démonstration. Soit par l'absurde un idéal $I \neq \{0\}$ ne vérifiant pas cette propriété $(*)$, on le prend de norme minimale parmi les idéaux ne vérifiant pas $(*)$. I n'est en particulier pas premier, donc il existe $x, y \notin I$ tel que $xy \in I$. Par définition de la norme, $N((x)+I)$ et $N((y)+I) < N(I)$. Par minimalité de $N(I)$, $(x)+I$ et $(y)+I$ contiennent un produit d'idéaux maximaux, donc I également car $I \supseteq ((x)+I)((y)+I)$, ce qui contredit l'hypothèse de départ sur I. Ainsi, tout idéal non nul de $\mathcal{O}_K$ vérifie $(*)$.

□

Lemme 3.6. Pour tout idéal premier P de $\mathcal{O}_K$ non nul, $PP' = \mathcal{O}_K$.

Démonstration. Pour tout $x \in P \setminus \{0\}$, d'après la proposition précédente pour (x), $P \supset (x) \supset P_1 \dots P_r$ où r est minimal tel que $(*)$ soit vérifiée. D'une part, d'après le corollaire 3.2, P est égal à l'un des P_j, on supposera sans perte de généralités que $j = 1$. D'autre part, par minimalité de r, $(x) \not\supseteq P_2 \dots P_r$. Soit alors $y \in P_2 \dots P_r$ tel que $y \notin (x)$ i.e. $\frac{y}{x} \notin \mathcal{O}_K$. Alors $\frac{y}{x} \in P'$ car $yP = yP_1 \subset P_1 \dots P_r \subset (x)$.

On vient de montrer que $\mathcal{O}_K \subsetneq P'$, en effet $\mathcal{O}_K \subset P'$ par définition de P'. Soit alors $z \in P'$ tel que $z \notin \mathcal{O}_K$. $P \subset P + zP \subset \mathcal{O}_K$, et comme P est maximal, $P + zP = P$ ou $\mathcal{O}_K$. Si $P + zP = P$, on a $zP \subset P$. En considérant alors $m_z : P \longrightarrow P$, on a un endomorphisme et χ_{m_z} annule z, ce qui est impossible car $z \notin \mathcal{O}_K$. D'où $P'P \supset zP + P \supset \mathcal{O}_K$, d'où l'égalité par définition de P'.

□

Théorème 3.7. Tout idéal I non nul de $\mathcal{O}_K$ se décompose en un produit d'idéaux premiers. Cette décomposition est unique à l'ordre près des facteurs.

Démonstration. Supposons qu'il existe deux décompositions en idéaux premiers i.e.

$$P_1 \dots P_s = Q_1 \dots Q_t \tag{4}$$

où $s \leq t$. Alors, $P_1 \supset Q_1 \dots Q_t$, et par le corollaire 3.2, on peut supposer $P_1 = Q_1$. Le lemme 3.6 permet de simplifier dans (4), et alors $P_2 \dots P_s = Q_2 \dots Q_t$. En itérant le raisonnement, il vient $P_s = Q_s \dots Q_t$. Finalement, $P_s \supset Q_s \dots Q_t$, donc on suppose encore par le corollaire 3.2 que $P_s = Q_s$. Ainsi, on obtient $s = t$, et ceci conclut la partie *unicité.*

Tout I non nul contient un produit de r idéaux maximaux d'après la proposition 3.5, on prend r minimal comme dans la preuve du lemme précédent. Notons $\mathcal{P}_n$: "Si $J \lhd \mathcal{O}_K$ contient un produit de n idéaux maximaux avec n minimal, alors la décomposition en idéaux premiers existe". Premièrement, $\mathcal{P}_1$ est vraie car si $J \supset P_1$ maximal, $J = P_1$ ou $\mathcal{O}_K$. Supposons maintenant $\mathcal{P}_{n-1}$ vraie pour $n \geq 2$. Soit J contenant $P_1 \dots P_n$ avec n minimal. J est par ailleurs contenu dans un idéal maximal P. Ainsi $P \supset J \supset P_1 \dots P_n$ si bien que :

$$\mathcal{O}_K = P'P \supset P'J \supset P'P_1P_2 \dots P_n = P_2 \dots P_n$$

On peut en effet supposer $P = P_1$ comme précédemment. De $P'J \supset P_2 \dots P_n$, on déduit par $\mathcal{P}_{n-1}$ qu'il existe une décomposition en idéaux premiers $P'J = Q_1 \dots Q_s$. Et alors $J = PQ_1 \dots Q_s$, d'où $\mathcal{P}_n$. Notamment, $\mathcal{P}_r$ est vraie, ce qui implique l'existence de la décomposition pour I. Ceci conclut la partie *existence* et ainsi la démonstration

□

Corollaire 3.8. N est multiplicative pour les idéaux i.e :

$$\forall I, J \lhd \mathcal{O}_K,\ N(IJ) = N(I)N(J)$$

Démonstration. Par la décomposition du théorème précédent. Il suffit de montrer que $N(IP) = N(I)N(P)$ où I est quelconque et P est premier ; i.e. $|\mathcal{O}_K/IP| = |\mathcal{O}_K/I||\mathcal{O}_K/P|$ i.e. $|I/IP| = |\mathcal{O}_K/P|$ par le troisième théorème d'isomorphisme. Or, I/IP est un $\mathcal{O}_K/P$-e.v., on cherche donc à montrer qu'il est de dimension 1 i.e. qu'il existe $x \in I \setminus IP$ tel que $(x) + IP = I$.

$IP \subsetneq I$ donc un tel x existe. En effet, notons $I = Q_1 \dots Q_s$ sa décomposition en idéaux premiers, I et IP ont deux décompositions différentes donc sont différents par unicité de la décomposition. Alors, $IP \subsetneq (x) + IP \subset I$ i.e. $Q_1 \dots Q_s P \subsetneq (x) + IP \subset Q_1 \dots Q_s$. Donc $(x) + IP = I$ par maximalité de P, ce qui conclut.

□

3.3 Construction de $Cl(\mathcal{O}_K)$

Nous avons besoin d'un second résultat majeur. L'idée est d'introduire une mesure du défaut de principalité de l'anneau $\mathcal{O}_K$. Soit $\mathcal{I}$ l'ensemble des idéaux non nuls de $\mathcal{O}_K$. On considère une relation d'équivalence sur $\mathcal{I}$:

$$I \sim J \iff \exists \alpha, \beta \in K^*,\ \alpha I = \beta J.$$

On remarque alors que la classe de l'idéal $\mathcal{O}_K$ est l'ensemble des idéaux principaux, si bien que $|\mathcal{I}/\sim| = 1$ lorsque l'anneau est principal. On obtient effectivement notre mesure : Intuitivement, plus $|\mathcal{I}/\sim|$ est grand, plus l'anneau est "loin" d'être principal, et plus on aura de chances de tomber sur un os le moment venu.

Remarque 3.9. La multiplication des idéaux passe à la relation d'équivalence, si bien que l'ensemble $\mathcal{I}/\sim$ est muni d'une structure de *monoïde*. Autrement dit, si on avait la possibilité de trouver un inverse à tout élément de $\mathcal{I}/\sim$, cela en ferait un groupe. C'est cette volonté qui justifie l'initiative suivante : on prolonge la relation d'équivalence aux idéaux fractionnaires, sans modifier les classes elles-mêmes. En effet, tout idéal fractionnaire M vérifie :

$$\exists x \in \mathcal{O}_K^*,\ xM \subset \mathcal{O}_K.\ \text{Et alors, } xM \lhd \mathcal{O}_K$$

ce qui fait que M est dans une des classes de $\mathcal{I}/\sim$ une fois la relation $\sim$ prolongée.

Définition 3.10. On obtient alors un groupe appelé le *groupe des classes d'idéaux de* $\mathcal{O}_K$, que l'on note $Cl(\mathcal{O}_K)$.

Finissons cette sous-section en motivant un peu notre démarche. Dans les théorèmes qui précèdent, nous avons remplacé les nombres par les idéaux. Ainsi, lorsque nous allons appliquer la théorie pour résoudre des équations diophantiennes, il arrivera le moment, par analogie avec la sous-section 1.2, où on tombera sur : "cet idéal principal J est donc un cube" c'est-à-dire qu'il existe un idéal I vérifiant $J = I^3$. De cela, on obtient que I^3 est principal, mais pour revenir aux nombres et introduire une paramétrisation, nous avons besoin que I soit lui même principal.

C'est le passage clef : cet obstacle justifie à lui seul l'existence de $Cl(\mathcal{O}_K)$. En effet, dans ce groupe, I est principal signifie $\overline{I} = \overline{\mathcal{O}}_K$. Ainsi, on aimerait avoir deux choses. Premièrement, si $Cl(\mathcal{O}_K)$ était fini, on pourrait trouver un entier $n \in \mathbb{N}^*$ tel que $\overline{I}^n = \overline{\mathcal{O}}_K$ par le Théorème de Lagrange. Ce point est l'objet de la sous-section suivante. Deuxièmement, si n était premier avec 3, il existerait une décomposition dans $\mathbb{Z}$ telle que $nu + 3v = 1$. Cela donnerait un argument permettant de sauter l'obstacle clef mentionné plus tôt, on aurait en effet :

$$\overline{I} = \overline{I}^{nu+3v} = (\overline{I}^n)^u(\overline{I}^3)^v = (\overline{\mathcal{O}}_K)^u(\overline{\mathcal{O}}_K)^v = \overline{\mathcal{O}}_K.$$

Ce second point explique l'introduction du concept des nombres *réguliers*, dont le sens exact varie pour chaque équation, on précisera donc au cas par cas. Cependant, l'idée est d'appeler cas réguliers les cas où on obtient cette relation de Bézout et où l'on peut donc conclure.

3.4 Finitude du groupe des classes d'idéaux

On cherche alors à montrer que le groupe construit plus haut est fini. L'idée est la suivante : on admet que l'anneau $\mathcal{O}_K$ est non factoriel lorsque $Cl(\mathcal{O}_K)$ est non trivial, et donc a fortiori $\mathcal{O}_K$ est non principal. Mais, l'anneau garde une propriété similaire, une certaine pseudo-principalité. Pour démontrer ceci, nous avons besoin d'introduire la notion de *pseudo division euclidienne*. Cette démarche n'est pas sans rappeler la méthode courante qui, pour montrer qu'un anneau est principal, consiste à montrer qu'il est en fait euclidien.

Lemme 3.11. Il existe $M \in \mathbb{N}^*$ tel que : $\forall \alpha, \beta \in \mathcal{O}_K \ \beta \neq 0$,

$$\exists t \in [\![1; M]\!], \exists \omega \in \mathcal{O}_K, |N(t\alpha - \omega\beta)| < |N(\beta)|$$

Démonstration. Remarquons d'abord que pour $z = \sum_{i=1}^d \lambda_i e_i \in K$, $|N(z)|$ s'écrit $P(\lambda_1, \ldots, \lambda_d)$ où P est un polynôme homogène de degré d indépendant de z. Donc il existe une constante C telle que : $|N(z)| \leq \text{Max}(|\lambda_i|)^d C$ (C ne dépend que de P, donc de K). Posons alors $M = \lceil C^{\frac{1}{d}} \rceil^d$.

Ensuite, z s'écrit $\lfloor z \rfloor + r_z$ où $\lfloor z \rfloor := \sum_{i=1}^d \lfloor \lambda_i \rfloor e_i \in \mathcal{O}_K$. Posons alors $\gamma = \frac{\alpha}{\beta} \in K$, et :

$$\begin{array}{rccc} f: & [\![0; M]\!] & \longrightarrow & \mathcal{O}_K \\ & k & \longmapsto & k\gamma - \lfloor k\gamma \rfloor \end{array}$$

si bien que les μ_i sont dans $[0, 1[$, où $\sum_{i=1}^d \mu_i e_i := f(k)$. On subdivise alors $[0, 1[^d$ en M cubes de même taille, ceci est possible car M s'écrit n^d avec $n \in \mathbb{N}^*$. Les cubes sont donc chacun de côté $1/n$. Pour obtenir des images assez proches dans le maillage, on cherche $k' > k$ deux entiers tels que $f(k)$ et $f(k')$ soient dans le même sous-cube. Ces entiers existent bien par le Principe des tiroirs, car on envoie $M + 1$ éléments dans M sous-cubes.

Notons alors $\sum_{i=1}^{d} \nu_i e_i := f(k') - f(k)$. Les $|\nu_i|$ sont dans $[0, 1/n[$, si bien que :

$$|N(f(k') - f(k))| \leq \text{Max}(|\nu_i|)^d C < \left(\frac{1}{n}\right)^d C = \frac{C}{M}$$

Enfin, posons $t = k' - k \in [\![1; M]\!]$ et $\omega = \lfloor k'\gamma \rfloor - \lfloor k\gamma \rfloor \in \mathcal{O}_K$. On conclut :

$$|N(t\alpha - \omega\beta)| = |N(t\gamma - \omega)||N(\beta)| = |N(f(k') - f(k))||N(\beta)| < \frac{C}{M}|N(\beta)| \leq |N(\beta)|$$

□

Théorème 3.12. Le groupe $Cl(\mathcal{O}_K)$ est fini.

Démonstration. On utilise la bijection suivante :

$$X := \{J \lhd \mathcal{O}_K \mid J \supset (M!)\} \xrightarrow{\sim} \{\bar{J} \lhd \mathcal{O}_K/(M!)\} =: Y$$

En effet, soit $\pi : \mathcal{O}_K \longrightarrow \mathcal{O}_K/(M!)$ le morphisme quotient. D'abord, pour tout $\bar{J} \in Y$, $\pi^{-1}(\bar{J}) =: I$ est un idéal de $\mathcal{O}_K$, et : $\forall m \in (M!),\ \pi(m) = \bar{0} \in \bar{J}$ i.e. $m \in I$. D'où, $I \in X$, et par surjectivité de π, $\pi(I) = \bar{J}$. Deuxièmement :

$$\forall I, I' \in X,\ \pi(I) = \pi(I') \implies \pi(I - I') = \{\bar{0}\} \implies I - I' \subset (M!),$$

or, I et I' contiennent $(M!)$, ceci implique alors :

$$I - I' = (M!) \implies I = I' + (M!) = I'.$$

Donc π induit bien une bijection entre X et Y.

Ainsi, comme $\mathcal{O}_K/(M!)$ est un anneau fini, Y et ainsi X sont également finis. On cherche alors à montrer que tout idéal non nul I de $\mathcal{O}_K$ est équivalent à un élément de X.

Soit $\beta \in I$ non nul tel que $|N(\beta)|$ soit minimale. Par le lemme précédent, pour tout $\alpha \in I$, il existe $t \in [\![1, M]\!]$ et $\omega \in \mathcal{O}_K$ tels que $z := t\alpha - \omega\beta$ vérifie $|N(z)| < |N(\beta)|$. Par minimalité de β et le fait que $z \in I$, $z = 0$, i.e. $t\alpha = \omega\beta$. Ainsi :

$$\forall \alpha \in I, M!\alpha \in (\beta)\ ;\ \text{donc } J := \frac{M!}{\beta} I$$

est un idéal de $\mathcal{O}_K$. Il est de plus équivalent à I. Et enfin, $M! = M!\frac{\beta}{\beta} \in J$ donc $J \in X$.

□

3.5 Méthode pour le calcul de $|Cl(\mathcal{O}_K)|$

Lorsque $[K : \mathbb{Q}] = 2$, il existe une méthode permettant de calculer efficacement le cardinal de $Cl(\mathcal{O}_K)$. Gauss a montré les résultats qui vont suivre en 1801, dans les *Disquisitiones Arithmeticae*. On peut noter que la notion d'idéal n'existait pas, Gauss raisonnait avec la nomenclature de l'époque.

Considérons $\Delta \in \mathbb{Z}^*_-$ sans facteur carré et $Q = X^2 - TX + D \in \mathbb{Z}[X]$ de discriminant Δ. Soit également :

$$\alpha = \frac{T + \sqrt{\Delta}}{2},\ \text{si bien que } Q(\alpha) = 0.$$

On obtient alors les correspondances suivantes :

$$Cl(\mathbb{Z}[\alpha]) \xrightarrow{\sim} \mathcal{M}_Q(\mathbb{Z})/SL_2(\mathbb{Z}) \xrightarrow{\sim} \mathcal{Q}_\Delta/SL_2(\mathbb{Z})$$

où l'on a posé d'une part :

$$\mathcal{M}_Q(\mathbb{Z}) = \{A \in \mathcal{M}_2(\mathbb{Z}) \mid \chi_A = Q\}$$

et d'autre part :

$$\begin{aligned}\mathcal{Q}_\Delta &= \{ax^2 + bxy + cy^2 \mid (a,b,c) \in \mathbb{Z}^3,\ b^2 - 4ac = \Delta\} \\ &\simeq \left\{ S_q = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \,\middle|\, \det(S_q) = -\frac{\Delta}{4} \right\}\end{aligned}$$

L'ensemble $\mathcal{M}_Q(\mathbb{Z})/SL_2(\mathbb{Z})$ fournit des bijections intermédiaires plus élémentaires, qui permettent de construire la bijection entre ce groupe des classes d'idéaux et ces classes de formes quadratiques. L'intérêt est que $|\mathcal{Q}_\Delta/SL_2(\mathbb{Z})|$ est calculable de façon assez élémentaire, via une approche étroitement liée au Pivot de Gauss.

Cette démarche consistant à compter des objets algébriques ou géométriques représentant les classes d'idéaux s'est avérée très prolifique, si bien qu'aujourd'hui, cette idée se généralise à des extensions de degré supérieur.

4 Première application : résolution de l'équation de Bachet

4.1 Résultats préliminaires

L'objectif de cette section est d'appliquer la théorie développée jusqu'à présent à un premier exemple simple. On cherche à résoudre les équations diophantiennes dites de *Bachet*. Concrètement, on fixe $d \in \mathbb{N}^*$, et on cherche les couples entiers qui vérifient :

$$x^3 = y^2 + d$$

On dira alors que (x, y) est une solution de l'équation de Bachet associée à d. On ne sait malheureusement pas résoudre une telle équation dans le cas général. Cependant, lorsque d vérifie des propriétés adaptées à notre arsenal, nous saurons énumérer les solutions efficacement. Regardons alors l'anneau $\mathbb{Z}[i\sqrt{d}]$ et ses propriétés, car c'est dans cet anneau que l'on travaillera.

Proposition 4.1. Soit $d \in \mathbb{N}^*$ sans facteur carré. Alors :

$$\mathcal{O}_{\mathbb{Q}(i\sqrt{d})} = \begin{cases} \mathbb{Z}[i\sqrt{d}] & \text{si } d \equiv 1 \text{ ou } 2 \pmod 4 \\ \mathbb{Z}[\frac{1+i\sqrt{d}}{2}] & \text{sinon.} \end{cases}$$

Démonstration. Notons $A := \mathcal{O}_{\mathbb{Q}(i\sqrt{d})}$ et $w_d := \frac{1+i\sqrt{d}}{2}$. On distingue alors deux cas :

• *1er cas* : Supposons d'abord d congru à 1 ou 2 modulo 4. On a :

$$(X^2 + d)(i\sqrt{d}) = (i\sqrt{d})^2 + d = 0, \text{ donc } i\sqrt{d} \in A$$

et ainsi $\mathbb{Z}[i\sqrt{d}] \subseteq A$. Réciproquement, soit $z = a + ib \in A$. Si $b = 0$, par la remarque 2.5, il vient $a \in \mathbb{Z} \subset \mathbb{Z}[i\sqrt{d}]$. Considérons désormais $b \neq 0$, et posons :

$$P(X) = X^2 - 2aX - a^2 + db^2 \in \mathbb{Q}[X]$$

P est unitaire et annule z, qui n'est pas dans $\mathbb{Z}$, et ainsi $\mu_z = P$. Par le lemme 2.4, il vient $P \in \mathbb{Z}[X]$. Notamment, $2a \in \mathbb{Z}$, et on admet ponctuellement que $2a$ est nécessairement pair. Alors $a \in \mathbb{Z}$, et comme $db^2 - a \in \mathbb{Z}$, on a $db^2 \in \mathbb{Z}$. On écrit alors :

$$b =: \frac{p}{q} \text{ avec } \begin{cases} p, q \in \mathbb{Z}^* \\ p \wedge q = 1 \end{cases}$$

Et donc :

$$\frac{p^2 d}{q^2} \in \mathbb{Z} \text{ i.e. } q^2 \mid p^2 d.$$

Ainsi, $q^2 \mid d$ par le Lemme de Gauss, et comme d est sans facteur carré, il vient $q = \pm 1$ i.e. $b \in \mathbb{Z}$. Ainsi, $z \in \mathbb{Z}[i\sqrt{d}]$, puis $A \subseteq \mathbb{Z}[i\sqrt{d}]$, ce qui conclut le premier cas.

• *2nd cas* : Supposons maintenant d congru à 3 modulo 4, c'est bien le seul cas restant car d est sans facteur carré. Posons :

$$Q(X) = X^2 - X + \frac{d+1}{4} \in \mathbb{Z}[X], \text{ car } d \equiv 3 \pmod 4$$

Il vient que $Q(w_d) = 0$ et alors comme précédemment $\mathbb{Z}[w_d] \subseteq A$. Réciproquement, soit à nouveau $z = a + ib \in A$ où l'on peut supposer de même $b \neq 0$. On obtient encore $P = \mu_z \in \mathbb{Z}[X]$. D'où, d'une part, $db^2 - a^2 \in \mathbb{Z}$, donc :

$$4db^2 - 4a^2 \in 4\mathbb{Z} \quad \text{i.e.} \quad 4a^2 \equiv 4db^2 \pmod 4 \tag{5}$$

D'autre part, $2a \in \mathbb{Z}$. Si l'on suppose par l'absurde que $2a$ est pair, via les arguments du premier cas, on aurait $A \subseteq \mathbb{Z}[i\sqrt{d}]$. Comme on a toujours $\mathbb{Z}[i\sqrt{d}] \subseteq A$ par ailleurs, on aurait $w_d \notin \mathbb{Z}[i\sqrt{d}] = A$, et alors Q ne serait pas à coefficients dans $\mathbb{Z}$, ce qui contredit le fait que $d \equiv 3 \pmod 4$. Ainsi, $2a$ est impair si bien que :

$$4db^2 \equiv 4a^2 \equiv 1 \pmod 4$$

en utilisant (5). Notamment, $(2b)^2 d \in \mathbb{Z}$, et en raisonnant avec $2b =: p/q$ comme précédemment, il vient $2b \in \mathbb{Z}$. Si $2b$ était pair, b serait dans $\mathbb{Z}$, et alors :

$$4db^2 \equiv 0 \pmod 4$$

ce qui est faux. On conclut alors que :

$$\exists \alpha, \beta \in \mathbb{Z}, \ \begin{cases} a = \alpha + 1/2 \\ b = \beta + 1/2 \end{cases}$$

et on obtient :

$$z = a + ib\sqrt{d} = \alpha - \beta + (2\beta + 1)w_d \in \mathbb{Z}[w_d]$$

si bien que $A \subseteq \mathbb{Z}[w_d]$ puis $A = \mathbb{Z}[w_d]$. On remarque enfin que :

$$2a \equiv 1 \pmod 2 \implies w_d \in A \implies Q \in \mathbb{Z}[X] \implies d \equiv 3 \pmod 4$$

si bien que, dans le 1er cas, $2a$ ne pouvait être que pair.

□

Dans toute la suite, on fixe donc un entier $d \geq 5$ sans facteur carré et congru à 1 ou 2 modulo 4.

Remarque 4.2. On connait les inversibles de l'anneau $\mathbb{Z}[i\sqrt{d}]$, car la norme d'un élément est particulièrement simple à calculer. Soit $z \in \mathbb{Z}[i\sqrt{d}]$ que l'on écrit $z = a + ib\sqrt{d}$ avec $a, b \in \mathbb{Z}$. Alors :

$$N(z) = \begin{vmatrix} a & -db \\ b & a \end{vmatrix} = a^2 + db^2$$

Donc, par la proposition 2.10, on obtient $\mathbb{Z}[i\sqrt{d}]^\times = \{\pm 1\}$.

4.2 Résolution et commentaires

En reprenant d tel que fixé dans la sous-section précédente, $\mathbb{Z}[i\sqrt{d}]$ est intégralement clos d'après la proposition 4.1. On peut donc utiliser tous les résultats précédents. Il reste alors à préciser le sens qu'a ici le terme *régulier*.

Définition 4.3. On dit que 3 est *régulier* pour d si $3 \wedge |Cl(\mathbb{Z}[i\sqrt{d}])| = 1$. Ainsi, d'après la sous-section 3.3, d vérifie :

$$\forall I \lhd \mathbb{Z}[i\sqrt{d}], \ I^3 \text{ principal} \implies I \text{ principal}$$

Théorème 4.4. Si 3 est régulier pour d, on sait alors décrire l'ensemble $\mathcal{S}_d$ des solutions de l'équation de Bachet associée :

$$\begin{cases} \mathcal{S}_d = \{(a^2+d, \pm a(a^2-3d))\} & \text{s'il existe } a \in \mathbb{N},\ d =: 3a^2 \pm 1 \\ \mathcal{S}_d = \varnothing & \text{lorsqu'un tel } a \in \mathbb{N} \text{ n'existe pas} \end{cases} \tag{6}$$

Démonstration. Soit $(x, y) \in \mathbb{Z}^2$ une solution. Supposons qu'il existe $P \lhd \mathbb{Z}[i\sqrt{d}]$ premier contenant les idéaux $(y + i\sqrt{d})$ et $(y - i\sqrt{d})$. Alors :

$$2y \in P \text{ et } -i\sqrt{d}[y + i\sqrt{d} - (y - i\sqrt{d})] = 2d \in P.$$

Puis, il existe $\alpha, \beta \in \mathbb{Z},\ 2 = 2\alpha y + 2\beta d \in P$. En effet, $y \wedge d = 1$ car tout diviseur premier commun diviserait x^3 donc x par le Lemme d'Euclide, et alors :

$$p^2 \mid x^3 - y^2 = d,$$

ce qui contredit le fait que d est sans facteur carré. Il vient donc $(2) \subseteq P$. On distingue alors deux cas : si $d \equiv 1 \pmod 4$, on a :

$$A/(2) = \{0, 1, 1 + i\sqrt{d}, i\sqrt{d}\}$$

n'est pas intègre car $(1 + i\sqrt{d})^2 = 1 - d = 0$, donc $(2) \neq P$ car P est premier non nul donc maximal d'après le corollaire 2.18. Puis, il vient que :

$$A/(2, 1 + i\sqrt{d}) = \{0, 1\} \simeq \mathbb{F}_2$$

qui est bien un corps. P étant propre, on a :

$$A/(2, 1 + i\sqrt{d}) \subseteq A/P \text{ i.e. } P \subseteq (2, 1 + i\sqrt{d}) \subsetneq A.$$

Donc $P = (2, 1 + i\sqrt{d})$ par maximalité de P. On a également $P^2 \subseteq (2)$. Comme, d'après le corollaire 3.8 et la proposition 2.20, on a :

$$N(P^2) = N(P)^2 = 4 = N((2)),$$

il vient $P^2 = (2)$. Puis, comme $(x)^3 \subseteq P$, $(x) \subseteq P$ car P est premier. D'où :

$$Q_1 \dots Q_s P_1 \dots P_r = (y + i\sqrt{d})(y - i\sqrt{d}) \subseteq P^3.$$

en considèrant les décompositions du théorème 3.7 suivantes :

$$(y + i\sqrt{d}) =: Q_1 \dots Q_s \text{ et } (y - i\sqrt{d}) =: P_1 \dots P_r.$$

Par le corollaire 3.2, il existe 3 idéaux parmi $Q_1 \dots Q_s P_1 \dots P_r$ égaux à P. Ceci contredit le fait que $P^2 = (2) \not\supseteq (y \pm i\sqrt{d})$.

Sinon, si $d \equiv 2 \pmod 4$, le raisonnement est complètement analogue : $A/(2)$ n'est pas intègre car $(i\sqrt{d})^2 = -d = 0$, et alors $A/(2, i\sqrt{d}) = \{0, 1\}$, ainsi $P = (2, i\sqrt{d})$ par le même argument. Puis, d étant pair, $P^2 \subseteq (2)$, et on conclut comme dans le cas précédent.

On vient de montrer que les idéaux $(y + i\sqrt{d})$ et $(y - i\sqrt{d})$ sont premiers entre eux. D'après le théorème 3.7, il existe donc $I \lhd A$ tel que :

$$(y + i\sqrt{d}) = I^3.$$

Or, $3 \wedge n = 1$ car d est régulier, avec $n := |Cl(\mathcal{O}_K)|$. Il existe donc des entiers tels que $3\alpha + n\beta = 1$. De plus, I^3 est principal i.e. $\bar{I}^3 = \bar{0}$ dans $Cl(\mathbb{Z}[i\sqrt{d}])$. Ainsi, comme $\bar{I}^n = \bar{0}$ par le Théorème de Lagrange, il vient :

$$\bar{I} = \bar{I}^{3\alpha+n\beta} = \bar{0}.$$

I est donc principal. Ainsi, il existe $a, b \in \mathbb{Z}$ tels que :

$$(y + i\sqrt{d}) = ((a + ib\sqrt{d})^3) \text{ i.e. } : \exists u \in A^\times,\ y + i\sqrt{d} = u(a + ib\sqrt{d})^3.$$

D'après la remarque 4.2, u vaut ± 1, ce qui entraine que u est un cube. On peut donc supposer $y + i\sqrt{d} = (a + ib\sqrt{d})^3$. Alors :

$$\begin{cases} y = a^3 - 3ab^2d \\ 1 = 3a^2b - b^3d \end{cases}$$

Ainsi $b \mid 1$ donc $b = \pm 1$. Supposons alors qu'il existe $a \in \mathbb{N}$ tel que $d = 3a^2 \pm 1$ (l'équation n'admet pas de solutions dans le cas contraire). On obtient donc que $y = \pm a(a^2 - 3d)$, et on vérifie que $x = a^2 + d$. Ces couples sont bien solutions, cela permet ainsi de décrire l'ensemble $\mathcal{S}_d$ des solutions.

□

Remarque 4.5. De façon générale, on ne sait pas résoudre l'équation dans la plupart des autres cas. Cependant, on sait que $\mathcal{S}_d$ est fini pour tout $d \in \mathbb{N}^*$ d'après un théorème de géométrie algébrique. Ce théorème de 1929, dit Théorème de Siegel-Mahler, adopte alors le point de vue de voir l'équation comme les points entiers d'une courbe elliptique.

5 Seconde application : à propos de l'équation de Fermat

5.1 Définitions et premières propriétés

On s'attaque à un second exemple plus technique, qui a motivé la construction de cette arithmétique moderne. On cherche les triplets entiers qui vérifient :

$$x^p + y^p + z^p = 0$$

où p est un nombre premier impair fixé. On sait depuis 1994 qu'un tel triplet non trivial n'existe pas (c'est-à-dire tel que $xyz \neq 0$), chose qu'on sera loin de pouvoir prouver, mais nous allons obtenir néanmoins un sous-résultat intéressant. On fixe dans toute la suite $p > 3$ premier, et on note $\zeta = e^{2i\pi/p}$. On exclut en effet le cas $p = 3$ que l'on sait traiter plus facilement par ailleurs car $\mathbb{Z}[j]$ est un anneau factoriel. Commençons donc par observer des propriétés de $\mathbb{Q}(\zeta)$.

Remarques 5.1. On rappelle que $\mu_\zeta(X) = \Phi_p(X) = \sum_{k=0}^{p-1} X^k$. D'après le rappel 1.2, on en déduit que $(1, \zeta, \dots, \zeta^{p-2})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\zeta)$, et notamment $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$.

Ceci permet d'introduire, par la proposition 1.8, les prolongements $\sigma_1, \dots, \sigma_{p-1}$ de $\mathrm{Id}_\mathbb{Q}$, définis par $\sigma_k(\zeta) = \zeta^k$ pour $k \in [\![1, p-1]\!]$. Comme les ζ^k sont dans $\mathbb{Q}(\zeta)$, les σ_k sont des automorphismes de $\mathbb{Q}(\zeta)$.

Alors, pour tout $z \in \mathbb{Q}(\zeta)$, on définit la *trace* de z par $\mathrm{Tr}(z) = \sum_{k=1}^{p-1} \sigma_k(z)$, linéaire car les σ_k sont des morphismes. Par le même argument, on a que la *norme* de z définie par $N(z) = \prod_{k=1}^{p-1} \sigma_k(z)$ est multiplicative.

Définition 5.2. Soit $z \in \mathbb{Q}[\zeta]$. On remarque que les $\sigma_k(z)$ sont exactement les racines de μ_z. On les appelera les *conjugués* de z.

Remarque 5.3 Si l'on travaillait dans $\mathbb{Q}(i)$, μ_z a au plus deux racines qui sont z et $\bar{z}$. Notamment, on retrouve $N(z) = z\bar{z}$, qui est la norme usuelle lorsque l'on fait de l'arithmétique sur $\mathbb{Z}[i]$. Les définitions précédentes ne sont ainsi qu'une généralisation naturelle à une extension de degré supérieur.

Les outils que nous venons d'introduire sont incontournables en théorie algébrique des nombres, car à la base d'un tas de résultats théoriques et de structures. On a en fait déjà pu l'observer car la norme que l'on vient de définir coïncide avec la définition 2.7, bien qu'ici on ne démontrera pas l'égalité des deux normes. On travaillera dans cette section avec cette nouvelle définition de la norme et on retombera assez vite sur les résultats dont nous avons besoin.

Démontrons maintenant un lemme préliminaire qui servira par la suite, avant de terminer cette sous-section en observant quelques propriétés de la norme.

Lemme 5.4. Soit $R \in \mathbb{Z}[X]$ unitaire, de degré $d \geq 1$. Notons $\alpha_1, \dots, \alpha_d$ ses racines complexes. Alors :

$$\forall Q \in \mathbb{Z}[X],\ \prod_{k=1}^{d} (X - Q(\alpha_k)) \in \mathbb{Z}[X]$$

Démonstration. Notons :

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ -1 & 0 & \cdots & 0 & -a_1 \\ 0 & -1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & -1 & -a_{d-1} \end{pmatrix}$$

où les a_i sont les coefficients de R. On a ainsi $M \in \mathcal{M}_d(\mathbb{Z})$ et $\chi_M = R$ par un calcul de déterminant. Alors, on trigonalise M dans $\mathbb{C}$ si bien que M s'écrit PTP^{-1} où P est inversible et T est triangulaire supérieure. On a :

$$M^2 = PTP^{-1}PTP^{-1} = PT^2P^{-1}, \text{ puis } M^k = PT^kP^{-1}$$

pour tout $k \in \mathbb{N}$ par récurrence, puis $Q(M) = PQ(T)P^{-1}$ par linéarité (relation que l'on note $(*)$). Comme $M \in \mathcal{M}_d(\mathbb{Z})$ et $Q \in \mathbb{Z}[X]$, on a $Q(M) \in \mathcal{M}_d(\mathbb{Z})$ puis $\chi_{Q(M)} \in \mathbb{Z}[X]$. De plus, les valeurs propres de T sont les α_k car T et M sont semblables, et alors les valeurs propres de $Q(T)$ sont les $Q(\alpha_k)$ car T est triangulaire supérieure. Et ainsi :

$$\prod_{k=1}^{d}(X - Q(\alpha_k)) = \chi_{Q(T)}(X) \overset{(*)}{=} \chi_{Q(M)}(X) \in \mathbb{Z}[X].$$

□

Corollaire 5.5. Pour tout $z \in \mathbb{Z}[\zeta]$, $\mathrm{Tr}(z)$ et $N(z)$ sont dans $\mathbb{Z}$.

Démonstration. Soit $z \in \mathbb{Z}[\zeta]$, il existe $Q \in \mathbb{Z}[X]$ tel que $Q(\zeta) = z$. Alors :

$$\forall k \in [\![1, p-1]\!],\ \sigma_k(z) = \sigma_k(Q(\zeta)) = Q(\sigma_k(\zeta)) = Q(\zeta^k).$$

De plus, Φ_p est unitaire à coefficients entiers, si bien que :

$$\sum_{j=0}^{p-1} a_j X^j := \prod_{k=1}^{p-1}(X - \sigma_k(z)) = \prod_{k=1}^{p-1}(X - Q(\zeta^k)) \in \mathbb{Z}[X],$$

d'après le lemme 5.4. Puis, on conclut par les relations coefficients-racines :

$$\mathrm{Tr}(z) = -a_{p-2} \in \mathbb{Z}, \text{ et } N(z) = (-1)^{p-1}a_0 \in \mathbb{Z}.$$

□

Remarque 5.6. D'après la définition de N donnée ici, on obtient : pour tout $k \in [\![1, p-1]\!]$ et $z \in \mathbb{Z}[\zeta]$, $\sigma_k(z) \mid N(z)$ dans $\mathbb{Z}[\zeta]$. Notamment $z \mid N(z)$.

Proposition 5.7 $z \in \mathbb{Z}[\zeta]^\times \iff N(z) = \pm 1$

Démonstration. Soit $z \in \mathbb{Z}[\zeta]$: Si $N(z) = \pm 1$, alors, par la remarque 5.6, $z \mid 1$ i.e. z et 1 sont associés c'est-à-dire z est inversible. Réciproquement, si z est inversible, il existe $x \in \mathbb{Z}[\zeta]$ tel que $xz = 1$. Alors, en passant à la norme, il vient $N(z) \mid \pm 1$ dans $\mathbb{Z}$ d'après le corollaire 5.5, et ainsi $N(z) = \pm 1$. □

Remarque 5.8 Retenons ces valeurs de N :

(i) $N(\zeta) = \prod_{k=1}^{p-1} \zeta^k = (-1)^p \Phi_p(0) = -1$

(ii) $N(1-\zeta) = \prod_{k=1}^{p-1}(1-\zeta^k) = \Phi_p(1) = p.$

5.2 Principaux résultats sur l'anneau $\mathbb{Z}[\zeta]$

Commençons par démontrer que $\mathbb{Z}[\zeta]$ est intégralement clos. Nous avons besoin pour cela de calculer des valeurs remarquables de la trace. Pour faire ces calculs efficacement, nous allons démontrer à la main une propriété de $G := \{\sigma_1, \dots, \sigma_{p-1}\}$, qui est en fait ce que l'on appelle en théorie de Galois le *Groupe de Galois de l'extension* $\mathbb{Q}(\zeta)/\mathbb{Q}$.

Proposition 5.9. Notons $\mathcal{Z}(\Phi_p) := \{\zeta, \dots, \zeta^{p-1}\}$. L'action naturelle de G sur $\mathcal{Z}(\Phi_p)$ est simplement transitive. Autrement dit :

$$\forall i, j \in [\![1, p-1]\!],\ i \neq j \Longrightarrow \exists!\ \sigma \in G,\ \sigma(\zeta^i) = \zeta^j.$$

Démonstration. On remarque d'abord que G est un sous ensemble fini du groupe des automorphismes de $\mathbb{Q}(\zeta)$, stable par composition, et est donc bien un groupe. De plus, si z est une racine de Φ_p, les $\sigma_j(z)$ en sont également, ce qui signifie bien que G agit sur $\mathcal{Z}(\Phi_p)$. Ensuite, pour tout $z \in \mathcal{Z}(\Phi_p)$, il existe $k \in [\![1, p-1]\!]$ tel que $z = \zeta^k$, et alors :

$$\forall j \in [\![1, p-1]\!],\ \sigma_j(\zeta^k) = (\sigma_j(\zeta))^k = \zeta^{jk} = \sigma_k(\zeta^j).$$

Comme σ_k est injectif en tant que morphisme de corps, on obtient :

$$\forall i \neq j \in [\![1, p-1]\!],\ \sigma_i(\zeta^k) \neq \sigma_j(\zeta^k),$$

ce qui signifie exactement :

$$\forall z \in \mathcal{Z}(\Phi_p), \forall \sigma \neq \sigma' \in G,\ \sigma(z) \neq \sigma'(z).$$

Notamment, l'action est libre, ce qui implique que le cardinal de chaque orbite vaut $|G|/1 = |G|$. Puis, en partitionnant $\mathcal{Z}(\Phi_p)$ en orbites, il vient $|\mathcal{Z}(\Phi_p)| = n|G|$ où n est le nombre d'orbites. Ainsi, comme $|\mathcal{Z}(\Phi_p)| = |G|$ par ailleurs, on conclut qu'il n'y a qu'une seule orbite i.e. que l'action est transitive. Comme elle est libre, elle est par définition simplement transitive.

□

Corollaire 5.10. $\mathrm{Tr}(1) = p - 1$. De plus, pour tout $k \in [\![1, p-1]\!]$, $\mathrm{Tr}(\zeta^k) = -1$.

Démonstration. D'abord, comme les σ_j fixent $\mathbb{Q}$, on a :

$$\mathrm{Tr}(1) = \sum_{j=1}^{p-1} \sigma_j(1) = \sum_{j=1}^{p-1} 1 = p - 1.$$

Ensuite, renotons $G := \{\sigma_1, \dots, \sigma_{p-1}\}$. De par la proposition précédente, on a :

$$\forall k \in [\![1, p-1]\!],\ \{\sigma(\zeta^k),\ \sigma \in G\} = \mathcal{Z}(\Phi_p).$$

Notons $(**)$ cette propriété. On peut alors effectuer le calcul :

$$\forall k \in [\![1, p-1]\!],\ \mathrm{Tr}(\zeta^k) = \sum_{j=1}^{p-1} \sigma_j(\zeta^k) = \sum_{\sigma \in G} \sigma(\zeta^k) \overset{(**)}{=} \sum_{l=1}^{p-1} \zeta^l = -1.$$

□

Théorème 5.11. L'anneau $\mathbb{Z}[\zeta]$ est intégralement clos, c'est-à-dire $\mathbb{Z}[\zeta] = \mathcal{O}_{\mathbb{Q}(\zeta)}$.

Démonstration. Soit $\theta \in \mathbb{Z}[\zeta]$, il existe $P \in \mathbb{Z}[X]$ tel que $\theta = P(\zeta)$. Or, $\zeta \in \mathcal{O}_{\mathbb{Q}(\zeta)}$ et $\mathcal{O}_{\mathbb{Q}(\zeta)}$ est un anneau par le théorème 2.3, donc $\theta \in \mathcal{O}_{\mathbb{Q}(\zeta)}$. Ainsi, $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}$.

Réciproquement, soit $\theta = \sum_{k=0}^{p-2} a_k \zeta^k \in \mathcal{O}_{\mathbb{Q}(\zeta)}$ que l'on écrit dans la $\mathbb{Q}$-base $(1, \dots, \zeta^{p-2})$. Par le corollaire précédent, on calcule :

$$\begin{aligned} \forall k \in [\![0, p-2]\!],\ b_k &:= \mathrm{Tr}(\theta\zeta^{-k} - \theta\zeta) \\ &= \sum_{j=0}^{p-2} \left[a_j \mathrm{Tr}(\zeta^{j-k}) - a_j \mathrm{Tr}(\zeta^j)\right] \\ &= (p-1)a_k - \sum_{\substack{j=0 \\ j\neq k}}^{p-2} a_j + \sum_{j=0}^{p-2} a_j \ = pa_k \end{aligned}$$

Par le corollaire 5.5, les b_k sont dans $\mathbb{Z}$. De plus, on a :

$$p\theta = \sum_{k=0}^{p-2} b_k \zeta^k = \sum_{k=0}^{p-2} c_k (1-\zeta)^k \tag{7}$$

où l'on a posé :

$$\forall k \in [\![0, p-2]\!],\ c_k = (-1)^k \sum_{j=k}^{p-2} \binom{j}{k} b_j \in \mathbb{Z}.$$

En effet, par la formule du Binôme :

$$\sum_{k=0}^{p-2} b_k \zeta^k = \sum_{k=0}^{p-2} b_k \sum_{j=0}^{k} \binom{k}{j} (\zeta-1)^j = \sum_{j=0}^{p-2} (\zeta-1)^j \sum_{k=j}^{p-2} \binom{k}{j} b_k = \sum_{j=0}^{p-2} c_j (1-\zeta)^j$$

En outre, dans ce calcul, ζ et $1-\zeta$ jouent des rôles symétriques. Ceci induit une symétrie entre les b_k et les c_k si bien que :

$$\forall k \in [\![0, p-2]\!],\ b_k = (-1)^k \sum_{j=k}^{p-2} \binom{j}{k} c_j \in \mathbb{Z}. \tag{8}$$

Montrons enfin par récurrence que $p \mid c_0, \dots, c_{p-2}$. Tout d'abord, d'après (7) et en raisonnant modulo $(1-\zeta)\mathcal{O}_{\mathbb{Q}(\zeta)}$, $c_0 = p\theta = 0$, donc $p = N(1-\zeta) \mid N(c_0) = c_0^{p-1}$ puis $p \mid c_0$. De plus, si $k \in [\![1, p-2]\!]$ vérifie $p \mid c_0, \dots, c_{k-1}$, on a :

$$c_k(1-\zeta)^k = 0 \ (\mathrm{mod}\ (1-\zeta)^{k+1}\mathcal{O}_{\mathbb{Q}(\zeta)}),\ \text{donc } c_k = 0 \ (\mathrm{mod}\ (1-\zeta)),$$

puis comme précédement, $p \mid c_k$, ce qui conclut la récurrence. Ainsi, p divise les c_k, donc les b_k d'après (8). Cela signifie que les a_k sont dans $\mathbb{Z}$, et que $\mathcal{O}_{\mathbb{Q}(\zeta)} \subseteq \mathbb{Z}[\zeta]$, ce qui termine la preuve.

□

Dans toute la suite, on notera $\lambda = 1 - \zeta$. Cet élément ne paie pas de mine mais c'est un couteau suisse et un argument clef dans la plupart des preuves. Nous avons déjà pu le remarquer dans la démonstration précédente. Observons d'autres propriétés utiles sur λ.

Proposition 5.12. Soit $z, z' \in \mathbb{Z}[\zeta]$ conjugués. On a les propriétés suivantes :

(i) $\forall j \in \mathbb{N},\ \zeta^j = 1$ dans $\mathbb{Z}[\zeta]/\lambda\mathbb{Z}[\zeta]$.

(ii) $z = z'$ dans $\mathbb{Z}[\zeta]/\lambda\mathbb{Z}[\zeta]$.

Démonstration. • *Point* (i) : dans $\mathbb{Z}[\zeta]/\lambda\mathbb{Z}[\zeta]$, on a $\lambda = 1 - \zeta = 0$ i.e. $\zeta = 1$, puis $\zeta^j = 1$ pour $j \in \mathbb{N}$. On en déduit (ii) car :

$$\forall z = \sum_{j=0}^{p-2} a_j \zeta^j \in \mathbb{Z}[\zeta],\quad z = \sum_{j=0}^{p-2} a_j \text{ dans } \mathbb{Z}[\zeta]/\lambda\mathbb{Z}[\zeta].$$

• *Point* (ii) : il suffit de montrer qu'on a alors la même égalité pour tout $z' = \sigma_k(z)$ conjugué de z, ce qui est vrai car alors $z' = \sum_{j=0}^{p-2} a_j \sigma_k(\zeta^j)$ et $\{\sigma_k(\zeta^j), j \in \mathbb{N}\} \subset \{\zeta^j, j \in \mathbb{N}\}$ donc on peut appliquer le même raisonnement qu'à z.

□

Proposition 5.13. L'idéal $\lambda\mathbb{Z}[\zeta]$ possède les propriétés suivantes :

(i) $\lambda\mathbb{Z}[\zeta]$ est un idéal premier.

(ii) $\lambda\mathbb{Z}[\zeta] \cap \mathbb{Z} = p\mathbb{Z}$

(iii) $p\mathbb{Z}[\zeta] = \lambda^{p-1}\mathbb{Z}[\zeta]$.

Démonstration. • *Point* (i) : Regardons d'abord l'image de $(1, \dots, \zeta^{p-2})$ par m_λ :

$$\forall k \in [\![0, p-2]\!],\ \lambda\zeta^k = \zeta^k - \zeta^{k+1}.$$

Notamment, comme $\Phi_p(\zeta) = 0$, on a :

$$\lambda\zeta^{p-2} = \zeta^{p-2} + \sum_{j=0}^{p-2} \zeta^j = 1 + \zeta + \cdots + \zeta^{p-3} + 2\zeta^{p-2}.$$

Ainsi, d'après la proposition 2.20 et le théorème 5.11, il vient :

$$N(\lambda\mathbb{Z}[\zeta]) = \pm\det(m_\lambda) = \pm \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ -1 & 1 & 0 & \cdots & 0 & 1 \\ 0 & -1 & 1 & \ddots & \vdots & 1 \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & -1 & 1 & 1 \\ 0 & \cdots & \cdots & 0 & -1 & 2 \end{vmatrix}_{p-1}$$

On effectue des opérations sur les colonnes : $C_{p-1} \leftarrow C_{p-1} - kC_k$ successivement pour $k = 1, \dots, p-2$. On obtient alors un déterminant triangulaire inférieur qui vaut p. Et alors $N(\lambda\mathbb{Z}[\zeta]) = \pm p$ donc vaut p car la norme d'un idéal est positive.

Soit $P_1 \dots P_s$ la décomposition de $\lambda\mathbb{Z}[\zeta]$ en produit d'idéaux premiers, de par les théorèmes 3.7 et 5.11. Alors, par le corollaire 3.8 :

$$N(\lambda\mathbb{Z}[\zeta]) = N(P_1) \dots N(P_s) \text{ si bien que, } \exists!\ j \in [\![1, s]\!],\ N(P_j) = p,$$

et alors $P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{s-1}$ et P_s sont de norme 1. De par la définition de la norme d'un idéal, ces idéaux valent donc tous $\mathbb{Z}[\zeta]$. On en conclut que $\lambda\mathbb{Z}[\zeta] = P_j$ et que $\lambda\mathbb{Z}[\zeta]$ est premier.

• *Point* (ii) : Notons $I = \lambda\mathbb{Z}[\zeta] \cap \mathbb{Z}$. Pour tout $x, y \in I$ et $m \in \mathbb{Z}$, $x - y \in I$ et $mx \in I$, donc I est un idéal de $\mathbb{Z}$. De plus, $\lambda \mid p$ donc $p\mathbb{Z} \subset p\mathbb{Z}[\zeta] \subset \lambda\mathbb{Z}[\zeta]$ et alors $p\mathbb{Z} \subset I \subset \mathbb{Z}$. Comme $N(\lambda) = p \neq \pm 1$, λ n'est pas inversible d'après la proposition 5.7, et ainsi $I \subsetneq \mathbb{Z}$. Enfin, $p\mathbb{Z}$ étant un idéal maximal de $\mathbb{Z}$, on déduit de la chaîne d'inclusion précédente que $p\mathbb{Z} = I$.

• *Point* (iii) : Pour tout $k \in [\![1, p-1]\!]$, k possède un inverse modulo p que l'on note $k' \in \mathbb{N}$. Et alors :

$$\frac{1-\zeta}{1-\zeta^k} = \frac{1-(\zeta^k)^{k'}}{1-\zeta^k} = 1 + \zeta^k + \zeta^{2k} + \cdots + (\zeta^k)^{k'-1} \in \mathbb{Z}[\zeta].$$

On a donc exhibé un inverse de $(1-\zeta^k)/(1-\zeta)$ dans $\mathbb{Z}[\zeta]$, qui est donc inversible. Ainsi :

$$\forall k \in [\![1, p-1]\!],\ (1-\zeta^k)\mathbb{Z}[\zeta] = \lambda\mathbb{Z}[\zeta],$$

et ainsi, en faisant le produit de tous les idéaux :

$$\lambda^{p-1}\mathbb{Z}[\zeta] = (1-\zeta)\dots(1-\zeta^{p-1})\mathbb{Z}[\zeta] = p\mathbb{Z}[\zeta].$$

La dernière égalité provient du fait que $N(\lambda) = (1-\zeta)\dots(1-\zeta^{p-1}) = p$.

□

Corollaire 5.14. Soit $\alpha \in \mathbb{Z}[\zeta]$. Il existe $a \in \mathbb{Z}$ tel que :

$$\alpha^p = a \ \text{ dans } \mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$$

Démonstration. Il existe $\alpha_0, \dots, \alpha_{p-2} \in \mathbb{Z}$ tels que $\alpha = \sum_{k=0}^{p-2} \alpha_k \zeta^k$. Alors, d'après la proposition 5.12, modulo $\lambda\mathbb{Z}[\zeta]$:

$$\alpha = \sum_{k=0}^{p-2} \alpha_k =: \beta \in \mathbb{Z}.$$

En fait, on obtient même $\alpha\zeta^j = \beta$ modulo $\lambda\mathbb{Z}[\zeta]$ pour tout $j \in \mathbb{N}$. Cela signifie que :

$$\forall j \in \mathbb{N},\ \exists\, \gamma_j \in \mathbb{Z}[\zeta],\ \beta - \alpha\zeta^j = \lambda\gamma_j$$

et alors, en factorisant $X^p - 1$, il vient :

$$\beta^p - \alpha^p = \prod_{j=0}^{p-1}(\beta - \alpha\zeta^j) = \lambda^p \prod_{j=0}^{p-1}\gamma_j = up\lambda\prod_{j=0}^{p-1}\gamma_j$$

pour un certain $u \in \mathbb{Z}[\zeta]^\times$. L'existence de u est garantie par la proposition 5.13.(iii). Alors, $a := \beta^p$ convient, ce qui conclut.

□

Enfin, finissons cette sous-section en donnant une caractérisation particulièrement simple des inversibles de $\mathbb{Z}[\zeta]$. Nous aurons d'abord besoin d'un résultat sur les polynômes dû à Kronecker. Il utilise les relations coefficients-racines que l'on a rappelé pour démontrer la proposition 2.11.

Théorème 5.15. Soit $P \in \mathbb{Z}[X]$ unitaire, de degré $d \geq 1$. Notons $\mathcal{Z}(P)$ l'ensemble des racines de P dans $\mathbb{C}$. Alors :

$$\mathcal{Z}(P) \subset \{z \in \mathbb{C} \mid 0 < |z| \leq 1\} \implies \mathcal{Z}(P) \subset \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$$

Démonstration. Soit Ω_n l'ensemble des polynômes T de $\mathbb{Z}[X]$, unitaires de degré $n \geq 1$, vérifiant $\mathcal{Z}(T) \subset \{z \in \mathbb{C} \mid 0 < |z| \leq 1\}$. Montrons que Ω_n est de cardinal fini. Notons d'abord :

$$T = X^n + \sum_{k=1}^{n} a_k X^{n-k} = \prod_{j=1}^{n} (X - \alpha_j)$$

un tel polynôme. Par les relations coefficients-racines, on obtient la majoration suivante :

$$\forall k \in [\![1, n]\!],\ |a_k| = \left| \sum_{1 \leq i_1 < \cdots < i_k \leq n} \prod_{j=1}^{k} \alpha_{i_j} \right| \leq \sum_{1 \leq i_1 < \cdots < i_k \leq n} \prod_{j=1}^{k} |\alpha_{i_j}| \leq \binom{n}{k} \leq n!$$

car le produit des modules est majoré par 1, puis par la définition combinatoire de ce qu'est un coefficient binomial. Ainsi, chaque polynôme de Ω_n est de degré n et les coefficients sont dans $[\![1, n!]\!]$. Il y a donc bien un nombre fini de tels polynômes, i.e. $|\Omega_n| < \infty$. On en déduit ainsi que l'ensemble $\mathcal{Z}_n := \bigcup_{P \in \Omega_n} \mathcal{Z}(P)$ est également de cardinal fini car chaque P vérifie $|\mathcal{Z}(P)| \leq n$.

Fixons $d \in \mathbb{N}^*$ et $P = \prod_{j=1}^{d} (X - \alpha_j) \in \Omega_d$. Remarquons que :

$$\forall k \geq 1,\ P_k := \prod_{j=1}^{d} (X - \alpha_j^k)\ \in \mathbb{Z}[X]$$

en utilisant le lemme 5.4 avec $Q = X^k$, et ainsi $P_k \in \Omega_d$. Alors, soit $\alpha \in \mathcal{Z}(P)$, il suffit pour conclure de trouver $n \in \mathbb{N}^*$ tel que $\alpha \in \mathbb{U}_n$. D'une part, on a $\alpha^k \in \mathcal{Z}(P_k) \subset \mathcal{Z}_d$ pour $k \geq 1$. Cela signifie que l'on peut définir :

$$\begin{array}{rccc} \Phi : & \mathbb{N}^* & \longrightarrow & \mathcal{Z}_d \\ & k & \longmapsto & \alpha^k \end{array}$$

D'autre part, $|\mathbb{N}^*| = \infty > |\mathcal{Z}_d|$, et ainsi Φ n'est pas injective. On en conclut qu'il existe $1 \leq r < s$ tels que $\alpha^r = \alpha^s$ i.e. $\alpha \in \mathbb{U}_{s-r}$.

□

Passons au second prérequis du théorème traitant de $\mathbb{Z}[\zeta]^\times$. Nous allons rappeler quelques propriétés de φ, qui désigne la fonction indicatrice d'Euler.

Proposition 5.16. Soient $k, l, m \in \mathbb{N}^*$, l'indicatrice d'Euler vérifie :

(*i*) Si $k \wedge l = 1$, alors $\varphi(kl) = \varphi(k)\varphi(l)$.

(*ii*) Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec les p_i premiers et distincts, alors :

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{\alpha_i - 1}$$

(*iii*) Il n'existe qu'un nombre fini d'entiers n tels que $\varphi(n) \leq m$.

Démonstration. • *Point* (*i*) : Via le Lemme Chinois, on a l'isomorphisme suivant :

$$\mathbb{Z}/kl\mathbb{Z} \simeq \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$$

et on conclut en regardant le nombre d'inversible de chaque anneau :

$$\varphi(kl) = |\mathbb{Z}/kl\mathbb{Z}^\times| = |(\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z})^\times| = |\mathbb{Z}/k\mathbb{Z}^\times \times \mathbb{Z}/l\mathbb{Z}^\times| = \varphi(k)\varphi(l)$$

• *Point* (ii) : Soit $\alpha \in \mathbb{N}^*$ et p premier. L'ensemble des entiers positifs non premiers avec p^α est l'ensemble des multiples de p. Il y en a $p^{\alpha-1}$ dans $[\![1, p^\alpha]\!]$, si bien que :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} \tag{9}$$

De plus, en itérant le point (i), il vient :

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$$

et on conclut alors via l'égalité (9).

• *Point* (iii) : Soit p^α l'un des facteurs dans la décomposition en nombres premiers de n. D'une part :

$$p - 1 = \varphi(p) \leq \varphi(n) = m, \text{ donc } p \leq m + 1$$

Ainsi, p est inclu dans un ensemble fini de nombres premiers que l'on note $\{q_1, \dots, q_s\}$. D'autre part, en notant $\beta \in \mathbb{N}^*$ le premier entier tel que $p^{\beta-1} \geq m$, il vient que $\beta \geq \alpha$. En effet, sinon :

$$m \geq \varphi(n) \geq \varphi(p^\alpha) > \varphi(p^\beta) \geq m$$

ce qui est absurde. Ainsi, en renotant :

$$\forall j \in [\![1, s]\!],\ \beta_j := \min\{\gamma \in \mathbb{N}^*, q_j^{\gamma-1} \geq m\}$$

on voit que tout entier n vérifiant $\varphi(n) \leq m$ s'écrit $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec chaque $p_i^{\alpha_i}$ dans $\{1, q_1, q_1^2, \dots q_1^{\beta_1}, q_2, q_2^2, \dots, q_2^{\beta_2}, \dots, q_s^{\beta_s}\}$. Ce dernier ensemble est de cardinal fini, donc l'ensemble des entiers n que l'on peut construire ainsi l'est également.

□

Théorème 5.17. $\mathbb{Z}[\zeta]^\times = \{\delta\zeta^r \mid \delta \in \mathbb{R} \cap \mathbb{Z}[\zeta]^\times,\ r \in \mathbb{Z}\}$

Démonstration. Pour $u \in \mathbb{Z}[\zeta]^\times$, notons $v = u/\overline{u}$ la fraction suivante. D'après le lemme 2.4, $P := \mu_v \in \mathbb{Z}[X]$. Notons que $\sigma_1(v), \dots, \sigma_{p-1}(v)$ sont les racines de P et vérifient :

$$\forall k \in [\![1, p-1]\!],\ \sigma_k(v) = \sigma_k(u/\overline{u}) = \sigma_k(u)/\overline{\sigma_k(u)} \in \mathbb{U}$$

Par le théorème 5.15, les racines de P sont donc des racines de l'unité, notamment v est une racine de l'unité. Notons alors G le sous groupe des racines de l'unité contenues dans $\mathbb{Z}[\zeta]$.

Premièrement, soit $t \in G$ et $m \in \mathbb{N}^*$ tel que t est une racine primitive m-ième de l'unité. Alors, $\mathbb{Q}(t) \subseteq \mathbb{Q}(\zeta)$. Notamment :

$$\varphi(m) = \deg(\mu_t) \leq \deg(\mu_\zeta) = p - 1.$$

Alors, d'après la proposition 5.16.(iii), m est inclu dans un ensemble fini i.e. il existe $M \in \mathbb{N}^*$ tel que $m \in [\![1, M]\!]$. Ainsi :

$$G \subseteq \bigcup_{k \in [\![1,M]\!]} \mathbb{U}_k\ ,\ \text{et alors } n := |G| < \infty.$$

Ensuite, notons :

$$H = \{1, \zeta, \dots, \zeta^{p-1}, -1, -\zeta, \dots, -\zeta^{p-1}\}.$$

C'est un sous-groupe de G, de cardinal $2p$. En effet, les p premiers termes $1, \zeta, \dots, \zeta^{p-1}$ sont distincts, et si l'on suppose par l'absurde qu'il existe $k \neq l$ tel que $\zeta^k = -\zeta^l$. Alors, comme p est impair :

$$-1 = -(\zeta^p)^l = (-\zeta^l)^p = (\zeta^k)^p \in \{1, \zeta, \dots, \zeta^{p-1}\},$$

et ainsi, $2 = \text{ord}(-1) \mid p$ par le Théorème de Lagrange, ce qui est faux. Toujours par le Théorème de Lagrange, on obtient que $|H|$ divise $|G|$ i.e. $2p \mid n$. On remarque enfin que $t^{|G|} = 1$, donc G est un sous groupe de $\mathbb{U}_n$. Ce groupe étant cyclique, G est également cyclique, donc engendré par $w \in \mathbb{Z}[\zeta]$ qui est alors une racine primitive n-ième de l'unité. Alors, $\mathbb{Q}(w) \subseteq \mathbb{Q}(\zeta)$ et $\zeta \in G$ i.e. ζ est une puissance de w, si bien que $\mathbb{Q}(w) = \mathbb{Q}(\zeta)$. Ainsi :

$$\varphi(n) = \deg(\mu_w) = \deg(\mu_\zeta) = p - 1 \tag{10}$$

et alors $2p = n$ donc $G = H$. En effet, si $2p < n$, comme $2p \mid n$, il existerait $a, b, c \in \mathbb{N}^*$ tels que $n = 2^a p^b c$ avec a, b ou $c > 1$ et où $c \wedge 2p = 1$. On aurait alors :

$$\varphi(n) = \varphi(2^a)\varphi(p^b)\varphi(c) = 2^{a-1}(p-1)p^{b-1}\varphi(c) > p - 1,$$

via la proposition précédente, ce qui contredit (10).

On conclut donc que $v \in H$ i.e. qu'il existe $k \in \mathbb{N}$ tel que $v = \pm\zeta^k$. Si on suppose par l'absurde qu'il y a un bien un signe "$-$", en raisonnant modulo $\lambda\mathbb{Z}[\zeta]$, on obtient :

$$u = -\zeta^k \overline{u} = -\overline{u} = -u, \text{ i.e. } \lambda \mid 2u$$

d'après la proposition 5.11.(iii), et en passant à la norme :

$$N(\lambda) \mid N(2u) = N(2)N(u) = \pm 2^{p-1}$$

car u est inversible donc de norme ± 1 par la proposition 5.7. On en conclut que $p \mid 2$, ce qui contredit l'hypothèse sur p. Ainsi, $v = \zeta^k$. Cela se réécrit $v = \zeta^{2r}$ pour un certain $r \in \mathbb{N}$, car soit k est pair, soit k est impair et il est donc congru à un nombre pair modulo p qui est impair. Posons donc enfin $\delta = u\zeta^{-r}$ qui est bien dans $\mathbb{R}$ car, d'après ce qui précède :

$$\overline{\delta} = \overline{u}\zeta^r = u\zeta^{-2r}\zeta^r = \delta.$$

Enfin, on conclut par multiplicativité de N et par la proposition 5.7. $N(\delta) = \pm 1$ i.e. $\delta \in \mathbb{Z}[\zeta]^\times$. Cela montre qu'on a bien l'inclusion directe du théorème, et on obtient l'inclusion réciproque encore par multiplicativité de la norme et la même proposition.

□

5.3 Résolution lorsque $p \nmid xyz$

On dira par la suite que p est un *nombre premier régulier* lorsque $p \wedge |Cl(\mathbb{Z}[\zeta])|$ vaut 1. Cette approche de Kummer permet alors de répondre positivement à la conjecture de Fermat pour tous les nombres premiers réguliers. Pour ce qui est de ce document, avec les outils développés, nous allons réussir à montrer qu'il n'existe pas de solutions non triviales dans le cas où $p \nmid xyz$.

La remarque suivante vient anticiper la résolution avec une observation générale. On peut souvent faire cette hypothèse bien pratique lorsqu'une équation est suffisamment symétrique comme celle que l'on considère.

Remarque 5.18. Lorsqu'un triplet est solution de l'équation de Fermat, on peut toujours se ramener au cas où x, y et z sont deux à deux premiers entre eux. Effectivement, considérons un triplet solution et notons $d = \text{pgcd}(x, y, z)$. Alors :

$$\left(\frac{x}{d}\right)^p + \left(\frac{y}{d}\right)^p + \left(\frac{z}{d}\right)^p = 0, \text{ et } \left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right) \in \mathbb{Z}^3.$$

On obtient donc encore un triplet solution où les termes sont globalement premiers entre eux. On suppose donc $\text{pgcd}(x, y, z) = 1$. Alors, ces entiers sont deux à deux premiers entre eux. En effet, notons cette fois :

$$d = x \wedge y, \text{ et } \begin{cases} x' = x/d \\ y' = y/d \end{cases}$$

Il suffit pour conclure de montrer que $d = 1$ par symétrie des rôles de x, y et z. Or :

$$d^p x'^p + d^p y'^p = -z^p, \text{ donc } d^p \mid z^p.$$

En regardant les valuations p-adiques de d et z, il vient alors que $d \mid z$, puis $d = 1$ car $\text{pgcd}(x, y, z) = 1$.

Muni de tout cet arsenal, la preuve du théorème suivant se déroule de façon assez classique. On mentionnera sur le moment lorsque des astuces plus originales sont utilisées.

Théorème 5.19. Soit $p > 3$ un nombre premier régulier. Alors, pour tout triplet $(x, y, z) \in \mathbb{Z}^3$:

$$x^p + y^p + z^p = 0 \implies p \mid xyz$$

Démonstration. On considère par l'absurde un triplet solution tel que $p \nmid xyz$, on suppose d'après la remarque précédente que x, y et z sont deux à deux premiers entre eux. Notons alors :

$$I_k = (x + \zeta^k y), \text{ si bien que : } \quad (z^p) = \prod_{k=0}^{p-1} I_k$$

Montrons alors, pour pouvoir conclure que les I_k sont des puissances p, que :

$$\forall k \neq l, \ 1 \in I_k + I_l$$

Déjà, $(x + \zeta^k y) \mid z^p$ i.e. $z^p \in I_k$, d'où $z^p \in I_k + I_l$. De plus :

$$y(1 - \zeta^{l-k}) = \zeta^{-k}(x + \zeta^k y) - \zeta^{-k}(x + \zeta^l y) \in I_k + I_l$$

où l'on a supposé sans pertes de généralités que $l > k$. Par les remarques 5.6 et 5.8.(ii), $(1 - \zeta^{l-k}) \mid p$, d'où $yp \in I_k + I_l$. On déduit enfin des hypothèses que

$yp \wedge z^p = 1$. Donc par le Théorème de Bézout, on en déduit que $1 \in I_k + I_l$. Notamment, il existe $I \lhd \mathbb{Z}[\zeta]$ tel que :

$$(x + \zeta y) = I^p \text{ i.e. } x + \zeta y = u\alpha^p$$

où u et α sont dans $\mathbb{Z}[\zeta]$ et tel que u est inversible. En effet, I^p est principal, et comme p est régulier, I aussi c'est-à-dire que I s'écrit effectivement (α). Par le théorème 5.17, cela se réécrit :

$$x + \zeta y = \delta\zeta^r\alpha^p \text{ avec } r \in \mathbb{Z},\ \delta \in \mathbb{R} \cap \mathbb{Z}[\zeta]^\times.$$

On cherche maintenant à transformer l'équation pour pouvoir, via la norme, obtenir des propriétés de x, y et z qui contredisent $p \nmid xyz$. C'est la partie plus astucieuse. Par le corollaire 5.14, lorsqu'on raisonne modulo $p\mathbb{Z}[\zeta]$, il existe $a \in \mathbb{Z}$ tel que $a = \alpha^p$. Ainsi, toujours dans $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$, il vient :

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = (x + \zeta y)\zeta^{-r} - (x + \zeta^{-1}y)\zeta^r = \delta a - \overline{\delta a} = 0$$

car $\delta a \in \mathbb{R}$. Ceci se réécrit :

$$\frac{x}{p}\zeta^{-r} + \frac{y}{p}\zeta^{1-r} - \frac{x}{p}\zeta^r - \frac{y}{p}\zeta^{r-1} \in \mathbb{Z}[\zeta] \text{ (notons le } \beta)$$

Comme $(1, \zeta, \ldots, \zeta^{p-2})$ est une base, si $r, -r, 1-r$ et $r-1$ sont non congrus modulo p, alors $x/p \in \mathbb{Z}$, ce qui contredit l'hypothèse. Ainsi, l'un de ces 3 cas, qui s'excluent mutuellement, est vérifié :

$$\begin{cases} r \equiv 0 \pmod p \\ r \equiv 1 \pmod p \\ 2r \equiv 1 \pmod p \end{cases}$$

Les deux premiers cas sont impossibles. En effet, si $r \equiv 1 \pmod p$, on a :

$$x\zeta^{-1}(1 + \zeta)\lambda = \beta p, \text{ donc } px^{p-1} = N(\beta)p^{p-1}$$

Alors $p \mid x$ ce qui est faux ici. De même, si r est congru à 0 modulo p, les calculs sont similaires : on remplace x par $-y$ et tombe sur $p \mid y$. Ainsi, $2r \equiv 1 \pmod p$, ce qui permet de terminer la preuve. En effet, on peut simplifier l'égalité :

$$\beta p\zeta^r = x + y\zeta - x\zeta - y = (x - y)\lambda,$$

et en passant à la norme, on obtient $p \mid x - y$. Alors :

$$x \equiv y \pmod p \text{ si bien que } x^p \equiv y^p \pmod p.$$

Par symétrie des rôles, $x^p \equiv z^p \pmod p$. Enfin, en revenant à l'équation de Fermat :

$$3x^p \equiv 0 \pmod p, \text{ donc } p \mid 3x^p.$$

Comme $p > 3$, par le Lemme d'Euclide, p divise x^p donc x, ce qui conclut en fournissant bien une absurdité.

□

5.4 Commentaires et conclusions

Pour conclure, il reste à traiter le cas $p \mid xyz$. C'est la partie de loin la plus ardue de la preuve et on ne la traitera pas. On peut cependant exposer certaines des difficultés.

On peut supposer $p \mid z$ car x, y et z sont premiers entre eux. On remplacera z par $-z$ dans la suite pour mieux visualiser comment l'équation va évoluer. Alors :

$$x^p + y^p = z^p = (z_0 p^m)^p \text{ avec } z_0 \in \mathbb{N}^*, p \nmid z_0.$$

Utilisons la proposition 5.13. Comme p et λ^{p-1} sont associés par le point (iii), il existe $u \in \mathbb{Z}[\zeta]^\times$ tel que :

$$x^p + y^p = (u^m \lambda^{(p-1)m} z_0)^p \text{ et } \lambda \nmid xyz_0$$

En effet, sinon on aurait $xyz_0 \in (\lambda)$ qui est premier par le point (i). Ainsi, on aurait x, y ou z_0 dans $(\lambda) \cap \mathbb{Z} = p\mathbb{Z}$ par le point (ii), ce qui est faux.
Il faut alors montrer que, pour tout $n \in \mathbb{N}^*$ et $\tilde{u} \in \mathbb{Z}[\zeta]^\times$, il n'existe pas de triplet entier $(\alpha, \beta, \gamma) \in \mathbb{Z}^3$ tel que :

$$\alpha^p + \beta^p = \tilde{u} \lambda^{pn} \gamma^p \text{ avec } \lambda \nmid \alpha\beta\gamma.$$

Kummer démontre ce résultat par récurrence sur n, par une méthode de descente assez technique. Le théorème 5.19 ne constitue donc que le cas initial $n = 0$. On remarque également que la nouvelle équation est bien moins commode et symétrique.

Pour traiter le problème de l'unité $\tilde{u}$, Kummer montre alors le lemme suivant. C'est un résultat plus difficile que le reste, qui établi un lien inattendu entre les unités de l'anneau et les classes d'idéaux de l'anneau.

Lemme 5.20. Soit $p > 2$ premier régulier et $u \in \mathbb{Z}[\zeta]^\times$. S'il existe $m \in \mathbb{Z}$ tel que $u = m$ dans $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$. Alors, il existe $v \in \mathbb{Z}[\zeta]^\times$, $u = v^p$.

Remarque 5.21. On l'admettra ici, de la même façon qu'on laissera de côté la récurrence. Ce lemme nécessite de comprendre comment le groupe de Galois agit sur les unités et les idéaux, ou encore de maîtriser les bases de la cohomologie des groupes.

Faisons un peu le bilan. Nous ne connaissons à ce jour pas de preuve complète du Théorème de Fermat-Wiles utilisant ce type d'approche. La démonstration d'Andrew Wiles s'inscrit elle au coeur de la théorie des nombres moderne, via la géométrie algébrique et ses travaux sur les formes modulaires. Indépendamment de ça, Kummer obtient une partie importante du résultat, d'une conjecture vraiment difficile au sens où sa résolution reste assez récente, le tout avec des outils que l'on peut qualifier d'abordables en comparaison. C'est là un tour de force de la théorie qu'a développé Kummer.

Remarque 5.22. Si la résolution couvre probablement un grand nombre de cas, on peut émettre une réserve : l'emploi du terme "probablement" se justifie par le fait qu'on conjecture qu'environ 60% des nombres premiers sont réguliers, mais on ne sait pas le prouver, et on ne sait même pas prouver qu'il en existe une infinité (contrairement aux irréguliers).

Pour terminer, intéressons nous d'avantage à cette proportion des nombres premiers réguliers. Le lemme suivant permet de faire la conjecture probabiliste sur cette proportion, et également de l'appuyer expérimentalement en testant chaque nombre premier très efficacement.

Lemme 5.23. Considérons la suite $(B_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ des nombres de Bernoulli définie notamment par la relation suivante, lorsque le développement a un sens :

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$$

Notons $k_n \in \mathbb{Z}$ le numérateur de B_n dans son écriture en fraction irréductible. Alors, un nombre premier $p > 3$ est régulier si et seulement si :

$$p \nmid k_2,\ p \nmid k_4, \dots \text{ et } p \nmid k_{p-3}$$

Remarque 5.24. Lorsque l'on teste expérimentalement chaque nombre premier pour savoir s'il est régulier, c'est en pratique cette condition que l'on étudie. Elle est en effet plus algorithmique que les méthodes généralisant la correspondance de Gauss, et donc plus commode à programmer et à tester de façon systématique pour un ordinateur.

A Éléments de théorie des modules

Dans toute l'annexe, A désigne un anneau commutatif unitaire. Se placer dans le cadre commutatif permet d'éviter de parler de A-module à gauche ou à droite, cette distinction n'apportant pas grand chose sachant qu'en pratique $A = \mathbb{Z}$ dans le reste du document.

A.1 Définitions

Introduisons d'abord les notions de base de la théorie. Comme dit plus tôt, on notera que, même si cette généralisation du cadre des espaces vectoriels est riche et complexe, les définitions suivantes sont quant à elles des adaptations parfaitement naïves de définitions connues d'algèbre linéaire.

Définition A.1. Un *A-module* est un ensemble M muni de deux lois : Une loi interne notée $+$ telle que $(M, +)$ est un groupe abélien ; et une loi externe $\star : A \times M \longrightarrow M$ qui vérifie :

(i) $a \star (x + y) = a \star x + a \star y$

(ii) $(a + b) \star x = a \star x + b \star x$

(iii) $(ab) \star x = a \star (b \star x)$

(iv) $1_A \star x = x$

et cela pour tout $x, y \in M$ et $a, b \in A$.

Définition A.2. Un *sous-module* N d'un A-module M est un sous ensemble de M tel que :

(i) $(N, +)$ est un sous groupe additif de $(M, +)$

(ii) $\forall (a, x) \in A \times N,\ a \star x \in N$

Lorsqu'il n'y a pas d'ambiguïté sur la loi utilisée, on notera la loi $\star$ plutôt par simple juxtaposition des éléments, i.e. ax au lieu de $a \star x$, comme c'est le cas pour la multiplication dans A.

Définition A.3. Soient M et N deux A-modules. Un *morphisme de A-module* entre M et N est une application $f : M \longrightarrow N$ telle que :

(i) f est un morphisme de groupe additif

(ii) $\forall (a, x) \in A \times M,\ f(ax) = af(x)$

A.2 Autour du théorème de la base adaptée

La structure de module est bien moins simple à manipuler que celle d'espace vectoriel de dimension finie. La notion de dimension n'a en fait pas de sens a priori. Typiquement, l'existence d'une base de cardinal fini pour un module M n'implique pas en général l'existence ne serait-ce que d'une famille génératrice finie pour les sous-modules de M.

Exemple A.4 Le contre exemple classique est le suivant. Prenons :

$$B := \mathbb{K}[X_1, X_2, \dots]$$

l'anneau des polynômes en un nombre quelconque d'indéterminées sur un corps $\mathbb{K}$. Cet anneau est un B-module, et $\{1\}$ en est trivialement une base. Cependant, considérons N le sous-module de B défini par l'ensemble des éléments de B de coefficient constant nul. Alors, N n'admet pas de famille B-génératrice de cardinal fini.

Heureusement, lorsque A est principal, certains résultats conformes à l'intuition demeurent. Le théorème suivant en est un bon exemple, bien que sa démonstration nécessite beaucoup de travail.

Théorème A.5. Soit A un anneau principal et M un A-module possédant une base $(e_1, \ldots, e_n)$ (on dit que M est un module *libre de rang* n). Alors, tout sous-module N possède une base $(a_1 e_1, ..., a_m e_m)$ telle que :

$$\begin{cases} m \leq n \\ a_1, \ldots, a_m \in A^* \\ \forall i \in [\![1, m-1]\!],\ a_i \mid a_{i+1} \end{cases}$$

Remarque A.6. On notera que les sous-modules de $\mathcal{O}_K$ sont exactement ses idéaux, et que par ailleurs $\mathbb{Z}$ est principal. Ce sont ces deux arguments qui permettent d'appliquer le théorème précédent pour démontrer la proposition 2.15.

Références

[1] P. Caldero, *Mini-cours : Anneaux d'entiers d'un corps de nombres*, série de vidéos, chaîne YouTube *Phil Caldero*, 2024.

[2] P. Tauvel, *Corps commutatifs et théorie de Galois*, Calvage & Mounet, 2021.

[3] M. Waldschmidt, *MM020 – Théorie des nombres*, polycopié de cours, Université Pierre et Marie Curie, 2009.

[4] D. Perrin, *L'équation de Bachet*, conférence à Marne-la-Vallée, 2019.

[5] A. Szpirglas, *Algèbre, Tome 3 - Anneaux, polynômes, modules*, Cassini Ed, 2023.

[6] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, 1997.