

Faculté des sciences

Conjugaison de matrices entières et Théorie algébrique des nombres

Auteur : Daniel Altman

Promoteur : Pierre-Emmanuel Caprace

Lecteurs : François Thilmany, Enrico Vitale

Année académique 2025-2026

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
FACULTÉ DES SCIENCES
ÉCOLE DE MATHÉMATIQUES

Conjugaison de matrices entières et Théorie algébrique des nombres

Daniel Altman

Promoteur : Pierre-Emmanuel Caprace
Lecteurs : François Thilmany, Enrico Vitale

Mémoire
Juin 2026

Introduction

Le problème de conjugaison est un problème classique de théorie des groupes apparu en 1911 ([2]). Étant donné un groupe G et deux éléments $a, b \in G$, on dit que a et b sont conjugués s'il existe $c \in G$ tel que $a = cbc^{-1}$. On dit alors que c conjugue a sur b . Le problème de conjugaison pour un certain groupe G consiste à donner une méthode ou un algorithme permettant de calculer si deux éléments de G sont conjugués, en fournissant si possible un élément qui les conjugue. Ce problème peut facilement se généraliser au cas des monoïdes. En effet, étant donné un monoïde M , on peut s'intéresser à l'ensemble des éléments inversibles de M , qui forme un groupe, disons G , et on dira alors que deux éléments $a, b \in M$ sont conjugués s'il existe $c \in G$ tel que $a = cbc^{-1}$. Ce problème est connu pour être indécidable; une preuve détaillée est donnée dans [17]. Pour autant, il existe plusieurs classes de groupes et de monoïdes pour lesquelles un algorithme est connu, on peut penser par exemple à certains types de matrices.

C'est cette piste que l'on va explorer dans ce mémoire en apportant les outils théoriques permettant de résoudre le problème de conjugaison dans $\mathcal{M}_n(\mathbb{Z})$. Dans ce contexte, la relation de conjugaison pour les matrices est exactement la même chose que la relation de similitude. Cette notion nous rappelle d'abord des souvenirs d'algèbre linéaire lorsque nos matrices sont à coefficients dans un corps commutatifs $\mathbb{K}$. Le premier chapitre se concentrera donc sur la résolution du problème de conjugaison dans $\mathrm{GL}_n(\mathbb{K})$. Dans ce cadre, résoudre le problème de conjugaison peut se faire en recherchant une forme canonique pour la matrice, c'est-à-dire, chercher une base où la matrice a des propriétés tellement restrictives, qu'un simple coup d'œil permet de la différencier des autres matrices partageant cette propriété. En ce sens, on apprend en deuxième année de bachelier la forme normale de Jordan, qui a la particularité d'être composée de blocs ayant sur la diagonale une certaine valeur propre et sur la surdiagonale des 1. Ainsi, si deux matrices admettent une telle forme, il suffit de comparer les blocs de Jordan pour savoir si les matrices sont semblables. Plus précisément, si A et B sont deux matrices à coefficients dans un corps qui admettent respectivement J et J' comme forme normale de Jordan, alors A et B sont semblables si et seulement si J et J' sont identiques à l'ordre des blocs près. Un rappel du théorème de Jordan fait l'objet de la toute première section. Pour autant, on n'a pas résolu le problème de conjugaison dans $\mathcal{M}_n(\mathbb{K})$ car il faut que $\mathbb{K}$ soit algébriquement clos pour que toute matrice admette une forme normale de Jordan. C'est pour cela qu'on introduit une autre forme canonique pour ces matrices : la forme normale de Frobenius. Une matrice est sous cette forme lorsqu'elle est composée de blocs compagnons, des blocs qu'on peut facilement associer à un polynôme. De ce fait, la preuve que toute matrice peut se réécrire sous cette forme se fait à travers l'étude des modules

sur l'anneau des polynômes à coefficients dans $\mathbb{K}$. Cet anneau noté $\mathbb{K}[X]$ est euclidien puisque $\mathbb{K}$ est un corps commutatif, et donc il est principal. Il en suit que notre étude des formes canoniques pour $\mathcal{M}_n(\mathbb{K})$ nous fera passer par l'étude plus générale et plus abstraite des modules de torsion de type fini sur un anneau principal. Ainsi, toute la seconde section du premier chapitre aura pour objectif d'apporter les lemmes et le vocabulaire nécessaires pour démontrer le théorème des facteurs invariants.

Théorème (Facteurs invariants). Tout $\mathbb{A}$ -module de torsion de type fini M est isomorphe à un biproduit fini de $\mathbb{A}$ -modules cycliques. De plus, il existe une telle décomposition

$$M \cong \bigoplus_{k=1}^m \mathbb{A}/b_k \mathbb{A},$$

satisfaisant b_{k+1} divise b_k pour tout $k \in \llbracket 1, m-1 \rrbracket$, et cette décomposition est unique.

En plus de résoudre le problème de conjugaison dans $\mathcal{M}_n(\mathbb{K})$, ce théorème va nous permettre dans la dernière section du chapitre de classier à isomorphisme près tous les groupes abéliens finis en les considérant comme des $\mathbb{Z}$ -modules. L'étude des groupes abéliens finis et libres de type fini va nous prodiguer des outils pour les chapitres suivants. L'ensemble des résultats du premier chapitre sont tirés de [14].

En outre, cela résout le problème de conjugaison dans $\mathcal{M}_n(\mathbb{K})$ mais cela ne nous donne qu'une réponse incomplète si l'on s'intéresse à $\mathcal{M}_n(\mathbb{Z})$. En effet, si on a $A, B \in \mathcal{M}_n(\mathbb{Z})$ qui ne sont pas conjugués dans $\mathcal{M}_n(\mathbb{Q})$, alors en particulier ils ne le sont pas dans $\mathcal{M}_n(\mathbb{Z})$, mais si par contre ils sont conjugués dans $\mathcal{M}_n(\mathbb{Q})$, alors on ne peut pas conclure car la matrice de changement de base pourrait avoir des coefficients non entiers. Par exemple, les matrices

$$\begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix}$$

ne sont pas conjuguées dans $\mathcal{M}_2(\mathbb{Z})$, pourtant,

$$\begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 1 & 0 \end{pmatrix}^{-1}.$$

À ce stade, on va avoir besoin d'un arsenal complètement différent pour aborder ce problème de conjugaison : la théorie algébrique des nombres. À l'origine, cette théorie a été développée pour fournir des outils à la résolution d'équations diophantiennes, comme celle du dernier théorème de Fermat, sur lequel il nous sera impossible de ne pas faire de digressions. En effet, au troisième chapitre, on introduit le concept de nombre premier régulier afin de démontrer une version faible du dernier théorème de Fermat que voici.

Théorème (Fermat–Kummer). Soit p un nombre premier régulier, alors l'équation diophantienne $x^p + y^p = z^p$ n'admet aucune solution non triviale.

Pour se faire, l'étude des anneaux p -cyclotomiques est indispensable. Ces anneaux sont de la forme $\mathbb{Z}[\zeta]$ où $\zeta = e^{i\frac{2\pi}{p}}$ avec p un nombre premier impair. On a par exemple dans cet anneau que $1 - \zeta$ est un nombre premier qui divise p . Ce nombre et ses propriétés vont s'avérer centraux dans la démonstration du théorème. La démonstration présentée dans ce mémoire est tirée de [21] et [5].

Savoir comment les nombres premiers se décomposent dans des anneaux du type $\mathbb{Z}[\zeta]$ est au cœur de la théorie algébrique des nombres. Le second chapitre du mémoire consistera donc majoritairement à développer les outils élémentaires de cette théorie. Pour comprendre comment manier ces outils, il est nécessaire de maîtriser certaines bases d'algèbre commutative et de théorie des anneaux. Cela s'explique par le besoin de traduire les propriétés arithmétiques de $\mathbb{Z}$ en propriétés sur les idéaux d'anneaux plus généraux. Par exemple, on étudiera dans la seconde section du deuxième chapitre les anneaux de Dedekind qui ont la particularité de posséder un équivalent au théorème fondamental de l'arithmétique pour leurs idéaux, alors qu'ils ne sont pas forcément factoriels. Pour ce chapitre, on se basera fortement sur [19], [4] et [16].

Par ailleurs, l'étude de ce défaut de factorialité dans ces anneaux sera aussi au centre de ce mémoire car cela va nous amener à considérer un nouveau concept : les classes d'idéaux fractionnaires. Si l'on voit les idéaux d'un anneau intègre $\mathbb{A}$ simplement comme les sous-modules de cet anneau vu comme un module, alors on peut voir les idéaux fractionnaire de $\mathbb{A}$ comme certains types de sous- $\mathbb{A}$ -modules de $\mathbb{K}$ où $\mathbb{K}$ désigne le corps des fractions de $\mathbb{A}$. La condition que doivent satisfaire ces modules I pour être des idéaux fractionnaires est qu'il existe $d \in \mathbb{A}^\times$ tel que $dI \subset \mathbb{A}$. Ceci motive la définition suivante : deux idéaux fractionnaires I et J sont dit équivalents s'il existe $d \in \mathbb{K}$ tel que $J = dI$. Remarquons que cette relation n'admet qu'une classe d'équivalence exactement lorsque l'anneau est principal. Et puisque un anneau de Dedekind a la particularité d'être principal si et seulement s'il est factoriel, on a alors que le nombre de classes d'idéaux fractionnaires mesure à quel point l'anneau n'est pas factoriel. De plus, on peut munir ces classes d'idéaux fractionnaires d'une loi de groupe où le neutre est la classe des idéaux fractionnaires principaux. La troisième section du second chapitre se concentre sur le calcul effectif de ce groupe. Les arguments pour cette section sont tirés de [21] et [19].

De surcroît, on étudiera des anneaux encore plus généraux que les anneaux de Dedekind appelés ordres. Ces ordres admettent des idéaux fractionnaires définis de la même façon, mais la grande différence avec les anneaux de Dedekind, c'est que les classes d'idéaux ne forment plus un groupe mais seulement un monoïde. Le calcul de ce monoïde pour un ordre $\mathcal{O}$ se fera à travers le calcul du groupe des classes d'idéaux fractionnaires inversibles des sur-ordres de $\mathcal{O}$. Ces derniers se calculent via une suite exacte faisant intervenir le groupe de classes d'un anneau de Dedekind, et un certain quotient de cet anneau. Ceci

est vu en détail dans la dernière section du chapitre 2. Les résultats proviennent de [15],[16] et [8].

Une fois tout ce travail effectué, on pourra comprendre les classes d'idéaux fractionnaires des anneaux de la forme $\mathbb{Z}[\alpha]$, qu'ils soient de Dedekind ou non. Cela va nous permettre dans le dernier chapitre de revenir à notre problème de conjugaison de matrices entières grâce au théorème suivant.

Théorème (Latimer–MacDuffee). Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire irréductible de degré $n \geq 1$. Il existe une bijection entre les classes de similitudes de matrices $n \times n$ entières ayant P comme polynôme caractéristique et les classes d'idéaux fractionnaires de $\mathbb{Z}[\alpha]$ où α est une racine de P .

Les sources pour ce chapitre sont [13],[22],[11],[15],[12] et [6].

Ce mémoire repose sur un grand nombre de références, dont l'étude a permis d'explorer en profondeur la théorie algébrique des nombres afin d'en proposer deux applications précises. D'une part, ce travail s'est concentré sur le théorème de Fermat–Kummer et, d'autre part, il s'est penché sur le problème de la conjugaison des matrices entières à travers le théorème de Latimer–MacDuffee. L'une des contributions personnelles de ce travail a consisté à rendre cohérent l'ensemble de la littérature confrontée, celle-ci s'étalant sur près d'un siècle et présentant des approches très variées. Enfin, j'ai enrichi ce mémoire d'exemples originaux, fruits de mon travail personnel. Il est conseillé au lecteur de ce mémoire d'avoir suivi un cours d'algèbre commutative et de théorie de Galois comme LMAT1331 et LMAT1361 donné à l'UCLouvain. En effet, on ne rappelle par exemple pas les théorèmes d'isomorphismes ou le théorème des restes chinois. Les notions plus classiques de ces cours ne seront pas forcément redémontrées, mais certaines seront quand même rappelées si cela s'avère nécessaire. Enfin, ce mémoire est loin de répondre au problème de conjugaison des matrices entières dans son ensemble. Le théorème de Latimer–MacDuffee ne nous donne une réponse que dans le cas où le polynôme caractéristique est irréductible, et même dans ce cas-là, les contraintes calculatoires nous ont forcé à traiter uniquement les matrices 2×2 dans les exemples. Le lecteur intéressé par la littérature récente à ce sujet, ou plus généralement aux solutions algorithmiques, est invité à consulter [11],[15] et [12].

Table des matières

Introduction	5
1 Problème de conjugaison dans $\mathcal{M}_n(\mathbb{K})$	11
1.1 Théorème de Jordan	11
1.2 Théorème des facteurs invariants	12
2 Théorie algébrique des nombres	25
2.1 Corps de nombres et anneaux d'entiers	25
2.2 Anneaux de Dedekind	40
2.3 Groupe des classes d'idéaux	49
2.4 Ordre d'un corps de nombres et conducteur	63
3 Dernier théorème de Fermat	75
4 Problème de conjugaison dans $\mathcal{M}_n(\mathbb{Z})$	87

Chapitre 1

Problème de conjugaison dans $\mathcal{M}_n(\mathbb{K})$

Tout au long de ce mémoire, les anneaux seront considérés unitaires et commutatifs et les sous-anneaux d'un anneau seront eux-aussi considérés unitaires. Le symbole $\mathbb{A}$ désignera toujours un anneau intègre. Pour tout anneau $\mathbb{A}$, le symbole $\mathbb{A}^\times$ désigne les éléments inversibles de $\mathbb{A}$ pour la multiplication et le symbole $\mathbb{A}^*$ désigne l'anneau $\mathbb{A}$ privé de son élément neutre additif. On étend cette notation aux entiers naturels, c'est-à-dire $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$.

1.1 Théorème de Jordan

Cette première section introductive sert uniquement à rappeler certains résultats d'algèbre linéaire rencontrés en bachelier, en lien avec le problème de conjugaison dans $\mathcal{M}_n(\mathbb{K})$. Le lecteur intéressé par les preuves des théorèmes présentés ou des exemples peut consulter [14].

Définition 1.1.1 (Bloc de Jordan). Soit $\mathbb{K}$ un corps commutatif et $a \in \mathbb{K}$. On appelle *bloc de Jordan* de a d'échelon m , toute matrice carré $m \times m$ de la forme

$$J_m(a) = \begin{pmatrix} a & 1 & 0 & 0 & \cdots & 0 \\ 0 & a & 1 & 0 & \cdots & 0 \\ 0 & 0 & a & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a & 1 \\ 0 & 0 & 0 & 0 & \cdots & a \end{pmatrix}.$$

Définition 1.1.2 (Forme normale de Jordan). Soit $\mathbb{K}$ un corps commutatif. On dit qu'une matrice admet une *forme normale de Jordan*, ou est *jordanisable* sur $\mathbb{K}$ si elle est

semblable à une matrice diagonale par blocs de la forme

$$\begin{pmatrix} J_{m_1}(a_1) & & & & \\ & J_{m_2}(a_2) & & & \\ & & J_{m_3}(a_3) & & \\ & & & \ddots & \\ & & & & J_{m_k}(a_k) \end{pmatrix},$$

où chaque $J_{m_i}(a_i)$ est le bloc de Jordan de $a_i \in \mathbb{K}$ d'échelon m_i .

Théorème 1.1.3 (Jordan). *Toute matrice à coefficients dans un corps commutatif, dont le polynôme caractéristique est scindé, est jordanisable sur ce corps.*

Corollaire 1.1.4. *Si $\mathbb{K}$ est un corps algébriquement clos, alors $A, B \in \mathcal{M}_n(\mathbb{K})$ sont semblables si et seulement s'ils ont la même forme normale de Jordan, à l'ordre des blocs près.*

1.2 Théorème des facteurs invariants

Le corollaire 1.1.4 ne nous donne une solution au problème de conjugaison dans $\mathcal{M}_n(\mathbb{K})$ que lorsque $\mathbb{K}$ est algébriquement clos. On a donc besoin d'une forme canonique plus générale que celle de Jordan. Le théorème des facteurs invariants va nous aider à trouver cette forme canonique.

1.2.1 Modules noethériens

Définition 1.2.1 (Module noethérien). Un $\mathbb{A}$ -module M est dit *noethérien* s'il satisfait la condition de la chaîne ascendante, c'est-à-dire que toute chaîne $H_1 \subset H_2 \subset H_3 \subset \dots$, de sous-modules de M est stationnaire.

Définition 1.2.2 (Anneau noethérien). Un anneau $\mathbb{A}$ est dit *noethérien* s'il est noethérien en tant que $\mathbb{A}$ -module sur lui-même.

Proposition 1.2.3. *Un $\mathbb{A}$ -module est noethérien si et seulement si tous ses sous-modules sont de type fini.*

Démonstration. Soit M un $\mathbb{A}$ -module noethérien et H un sous-module de M . Supposons par l'absurde que H n'est pas de type fini. En particulier, en prenant $h_1 \in H$, h_1 n'engendre pas H . Cela implique qu'il existe $h_2 \in H \setminus \langle h_1 \rangle$, et par hypothèse, $H \neq \langle h_1, h_2 \rangle$. Il en suit qu'il existe $h_3 \in H \setminus \langle h_1, h_2 \rangle$. Ainsi de suite, on crée une chaîne ascendante

$\langle h_1 \rangle \subset \langle h_1, h_2 \rangle \subset \langle h_1, h_2, h_3 \rangle \subset \dots$ de $\mathbb{A}$ -modules qui n'est pas stationnaire. On obtient donc une contradiction.

Réciproquement, prenons M un $\mathbb{A}$ -module ayant la propriété que tous ses sous-modules soient de type fini. Étant donné une chaîne de sous-modules de $M : H_1 \subset H_2 \subset H_3 \subset \dots$, on peut considérer $H = \bigcup_{k \in \mathbb{N}^*} H_k$ qui est aussi un sous-module de M . Par hypothèse, il existe $m_1, \dots, m_l \in M$ tels que $H = \langle m_1, \dots, m_l \rangle$, et la définition de H nous dit que pour tout $k \in \llbracket 1, l \rrbracket$, il existe $s \in \mathbb{N}^*$ tel que $m_k \in H_s$. On peut prendre alors t comme le plus grand de ses indices s , et on obtient que $m_k \in H_t$ pour tout $k \in \llbracket 1, l \rrbracket$. Il en suit que $H \subset H_t$, ce qui conclut. $\square$

Définition 1.2.4 (Anneau principal). Un anneau intègre est dit *principal* si tous ses idéaux sont principaux.

Proposition 1.2.5. *Tout anneau principal est noethérien.*

Démonstration. D'après la proposition 1.2.3, un anneau est noethérien si et seulement si tous ses idéaux sont finiment engendrés, et ceci est le cas pour les anneaux principaux. $\square$

Proposition 1.2.6. *Soit $\mathbb{B}$ un anneau et $\mathbb{A}$ un sous-anneau de $\mathbb{B}$. Si $\mathbb{B}$ est un $\mathbb{A}$ -module de type fini, alors les $\mathbb{B}$ -modules de type fini sont des $\mathbb{A}$ -modules de type fini.*

Démonstration. Soit $M = \langle m_1, \dots, m_l \rangle$ un $\mathbb{B}$ -module de type fini, cela veut dire que pour tout $m \in M$, il existe $b_1, \dots, b_l$ tels que

$$m = \sum_{i=1}^l b_i m_i$$

Si $\mathbb{B}$ est un $\mathbb{A}$ module de type fini, cela veut dire qu'il existe $b'_1, \dots, b'_n \in \mathbb{B}$ satisfaisant la propriété que pour tout $b \in \mathbb{B}$, il existe $a_1, \dots, a_n \in \mathbb{A}$ tels que

$$b = \sum_{j=1}^n a_j b'_j.$$

En particulier, pour tout $i \in \llbracket 1, l \rrbracket$, il existe $a_{i,1}, a_{i,2}, \dots, a_{i,n}$ tels que

$$b_i = \sum_{j=1}^n a_{i,j} b'_j.$$

Ainsi, pour tout $m \in M$, on a

$$m = \sum_{i=1}^l b_i m_i = \sum_{i=1}^l \left(\sum_{j=1}^n a_{i,j} b'_j \right) m_i = \sum_{i=1}^l \sum_{j=1}^n a_{i,j} (b'_j m_i).$$

Ce qui conclut. □

Proposition 1.2.7. *Étant donné une suite exacte courte $0 \rightarrow K \xrightarrow{i} M \xrightarrow{q} Q \rightarrow 0$ de $\mathbb{A}$ -modules, on a que M est noethérien si et seulement si K et Q le sont.*

Démonstration. Montrons d'abord que si M est noethérien, alors K et Q le sont. Le fait que K le soit découle de la proposition 1.2.3. Ensuite, le premier théorème d'isomorphisme nous dit que $Q \cong M/K$, on a alors que les sous-modules de Q sont en bijection (croissante) avec les sous-modules de M contenant K . Puisque M est noethérien, il satisfait la condition de la chaîne ascendante et donc Q aussi. On a donc bien que Q est noethérien.

Réciproquement, étant donné une chaîne de sous-modules de $M : H_1 \subset H_2 \subset H_3 \subset \dots$, on peut considérer les chaînes de sous-modules de K et Q suivante : $i^{-1}(H_1) \subset i^{-1}(H_2) \subset i^{-1}(H_3) \subset \dots$ et $q(H_1) \subset q(H_2) \subset q(H_3) \subset \dots$. Puisque K et Q sont noethériens, il existe $r, t \in \mathbb{N}^*$ tels que pour tout $n \geq r$ et tout $n' \geq t$, on aie $i^{-1}(H_n) = i^{-1}(H_r)$ et $q(H_{n'}) = q(H_t)$. On a donc en particulier que $i^{-1}(H_n) = i^{-1}(H_m)$ et $q(H_n) = q(H_m)$ pour tout $n \geq m$ où $m = \max(r, t)$. Montrons alors que pour tout $n \geq m$, on a $H_n = H_m$. On a déjà par hypothèse que $H_m \subset H_n$, on va donc montrer l'autre inclusion. Soit $x \in H_n$, on a $q(x) \in q(H_n) = q(H_m)$, cela veut dire qu'il existe $y \in H_m$ tel que $q(x) = q(y)$. On a donc $x - y \in \text{Ker}(q) = \text{Im}(i)$ car $q(x - y) = q(x) - q(y) = 0$. Il existe ainsi $z \in K$ tel que $i(z) = x - y$, mais $x - y \in H_n$ car $x, y \in H_n$, et donc $z \in i^{-1}(H_n) = i^{-1}(H_m)$. Il en suit qu'il existe $w \in H_m$ tel que $i(z) = w$, on trouve donc $x - y = i(z) = w \in H_m$, ce qui implique $x \in H_m$ car $y \in H_m$. □

En particulier, tout quotient d'un module noethérien est noethérien.

Proposition 1.2.8. *Si $\mathbb{A}$ est un anneau noethérien, tout $\mathbb{A}$ -module de type fini est noethérien.*

Démonstration. Montrons d'abord que $\mathbb{A}^n$ est noethérien pour tout $n \in \mathbb{N}^*$ et procédons par récurrence car l'initialisation est déjà vérifiée par l'hypothèse. Pour l'hérédité, on considère la suite exacte courte $0 \rightarrow \mathbb{A}^{n-1} \xrightarrow{i} \mathbb{A}^n \xrightarrow{q} \mathbb{A} \rightarrow 0$ et on applique la proposition 1.2.7. Ensuite, prenons $M = \langle t_1, \dots, t_m \rangle$ un $\mathbb{A}$ -module de type fini quelconque, on sait qu'il existe un morphisme surjectif canonique $r : \mathbb{A}^m \rightarrow M$. On conclut encore une fois par la proposition 1.2.7. □

1.2.2 Modules cycliques

À partir de maintenant et jusqu'à la fin du chapitre, l'anneau $\mathbb{A}$ est principal.

Définition 1.2.9 (Module cyclique). Un $\mathbb{A}$ -module M est dit *cyclique* s'il est engendré par un seul élément, c'est-à-dire, s'il existe $m \in M$ tel que pour tout $m' \in M$, il existe $a \in \mathbb{A}$ satisfaisant $a \cdot m = m'$.

Proposition 1.2.10. Les $\mathbb{A}$ -modules cycliques sont à isomorphisme près les quotients de $\mathbb{A}$.

Démonstration. Si $M = \langle m \rangle$ est un module cyclique, cela veut dire que le morphisme $t : \mathbb{A} \rightarrow M : x \mapsto x \cdot m$ est surjectif. Par le premier théorème d'isomorphisme, on a $M \cong \mathbb{A}/\text{Ker}(t)$ mais $\text{Ker}(t)$ est un sous-module de $\mathbb{A}$, donc un idéal, ce qui conclut. $\square$

Définition 1.2.11 (Associés). Soit $\mathbb{A}$ un anneau et $a, b \in \mathbb{A}^*$, on dit que a et b sont *associés* si a divise b et b divise a , ou de façon équivalente, si les idéaux $a\mathbb{A}$ et $b\mathbb{A}$ sont égaux.

Définition 1.2.12. Tout $\mathbb{A}$ -module cyclique M est isomorphe à $\mathbb{A}/b\mathbb{A}$ par la proposition 1.2.10. Cet élément $b \in \mathbb{A}$ est appelé l'*ordre* de M .

L'ordre d'un module cyclique est unique à relation d'association près. Remarquons d'une part que $b = 0$ si et seulement si $M \cong \mathbb{A}$, et d'autre part, on a que $a \cdot m = 0$ si et seulement si $a \in b\mathbb{A}$.

Lemme 1.2.13. Soit C un $\mathbb{A}$ -module cyclique d'ordre $ab \neq 0$, s'il existe $m \in C$ tel que $a \cdot m = 0$, alors il existe $t \in C$ tel que $m = b \cdot t$.

Démonstration. Disons que $C = \langle c \rangle$, il existe alors $x \in \mathbb{A}$ tel que $m = x \cdot c$ et donc $a \cdot m = ax \cdot c = 0$. Il en suit que ab divise ax et donc b divise x puisque $\mathbb{A}$ est intègre. Cela veut dire qu'il existe $d \in \mathbb{A}$ tel que $bd = x$, on pose alors $t = d \cdot c$ et on obtient bien $b \cdot t = bd \cdot c = x \cdot c = m$. $\square$

Lemme 1.2.14. Soit M un $\mathbb{A}$ -module cyclique et L un sous-module de M tel que $M/L \not\cong \mathbb{A}$ soit cyclique. Soit $m_0 + L$ son générateur, d'ordre n , on a la suite exacte courte de $\mathbb{A}$ -modules

$$0 \longrightarrow \mathbb{A} \xrightarrow{f} L \oplus \mathbb{A} \xrightarrow{g} M \longrightarrow 0$$

où $f : a \mapsto (an \cdot m_0, -na)$ et $g : (l, a) \mapsto l + a \cdot m_0$.

Démonstration. On a bien que f est injectif car $\mathbb{A}$ est intègre. Puisque $m_0 + L$ engendre M/L , on a que tout élément de M est de la forme $a \cdot m_0 + l$ pour $a \in \mathbb{A}$ et $l \in L$ et donc g est surjectif. Ensuite, $g(f(a)) = g(an \cdot m_0, -n \cdot a) = an \cdot m_0 - an \cdot m_0 = 0$. Enfin, si $(l, a) \in \text{Ker}(g)$, alors $-a \cdot m_0 = l \in L$ et donc n divise a , c'est-à-dire qu'il existe $x \in \mathbb{A}$ tel que $a = -nx$. Ainsi, $(l, a) = (-a \cdot m_0, -nx) = (nx \cdot m_0, -nx)$ et donc $\text{Ker}(g) = \text{Im}(f)$, ce qui conclut. $\square$

Proposition 1.2.15. Soit C un $\mathbb{A}$ -module cyclique d'ordre $n \neq 0$, M un $\mathbb{A}$ -module noethérien tel que $n \cdot m = 0$ pour tout $m \in M$ et L un sous-module de M . Pour tout morphisme $h : L \rightarrow C$, il existe un morphisme $k : M \rightarrow C$ tel que $k \circ \iota = h$, où $\iota : L \rightarrow M$ est le morphisme d'inclusion. On dit alors que k prolonge h .

Démonstration. Supposons d'abord que $M = \langle L, m \rangle$. Puisque $n \cdot m = 0$, l'ordre ν de la classe $m + L \in M/L$ divise n . Cela veut dire qu'il existe $d \in \mathbb{A}$ tel que $d\nu = n$ et donc $dh(\nu \cdot m) = h(d\nu \cdot m) = h(n \cdot m) = h(0) = 0$. D'après le lemme 1.2.13, il existe $t \in C$ tel que $h(\nu \cdot m) = \nu \cdot t$. On définit alors le morphisme $h' : L \oplus \mathbb{A} \rightarrow C : (x, a) \mapsto h(x) + a \cdot t$. Soit $f : \mathbb{A} \rightarrow L \oplus \mathbb{A}$ et $g : L \oplus \mathbb{A} \rightarrow M$ définies comme dans le lemme 1.2.14, alors $h' \circ f = 0$, et puisque g est le conoyau de f , on trouve le morphisme $k : M \rightarrow C$ à l'aide de la propriété universelle du conoyau.

Attaquons-nous maintenant au cas général. Puisque M est noethérien, il existe des éléments $m_1, \dots, m_l \in M$ tels que $M = \langle L, m_1, \dots, m_l \rangle$. En définissant $L_i = \langle L, m_1, \dots, m_i \rangle$ pour tout $i \in \llbracket 1, l \rrbracket$, on obtient par le point précédent un morphisme $k_1 : L_1 \rightarrow C$ qui prolonge h . Mais pour tout $i \in \llbracket 2, l \rrbracket$, $L_i = \langle L_{i-1}, m_i \rangle$, on obtient donc successivement des prolongements k_i , jusqu'au prolongement $k_l : M \rightarrow C$ qu'on recherchait. $\square$

Définition 1.2.16 (Facteur direct). Soient M et L deux $\mathbb{A}$ -modules. On dit que L est un *facteur direct* de M s'il existe un $\mathbb{A}$ -module H tel que $M \cong L \oplus H$.

Corollaire 1.2.17. Soit M un $\mathbb{A}$ -module noethérien et C un sous-module cyclique de M d'ordre $n \neq 0$ tel que $n \cdot m = 0$ pour tout $m \in M$. Alors, C est un facteur direct de M .

Démonstration. En appliquant la proposition 1.2.15 à notre cas en prenant $L = C$ et h l'identité sur C , on trouve $k : M \rightarrow C$ tel que $k \circ \iota = 1_C$ où $\iota : C \rightarrow M$ est le morphisme d'inclusion. On a alors que $\text{Ker}(k)$ est un sous-module de M satisfaisant $C \cap \text{Ker}(k) = \emptyset$. Remarquons que tout $m \in M$ s'écrit comme $m = \iota \circ k(m) + (m - \iota \circ k(m))$, on a bien sûr que $\iota \circ k(m) \in C$ mais aussi $(m - \iota \circ k(m)) \in \text{Ker}(k)$ car

$$k(m - \iota \circ k(m)) = k(m) - k \circ \iota \circ k(m) = k(m) - k(m) = 0.$$

Ainsi, $M = C + \text{Ker}(k)$, ce qui conclut. $\square$

1.2.3 Modules de torsion

Définition 1.2.18. Soit M un $\mathbb{A}$ -module. Un élément $m \in M$ est dit de *torsion* s'il existe $a \in \mathbb{A}^*$ tel que $a \cdot m = 0$. Puisqu'on considère que $\mathbb{A}$ est principal, le noyau du morphisme $f_m : \mathbb{A} \rightarrow M : a \mapsto a \cdot m$ est un idéal principal, et on appelle son générateur l'*ordre* de m .

Remarquons que l'ordre d'un élément de torsion est non nul et qu'il est unique à relation d'association près.

Définition 1.2.19 (Torsion). Un $\mathbb{A}$ -module est dit de *torsion* si tous ses éléments sont de torsion.

Définition 1.2.20 (Annulateur minimal). Soit M un $\mathbb{A}$ -module de torsion de type fini. L'ensemble des $s \in \mathbb{A}$ tels que $s \cdot m = 0$ pour tout $m \in M$ est un idéal de $\mathbb{A}$ et son générateur est appelé *annulateur minimal* de M .

On rappelle les définitions et propositions d'algèbre commutative suivantes. Le lecteur peut trouver les preuves dans [23].

Définition 1.2.21 (Irréductible). Soit $\mathbb{A}$ un anneau. On dit que $x \in \mathbb{A} \setminus \mathbb{A}^\times$ est *irréductible* si chacun de ses diviseurs est soit inversible, soit associé à x .

Définition 1.2.22 (Factoriel). Un anneau intègre est dit *factoriel* ou *gaussien* si tous ses éléments non inversibles admettent une décomposition essentiellement unique en facteurs irréductibles.

Définition 1.2.23 (PGCD). Soit $\mathbb{A}$ un anneau intègre et $a, b \in \mathbb{A}^*$. On dit que $d \in \mathbb{A}^*$ est un PGCD de a et b si d divise a et b et si pour tout $c \in \mathbb{A}^*$ qui divise a et b , on a que c divise d . On note $d = \text{PGCD}(a, b)$.

Remarquons que le PGCD est unique à relation d'association près.

Proposition 1.2.24. Dans un anneau factoriel, deux éléments non nuls admettent toujours un PGCD.

Définition 1.2.25 (Copremiers). Soit $\mathbb{A}$ un anneau intègre et $a, b \in \mathbb{A}^*$. On dit que a et b sont *copremiers* ou *premiers entre eux* s'ils admettent 1 comme leur PGCD.

Proposition 1.2.26. Tout anneau principal est factoriel.

Théorème 1.2.27 (Bézout). Soit $\mathbb{A}$ un anneau principal et $a, b \in \mathbb{A}^*$. Si $d = \text{PGCD}(a, b)$, alors il existe $u, v \in \mathbb{A}$ tels que $au + bv = d$.

Proposition 1.2.28. Soient m et m' des éléments d'un $\mathbb{A}$ -module ayant respectivement pour ordre n et n' non nuls, si n et n' sont premiers entre eux, alors $m + m'$ a pour ordre nn' .

Démonstration. Soit ν l'ordre de $m+m'$, on doit montrer que ν est associé à nn' . D'après le théorème de Bézout 1.2.27, il existe $u, v \in \mathbb{A}$ tels que $nu + n'v = 1$. On a alors

$$(m + m') \cdot n'v = m \cdot n'v + m' \cdot n'v = m \cdot n'v = m \cdot (1 - nu) = m - m \cdot nu = m,$$

donc $m \in \langle m + m' \rangle$, et similairement, on trouve $m' \in \langle m + m' \rangle$. Il en découle que $\nu \cdot m = 0 = \nu m'$ et donc n et n' divisent ν . Puisque n et n' sont premiers entre eux et que $\mathbb{A}$ est factoriel d'après la proposition 1.2.26, on a que nn' divise ν . Remarquons maintenant que

$$(m + m') \cdot nn' = m \cdot nn' + m' \cdot n'n = 0 + 0 = 0,$$

et donc ν divise nn' , ce qui conclut. $\square$

Lemme 1.2.29. *Un $\mathbb{A}$ -module M de torsion de type fini et d'annulateur minimal a admet un élément d'ordre a .*

Démonstration. Puisque $\mathbb{A}$ est principal, il est aussi factoriel par la proposition 1.2.26. On a alors la décomposition suivante $a = \varepsilon p_1^{e_1} \cdots p_s^{e_s}$ où $\varepsilon \in \mathbb{A}^\times$ et les p_k sont irréductibles. Ensuite, puisque pour tout $k \in \llbracket 1, s \rrbracket$, on a que $\frac{a}{p_k} \notin a\mathbb{A}$, il existe $\beta_k \in M$ tel que $\frac{a}{p_k} \cdot \beta_k \neq 0$. Remarquons alors que $\delta_k := \frac{a}{p_k^{e_k}} \beta_k$ est d'ordre $p_k^{e_k}$. Puisque les $p_k^{e_k}$ sont premiers entre eux, on obtient par la proposition 1.2.28 que $\sum_{k=1}^s \delta_k$ est d'ordre $\prod_{k=1}^s p_k^{e_k} = \frac{a}{\varepsilon}$. On conclut car ε est inversible. $\square$

Théorème 1.2.30 (Facteurs invariants). *Tout $\mathbb{A}$ -module de torsion de type fini M est isomorphe à un biproduct fini de $\mathbb{A}$ -modules cycliques. De plus, il existe une telle décomposition*

$$M \cong \bigoplus_{k=1}^m \mathbb{A}/b_k \mathbb{A},$$

satisfaisant b_{k+1} divise b_k pour tout $k \in \llbracket 1, m-1 \rrbracket$, et cette décomposition est unique.

Démonstration. Montrons premièrement que M est isomorphe à un biproduct fini de $\mathbb{A}$ -modules cycliques. Si on note a l'annulateur minimal de $\mathbb{A}$, le lemme 1.2.29 nous dit qu'il existe un élément de M d'ordre a , disons c_1 . On obtient alors un sous-module cyclique $C_1 = \langle c_1 \rangle$ de M d'ordre a , et d'après le corollaire 1.2.17, il existe M_2 un sous-module de M tel que $M \cong C_1 + M_2$. De même, si on note a_2 l'annulateur minimal de M_2 , on obtient par les mêmes arguments une décomposition $M_2 \cong C_2 + M_3$ où C_2 et M_3 sont des sous-modules de M_2 avec C_2 cyclique d'ordre a_2 . On obtient alors $M \cong C_1 + C_2 + M_3$. En continuant ainsi, on obtient une chaîne ascendante de sous-modules de M : $C_1 \subset C_1 + C_2 \subset C_1 + C_2 + C_3 \subset \cdots$, qui est stationnaire si M est noethérien. C'est bien le cas : $\mathbb{A}$ est principal donc noethérien d'après la proposition 1.2.5,

donc M est noethérien par la proposition 1.2.8. On obtient alors qu'il existe $m \in \mathbb{N}^*$ tel que

$$M \cong \bigoplus_{k=1}^m C_k.$$

Pour le second point, montrons d'abord que la longueur de telles décompositions est nécessairement unique. Supposons par l'absurde que

$$M \cong \bigoplus_{k=1}^m \mathbb{A}/b_k \mathbb{A} \cong \bigoplus_{k=1}^l \mathbb{A}/d_k \mathbb{A}$$

avec $m > l$ et b_{k+1} divisant b_k pour tout $k \in \llbracket 1, m-1 \rrbracket$ et d_{k+1} divisant d_k pour tout $k \in \llbracket 1, l-1 \rrbracket$. On a que b_m n'est pas inversible, il existe donc un élément irréductible $p \in \mathbb{A}$ divisant b_m puisque $\mathbb{A}$ est factoriel d'après la proposition 1.2.26. On a alors que p divise b_k pour tout $k \in \llbracket 1, m \rrbracket$ et donc d'après les théorèmes d'isomorphisme, on a

$$M/p\mathbb{A} \cong \bigoplus_{k=1}^m (\mathbb{A}/b_k \mathbb{A})/p(\mathbb{A}/b_k \mathbb{A}) \cong \bigoplus_{k=1}^m \mathbb{A}/p\mathbb{A}.$$

En posant $h = \max\{k \in \llbracket 1, l \rrbracket : p|d_k\}$ si h divise l'un des d_k et $h = 0$ sinon ; on obtient une seconde décomposition de la même façon

$$M/p\mathbb{A} \cong \bigoplus_{k=1}^h (\mathbb{A}/d_k \mathbb{A})/p(\mathbb{A}/d_k \mathbb{A}) \cong \bigoplus_{k=1}^h \mathbb{A}/p\mathbb{A}.$$

Remarquons que p est irréductible et donc $p\mathbb{A}$ est un idéal maximal de $\mathbb{A}$. Ainsi, $\mathbb{A}/p\mathbb{A}$ est un corps et $M/p\mathbb{A}$ est un $\mathbb{A}/p\mathbb{A}$ -espace vectoriel de dimension m mais aussi de dimension $h \leq l < m$, ce qui n'est pas possible. On en déduit que $m = l$.

Ensuite, supposons par l'absurde que les idéaux $b_k \mathbb{A}$ et $d_k \mathbb{A}$ ne soient pas tous égaux deux à deux, on peut alors définir $r = \min\{k \in \llbracket 1, m \rrbracket \mid b_k \mathbb{A} \neq d_k \mathbb{A}\}$. On a alors que b_r et d_r ne sont pas associés. Supposons alors sans perte de généralité que d_r ne divise pas b_r . Les théorèmes d'isomorphismes nous donnent que $b_r(\mathbb{A}/b_k \mathbb{A}) \cong 0$ pour tout $k \in \llbracket r, m \rrbracket$. Ainsi, la première décomposition

$$b_r M \cong \bigoplus_{k=1}^m b_r(\mathbb{A}/b_k \mathbb{A}) \cong \bigoplus_{k=1}^{r-1} b_r(\mathbb{A}/b_k \mathbb{A})$$

a au plus $r-1$ facteurs cycliques non nuls. Mais de la même façon, on a $b_r(\mathbb{A}/d_k \mathbb{A})$ non nul pour tout $k \in \llbracket 1, r \rrbracket$ puisque d_r ne divise pas b_r . On a donc que la deuxième décomposition

$$b_r M \cong \bigoplus_{k=1}^m b_r(\mathbb{A}/d_k \mathbb{A})$$

a au moins r facteurs cycliques non nuls. Ceci contredit l'unicité de la longueur de la décomposition de $b_r M$ en somme directe de modules cycliques, qu'on a prouvé précédemment. $\square$

1.2.4 Groupes abéliens de type fini

Groupes abéliens finis

Une première application du théorème des facteurs invariants 1.2.30 est le théorème de Kronecker qui classifie tous les groupes abéliens finis. Pour ce faire, il suffit de voir qu'un groupe abélien est exactement la même chose qu'un $\mathbb{Z}$ -module. On obtient alors directement les propositions suivantes. On se permet cette digression car on aura l'occasion plus tard de manipuler des groupes abéliens finis.

Définition 1.2.31 (Groupe noethérien). Un groupe abélien est dit *noethérien* si tous ses sous-groupes sont de type fini.

Corollaire 1.2.32. *Les groupes abéliens de type fini sont des groupes noethériens.*

Démonstration. Puisque $\mathbb{Z}$ est principal donc noethérien par la proposition 1.2.5, on peut simplement appliquer la proposition 1.2.8. $\square$

Théorème 1.2.33 (Kronecker). *Pour tout groupe abélien G de torsion de type fini, il existe une unique liste $n_1, \dots, n_m \in \mathbb{N}^*$ telle que*

$$G \cong \bigoplus_{k=1}^m \mathbb{Z}/n_k \mathbb{Z}$$

avec n_{k+1} qui divise n_k pour tout $k \in \llbracket 1, m-1 \rrbracket$.

Démonstration. On applique le théorème des facteurs invariants au cas $\mathbb{A} = \mathbb{Z}$. $\square$

Remarquons qu'on obtient un corollaire intéressant.

Corollaire 1.2.34. *Tout groupe abélien de torsion de type fini est fini.*

Groupes abéliens libres de type fini

Nous poussons plus loin la digression sur les groupes abéliens de type fini afin d'y ajouter un théorème qui va s'avérer utile pour la suite.

Proposition 1.2.35. *Soit G un groupe abélien libre de rang n et H un sous-groupe de même rang, avec pour $\mathbb{Z}$ -bases respectives $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$. Si $y = xB$ pour $B = (b_{ij})_{i,j \in \llbracket 1, n \rrbracket}$, alors $|G/H| = |\det(B)|$.*

Démonstration. Il s'avère que G et H ont aussi pour $\mathbb{Z}$ -bases respectives $u = (u_1, \dots, u_n)$ et $v = (v_1, \dots, v_n)$ avec $v_k = d_k u_k$, $d_k \in \mathbb{N}^*$ pour $k \in \llbracket 1, n \rrbracket$ et $|G/H| = \prod_{k=1}^n d_k$. Il existe alors $A, C \in \text{GL}_n(\mathbb{Z})$ tels que $u = xA$ et $v = yC$ et en posant $D = \text{diag}(d_1, \dots, d_n)$, on trouve $B = ADC^{-1}$. Finalement,

$$\begin{aligned} |\det(B)| &= |\det(A)| \cdot |\det(D)| \cdot |\det(C^{-1})| = |\pm 1| \cdot |\det(D)| \cdot |\pm 1| \\ &= |\det(D)| = \prod_{k=1}^n d_k = |G/H|. \end{aligned}$$

□

1.2.5 Forme normal de Frobenius

Nous allons maintenant voir comment le théorème des facteurs invariants 1.2.30 nous permet de répondre au problème de conjugaison dans $\mathcal{M}_n(\mathbb{K})$.

Définition 1.2.36 (Matrice compagne). Pour $P(X) = X^m + a_{m-1}X^{m-1} + a_{m-2}X^{m-2} + \dots + a_1X + a_0 \in \mathbb{A}[X]$, on définit la *matrice compagne* de P comme

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{pmatrix}.$$

On rappelle informellement la définition et les propositions suivantes. Le lecteur peut trouver les preuves dans [23].

Définition 1.2.37 (Anneau euclidien). Un anneau intègre est dit *euclidien* s'il est possible d'y définir une division euclidienne.

Proposition 1.2.38. *Tout anneau euclidien est principal.*

Proposition 1.2.39. *Soit $\mathbb{K}$ un corps commutatif. On a que l'anneau $\mathbb{K}[X]$ est euclidien, et donc principal.*

Proposition 1.2.40. *Soit $\mathbb{K}$ un corps commutatif, on a une bijection entre les $\mathbb{K}[X]$ -modules et les $\mathbb{K}$ -espaces vectoriels munis d'un endomorphisme.*

Démonstration. Soit M un $\mathbb{K}[X]$ -module, c'est en particulier un $\mathbb{K}$ -module donc un $\mathbb{K}$ -espace vectoriel. En posant $t(y) := X \cdot y$, la multiplication par le scalaire X provenant de la structure de $\mathbb{K}[X]$ -module de M , on obtient bien un endomorphisme du $\mathbb{K}$ -espace vectoriel M . Réciproquement, étant donné V un $\mathbb{K}$ -espace vectoriel et t un endomorphisme de V , on pose comme multiplication scalaire par X , $X \cdot v := t(v)$. En gardant la multiplication scalaire comme elle est pour les éléments de $\mathbb{K}$, on obtient une multiplication scalaire définie pour tous les éléments de $\mathbb{K}[X]$, ce qui munit V d'une structure de $\mathbb{K}[X]$ -module. Les deux fonctions ainsi définies sont clairement inverse l'une de l'autre. $\square$

Notons Ψ cette bijection (de domaine les espaces vectoriels muni d'un endomorphisme).

Proposition 1.2.41. *Si V est un $\mathbb{K}$ -espace vectoriel de dimension finie muni d'un endomorphisme t , alors $\Psi(V, t)$ est un $\mathbb{K}[X]$ -module de torsion de type fini et le polynôme minimal de t est l'annulateur minimal de $\Psi(V, t)$.*

Démonstration. Si V est un $\mathbb{K}$ -espace vectoriel de dimension finie, cela veut dire que c'est un $\mathbb{K}$ -module de type fini, et en particulier c'est un $\mathbb{K}[X]$ -module de type fini car $\mathbb{K} \subset \mathbb{K}[X]$. Ensuite, étant donné $v \in V \setminus \{0\}$, si on note $n = \dim_{\mathbb{K}}(V)$, on a que $v, t(v), t^2(v), \dots, t^n(v)$ ne sont pas linéairement indépendants. Il existe donc $a_0, \dots, a_n \in \mathbb{K}$ tels que $\sum_{k=0}^n a_k t^k(v) = 0$. Ainsi, en prenant $P = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$, on obtient $P \cdot v = 0$, et donc v est un élément de torsion. Enfin, si $T \in \mathbb{K}[X]$ est tel que $T \cdot v = 0$ pour tout $v \in V$, alors $T(t) = 0$ et donc le polynôme minimal de t divise T . $\square$

Définition 1.2.42. Soit V un espace vectoriel et t un endomorphisme de V . On dit qu'un sous-espace vectoriel W de V est *t -invariant* si $t(W) \subset W$. On dit qu'il est *t -cyclique* si de plus, il existe $w \in W$ et $n \in \mathbb{N}$ tel que $W = \text{Vect}(w, t(w), t^2(w), \dots, t^n(w))$.

Théorème 1.2.43. *Soit V un $\mathbb{K}$ -espace vectoriel de dimension finie et t un endomorphisme de V . Il existe une liste unique $P_1, \dots, P_m \in \mathbb{K}[X]$ de polynômes unitaires non constants tels que P_{k+1} divise P_k et aussi, il existe une base de V dans laquelle la matrice représentant t est une somme directe des matrices compagnons des P_k .*

On appelle les P_k les *facteurs invariants* de t .

Démonstration. On applique le théorème des facteurs invariants 1.2.30 à $\Psi(V, t)$ avec $\mathbb{A} = \mathbb{K}[X]$, ce que l'on peut faire car c'est un $\mathbb{K}[X]$ -module de torsion de type fini d'après la proposition 1.2.41. $\square$

Corollaire 1.2.44. *Soit $A \in \mathcal{M}_n(\mathbb{K})$, il existe une liste unique $P_1, \dots, P_m \in \mathbb{K}[X]$ de polynômes unitaires non constants tel que P_{k+1} divise P_k , et tel que A soit semblable à la somme directe des matrices compagnons de P_k .*

Démonstration. On applique le théorème 1.2.43 à l'endomorphisme de $\mathbb{K}^n$ que représente A dans la base canonique. $\square$

On obtient finalement le corollaire suivant qui clôt notre chapitre ainsi que la question du problème de conjugaison dans $\mathcal{M}_n(\mathbb{Z})$.

Corollaire 1.2.45. *Soit $\mathbb{K}$ un corps commutatif, alors $A, B \in \mathcal{M}_n(\mathbb{K})$ sont semblables si et seulement s'ils ont les mêmes facteurs invariants.*

Chapitre 2

Théorie algébrique des nombres

Ce chapitre est le cœur du mémoire. Il a pour but d'introduire la matière qu'est la théorie algébrique des nombres afin que le lecteur puisse s'emparer des outils nécessaires pour affronter le théorème de Fermat–Kummer au chapitre suivant.

2.1 Corps de nombres et anneaux d'entiers

2.1.1 Entiers algébriques

Définition 2.1.1 (Entier). Soit $\mathbb{B}$ un anneau et $\mathbb{A}$ un sous-anneau de $\mathbb{B}$. On dit que $x \in \mathbb{B}$ est *entier* sur $\mathbb{A}$ s'il existe $P \in \mathbb{A}[X]$ unitaire tel que $P(x) = 0$. Une telle équation polynomiale est appelé *équation de dépendance intégrale* de x sur $\mathbb{A}$.

Exemple 2.1.2. On a que $\sqrt{2} \in \mathbb{R}$ est entier sur $\mathbb{Z}$ et $X^2 - 2 = 0$ est une équation de dépendance intégrale de $\sqrt{2}$ sur $\mathbb{Z}$. De la même façon, $\frac{i}{2} \in \mathbb{C}$ est entier sur $\mathbb{Q}$ et une équation de dépendance intégrale sur $\mathbb{Q}$ pour cette élément est donnée par $X^2 + \frac{1}{4}$. Par contre $\frac{1}{2} \in \mathbb{Q}$ n'est pas entier sur $\mathbb{Z}$.

On fait le rappel suivant d'algèbre linéaire :

Proposition 2.1.3. Soit $\mathbb{A}$ un anneau intègre, $A \in \mathcal{M}_n(\mathbb{A})$ et $a \in \mathbb{A}^n$ un vecteur non nul. Si $Aa = 0$ alors $\det(A) = 0$.

Proposition 2.1.4. Soit $\mathbb{B}$ un anneau intègre et $\mathbb{A}$ un sous-anneau de $\mathbb{B}$. On a que $x_1, \dots, x_n \in \mathbb{B}$ sont entiers sur $\mathbb{A}$ si et seulement si $\mathbb{A}[x_1, \dots, x_n]$ est un $\mathbb{A}$ -module de type fini.

Démonstration. Montrons d'abord que si $x_1, \dots, x_n \in \mathbb{B}$ sont entiers sur $\mathbb{A}$, alors $\mathbb{A}[x_1, \dots, x_n]$ est un $\mathbb{A}$ -module de type fini, en procédant par induction sur n .

- Initialisation : Soit $x \in \mathbb{B}$ entier sur $\mathbb{A}$, on veut montrer que $\mathbb{A}[x]$ est un $\mathbb{A}$ -module de type fini. Soit $T \in \mathbb{A}[x]$, on va le regarder comme un polynôme formel $T \in \mathbb{A}[X]$. Par définition, il existe $P \in \mathbb{A}[X]$ unitaire tel que $P(x) = 0$ et puisque ce polynôme est unitaire, on peut effectuer la division euclidienne de T par P dans $\mathbb{A}[X]$ (en prenant le degré comme stathme euclidien). Il existe donc $Q, R \in \mathbb{A}[X]$ tel que $T = PQ + R$ avec $\deg(R) < \deg(P)$ et en évaluant cette égalité en x , on obtient $T(x) = R(x)$. Ainsi, on trouve que $T \in \mathbb{A}[x]$ est engendré par au plus $\deg(P)$ éléments, on en déduit que $\mathbb{A}[x]$ est un module de type fini.
- Hérité : si x_n est entier sur $\mathbb{A}$ alors il est entier sur $\mathbb{A}[x_1, \dots, x_{n-1}]$ car $\mathbb{A} \subset \mathbb{A}[x_1, \dots, x_{n-1}]$. L'hypothèse d'hérité nous dit alors que $\mathbb{A}[x_1, \dots, x_{n-1}]$ est un $\mathbb{A}$ -module de type fini et que $\mathbb{A}[x_1, \dots, x_{n-1}][x_n]$ est un $\mathbb{A}[x_1, \dots, x_{n-1}]$ -module de type fini. Par la proposition 1.2.6, on a que $\mathbb{A}[x_1, \dots, x_{n-1}][x_n]$ est un $\mathbb{A}$ -module de type fini. On conclut alors par l'isomorphisme de $\mathbb{A}$ -modules suivant $\mathbb{A}[x_1, \dots, x_{n-1}, x_n] \cong \mathbb{A}[x_1, \dots, x_{n-1}][x_n]$.

Réciproquement, soit $x \in \{x_1, \dots, x_n\}$ et $\alpha = (\alpha_1, \dots, \alpha_m)$ une famille génératrice de $\mathbb{A}[x_1, \dots, x_n]$, alors pour tout $i \in \llbracket 1, m \rrbracket$, il existe $(a_{ij})_{j \in \llbracket 1, m \rrbracket} \in \mathbb{A}$ tel que

$$x\alpha_i = \sum_{j=1}^m a_{ij}\alpha_j.$$

En posant $A = (a_{ij})_{i,j \in \llbracket 1, m \rrbracket} \in \mathcal{M}_m(\mathbb{A})$ et $I \in \mathcal{M}_m(\mathbb{A})$ la matrice identité, l'expression ci-dessus se réécrit comme $(xI - A)\alpha = 0$ et donc par la proposition 2.1.3, on a $\det(xI - A)\alpha = 0$, en particulier $\det(xI - A)\alpha_1 = 0$. Puisque $\mathbb{B}$ est intègre, on obtient $\det(xI - A) = 0$ qui est une équation de dépendance intégrale de x sur $\mathbb{A}$. $\square$

Corollaire 2.1.5. *Soit $\mathbb{B}$ un anneau intègre et $\mathbb{A}$ un sous-anneau de $\mathbb{B}$. L'ensemble des éléments de $\mathbb{B}$ entiers sur $\mathbb{A}$ forment un sous-anneau de $\mathbb{B}$ contenant $\mathbb{A}$.*

Définition 2.1.6 (Fermeture intégrale). Soit $\mathbb{B}$ un anneau intègre et $\mathbb{A}$ un sous-anneau de $\mathbb{B}$. L'anneau des éléments de $\mathbb{B}$ entiers sur $\mathbb{A}$ s'appelle la *fermeture intégrale* de $\mathbb{A}$ dans $\mathbb{B}$.

Définition 2.1.7 (Entiers algébriques). L'anneau des *entiers algébriques* est la fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{C}$.

On rappelle le résultat de théorie de Galois suivant. Une preuve est donnée dans le cours LMAT1361 [3].

Lemme 2.1.8 (Gauss). *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $m \geq 1$. On a que P est irréductible sur $\mathbb{Z}$ si et seulement s'il est irréductible sur $\mathbb{Q}$.*

Proposition 2.1.9. *Soit $\alpha \in \mathbb{C}$, on a que α est un entier algébrique si et seulement si c'est un nombre algébrique dont le polynôme minimal sur $\mathbb{Q}$ est à coefficients entiers.*

Démonstration. Supposons que α est un entier algébrique, il existe donc par définition un polynôme unitaire $Q \in \mathbb{Z}[X]$ dont α est racine. Puisque $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, α est donc aussi racine d'un polynôme à coefficients rationnels, ce qui veut dire que α est un nombre algébrique. Ensuite, si Q est irréductible sur $\mathbb{Z}$, alors d'après le lemme de Gauss 2.1.8, il est aussi irréductible sur $\mathbb{Q}$ et puisque Q est aussi unitaire, il en suit que c'est le polynôme minimal de α , et il est bien à coefficients entiers comme souhaité. Si Q n'est pas irréductible sur $\mathbb{Z}$, alors cela implique qu'il peut s'écrire comme produit de polynômes irréductibles sur $\mathbb{Z}$ ayant des degrés strictement inférieurs au degré de Q . Appelons ces polynômes $Q_1, Q_2, \dots, Q_m$, puisque α est racine de Q , alors il est aussi racine de l'un de ces polynômes. Supposons sans perte de généralité que α est racine de Q_1 , alors il suffit maintenant pour conclure de montrer que Q_1 est unitaire pour retomber dans le cas précédent. Or, puisque Q est unitaire et qu'il est le produit des Q_i : $Q = \prod_{i=1}^m Q_i$, il en suit que si on note a le coefficient dominant de Q et a_i le coefficient dominant de Q_i pour $i \in \llbracket 1, m \rrbracket$ alors on a que : $1 = a = \prod_{i=1}^m a_i$. On a donc que pour tout $i \in \llbracket 1, m \rrbracket$, a_i est inversible, mais aussi entier, on en déduit donc que $a_i = \pm 1$. Ainsi si $a_1 = 1$, Q_1 est unitaire et cela conclut, et sinon, le polynôme $-Q_1$ est un polynôme unitaire qui est aussi irréductible sur $\mathbb{Z}$ dont α est racine, donc cela conclut aussi.

Réciproquement, si α est un nombre algébrique dont le polynôme minimal sur $\mathbb{Q}$ est à coefficient entiers, alors en particulier, ce polynôme minimal est un polynôme unitaire (à coefficients dans $\mathbb{Z}$) dont α est racine, donc α est un entier algébrique. $\square$

Définition 2.1.10 (Clôture intégrale). Soit $\mathbb{A}$ un anneau intègre et $\mathbb{K}$ son corps de fractions. On appelle *clôture intégrale* de $\mathbb{A}$ la fermeture intégrale de $\mathbb{A}$ dans $\mathbb{K}$.

Définition 2.1.11 (Intégralement Clos). Un anneau intègre $\mathbb{A}$ est dit *intégralement clos* si sa clôture intégrale est $\mathbb{A}$ lui-même.

Définition 2.1.12 (Corps de Nombres). Un *corps de nombres* est une extension finie de $\mathbb{Q}$.

Remarquons que $\mathbb{R}$ et $\mathbb{C}$ ne sont pas des corps de nombres car tout corps de nombres est dénombrable. Les deux définitions suivantes nous procurent les exemples de corps de nombres que l'on va traiter dans ce mémoire.

Définition 2.1.13 (Corps quadratique). Un *corps quadratique* est un corps de nombres de degré 2. En particulier, il est de la forme $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z} \setminus \{0, 1\}$ est sans facteurs carrés.

Définition 2.1.14 (Corps cyclotomique). Un *corps p -cyclotomique* est un corps de la forme $\mathbb{Q}(\zeta)$ où $\zeta = e^{i\frac{2\pi}{p}}$ pour p est un nombre premier impair.

Définition 2.1.15 (Anneau des entiers). L'*anneau des entiers* d'un corps de nombres $\mathbb{K}$, noté $\mathcal{O}_{\mathbb{K}}$, est la fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{K}$. On appelle ses éléments les *entiers* de $\mathbb{K}$.

En vue de la proposition 2.1.21, un corps de nombres peut être vu comme un sous-corps de $\mathbb{C}$. Dans ce cadre, on obtient la proposition suivante.

Proposition 2.1.16. Soit $\mathbb{A}$ l'anneau des entiers algébriques et $\mathbb{K}$ un corps de nombres, on a que $\mathcal{O}_{\mathbb{K}} = \mathbb{A} \cap \mathbb{K}$.

Démonstration. Si $x \in \mathcal{O}_{\mathbb{K}}$, alors x est un élément de $\mathbb{K}$ entier sur $\mathbb{Z}$, en particulier c'est un élément de $\mathbb{C}$ entier sur $\mathbb{Z}$. On a donc $\mathcal{O}_{\mathbb{K}} \subset \mathbb{A} \cap \mathbb{K}$. Si maintenant $x \in \mathbb{A} \cap \mathbb{K}$, alors x est un élément de $\mathbb{K}$ entier sur $\mathbb{Z}$ donc $x \in \mathcal{O}_{\mathbb{K}}$, ce qui conclut. $\square$

Proposition 2.1.17. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteurs carrés et $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Le polynôme minimal de $a + b\sqrt{d}$ sur $\mathbb{Q}$ est $X^2 - 2aX + a^2 - db^2$ si $b \neq 0$.

Démonstration. On a bien que ce polynôme est unitaire et annule $a + b\sqrt{d}$:

$$(a + b\sqrt{d})^2 - 2a(a + b\sqrt{d}) + a^2 - db^2 = a^2 + 2ab\sqrt{d} + db^2 - 2a^2 - 2ab\sqrt{d} + a^2 - db^2 = 0.$$

Il est bien irréductible, car si ce n'était pas le cas, le polynôme minimal de $a + b\sqrt{d}$ serait de degré 1 et on aurait $a + b\sqrt{d} \in \mathbb{Q}$. Or, ce n'est pas possible car $b \neq 0$ et $\sqrt{d} \notin \mathbb{Q}$. $\square$

Lemme 2.1.18. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteurs carrés congru à 1 modulo 4. Tout élément de $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est de la forme $\frac{u}{2} + \frac{v}{2}\sqrt{d}$ avec $u, v \in \mathbb{Z}$ de même parité.

Démonstration. Soit $x \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, on a qu'il existe $a, b \in \mathbb{Z}$ tel que $x = a + b\frac{1+\sqrt{d}}{2}$, on trouve donc

$$x = a + b\frac{1 + \sqrt{d}}{2} = \frac{2a + b}{2} + \frac{b}{2}\sqrt{d}.$$

Puisque $2a + b \equiv b \pmod{2}$, on peut conclure en posant $u = 2a + b$ et $v = b$. $\square$

Proposition 2.1.19. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteurs carrés et $\mathbb{Q}(\sqrt{d})$ un corps quadratique. L'anneau d'entiers de ce corps est de la forme $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 2, 3 \pmod{4}$ et $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \pmod{4}$.

Démonstration. On a premièrement que $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ puisque $\sqrt{d}$ a pour polynôme minimal $X^2 - d \in \mathbb{Z}[X]$. Si $d \equiv 1 \pmod{4}$, alors le polynôme minimal de $\frac{1+\sqrt{d}}{2}$, $X^2 - X + \frac{1-d}{4}$, est à coefficients entiers et donc $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Pour l'autre inclusion, prenons $a + b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ un entier algébrique, montrons que $a, b \in \mathbb{Z}$ si $d \equiv 2, 3 \pmod{4}$ et que $a, b \in \frac{1}{2}\mathbb{Z}$ si $d \equiv 1 \pmod{4}$. Le cas $b = 0$ est traité par les propositions 2.1.16 et 2.1.9, on considère donc maintenant que $b \neq 0$. Le polynôme minimal de $a + b\sqrt{d}$ est $X^2 - 2aX + a^2 - db^2$ d'après la proposition 2.1.17, et donc $2a, a^2 - db^2 \in \mathbb{Z}$. Il en suit que

$$4(a^2 - db^2) = 4a^2 - 4db^2 = (2a)^2 - d(2b)^2 \in 4\mathbb{Z} \subset \mathbb{Z} \quad (2.1)$$

et donc $(2b)^2 \in \mathbb{Z}$ car d est sans facteurs carrés. Ainsi, $2a, 2b \in \mathbb{Z}$, on peut alors écrire $a = \frac{r}{2}, b = \frac{t}{2}$ avec $r, t \in \mathbb{Z}$. Remarquons d'abord que tout carré est congru à 0 ou 1 modulo 4 et que $r, t \equiv 0 \pmod{2}$ si et seulement si $r^2, t^2 \equiv 0 \pmod{4}$. Si $d \equiv 1 \pmod{4}$, alors (2.1) nous donne

$$(2a)^2 - d(2b)^2 \in 4\mathbb{Z} \Leftrightarrow r^2 - dt^2 \in 4\mathbb{Z} \Leftrightarrow r^2 - dt^2 \equiv 0 \pmod{4} \Leftrightarrow r^2 \equiv t^2 \pmod{4} \Leftrightarrow r \equiv t \pmod{2}. \quad (2.2)$$

Ceci achève la preuve pour le cas $d \equiv 1 \pmod{4}$ par le lemme 2.1.18, on peut donc maintenant supposer que $d \equiv 2, 3 \pmod{4}$, et montrer que $r, t \in 2\mathbb{Z}$. Supposons par l'absurde que $r^2 \equiv 1 \pmod{4}$, alors (2.1) nous donne

$$(2a)^2 - d(2b)^2 \in 4\mathbb{Z} \Leftrightarrow r^2 - dt^2 \in 4\mathbb{Z} \Leftrightarrow r^2 - dt^2 \equiv 0 \pmod{4}. \quad (2.3)$$

Si t est pair, on a $1 \equiv r^2 \equiv 0 \pmod{4}$ qui nous donne la contradiction, et si t est impair, on obtient $1 \equiv r^2 \equiv dt^2 \equiv d \equiv 2, 3 \pmod{4}$ qui est aussi une contradiction. Il reste à montrer que $t^2 \equiv 0 \pmod{4}$, supposons par l'absurde que ce n'est pas le cas et donc que $t^2 \equiv 1 \pmod{4}$, puisque t est pair, (2.3) nous donne $2, 3 \equiv d \equiv 0 \pmod{4}$. $\square$

2.1.2 Norme et Trace

On rappelle le résultat de théorie de Galois suivant. Une preuve est donnée dans le cours LMAT1361 [3].

Théorème 2.1.20 (Théorème de l'élément primitif). *Toute extension finie séparable est monogène.*

En particulier, tout corps de nombres $\mathbb{K}$ est de la forme $\mathbb{Q}(\theta)$ avec $\theta \in \mathbb{K}$.

Proposition 2.1.21. *Un corps de nombres $\mathbb{K}$ de degré n admet exactement n morphismes de corps $\mathbb{K} \rightarrow \mathbb{C}$ distincts.*

Démonstration. Par le théorème de l'élément primitif 2.1.20, il existe $\theta \in \mathbb{K}$ tel que $\mathbb{K} = \mathbb{Q}(\theta)$. Ainsi, $(1, \theta, \dots, \theta^{n-1})$ est une $\mathbb{Q}$ -base de $\mathbb{K}$ et donc tout morphisme de corps provenant de $\mathbb{K}$ est déterminé par l'image de θ . Soit P le polynôme minimal de θ sur $\mathbb{Q}$, il est séparable et de degré n , il a donc n racines $\theta_1, \theta_2, \theta_3, \dots, \theta_n \in \mathbb{C}$ d'après le théorème fondamental de l'algèbre. On a alors au moins n morphismes $\mathbb{Q}(\theta) \rightarrow \mathbb{C}$ provenant des isomorphismes $\mathbb{Q}(\theta) \cong \mathbb{Q}(\theta_k)$. Enfin, si σ est un morphisme de corps, on a que $P(\sigma(\theta)) = \sigma(P(\theta)) = \sigma(0) = 0$, et donc σ envoie θ sur l'un des θ_k . Il y a donc au plus n morphismes $\mathbb{Q}(\theta) \rightarrow \mathbb{C}$, ce qui conclut. $\square$

L'ensemble des morphismes de corps $\mathbb{K} \rightarrow \mathbb{C}$ est noté $\text{Hom}(\mathbb{K}, \mathbb{C})$.

Proposition 2.1.22. *Soit $\mathbb{K}$ un corps de nombres et $G := \text{Hom}(\mathbb{K}, \mathbb{C})$. Si $x \in \mathbb{K}$, alors*

$$\prod_{\sigma \in G} \sigma(x) = ((-1)^m a_0)^{[\mathbb{K}:\mathbb{Q}(x)]} \in \mathbb{Q}, \quad \sum_{\sigma \in G} \sigma(x) = -[\mathbb{K}:\mathbb{Q}(x)] \times a_{m-1} \in \mathbb{Q},$$

où $P(X) = X^m + a_{m-1}X^{m-1} + \dots + a_1X + a_0$ le polynôme minimal de x sur $\mathbb{Q}$.

Démonstration. Notons $x_1, \dots, x_m$ les racines de P . En appliquant la proposition 2.1.21 au corps de nombres $\mathbb{Q}(x)$, on trouve qu'il y a exactement m morphismes distincts $\mathbb{Q}(x) \rightarrow \mathbb{C}$. Notons $d = [\mathbb{K}:\mathbb{Q}(x)]$, on a par la formule des dimensions que $n = dm$. Par le théorème de l'élément primitif 2.1.20, on a qu'il existe $y \in \mathbb{K}$ tel que $\mathbb{K} = \mathbb{Q}(x)(y)$, en particulier $\mathbb{K} \cong \mathbb{Q}(x)[X]/Q$ où Q est le polynôme minimal de y sur $\mathbb{Q}(x)$. Soit $\tau \in \text{Hom}(\mathbb{Q}(x), \mathbb{C})$, notons $H = \{\sigma \in \text{Hom}(\mathbb{K}, \mathbb{C}) : \sigma|_{\mathbb{Q}(x)} = \tau\}$. Notons aussi T_τ , pour $T \in \mathbb{Q}(x)[X]$, le polynôme T où on applique τ à chacun de ses coefficients. Remarquons que $T_\tau \in \tau(\mathbb{Q}(x))[X]$, et que cette procédure est multiplicative : $(TS)_\tau = T_\tau S_\tau$ pour tout $T, S \in \mathbb{Q}(x)[X]$. Ainsi, si T est irréductible sur $\mathbb{Q}(x)$, alors T_τ est irréductible sur $\tau(\mathbb{Q}(x))[X]$. Ensuite, on a que l'application $E : H \rightarrow \mathbb{C} : \sigma \mapsto \sigma(y)$ est injective, et son image est l'ensemble des racines de Q_τ qui est irréductible. On trouve alors

$$|H| = \deg(Q_\tau) = \deg(Q) = [\mathbb{K}:\mathbb{Q}(x)] = d.$$

Il en suit que tout morphisme $\mathbb{Q}(x) \rightarrow \mathbb{C}$ se prolonge de d manières différentes en un morphisme $\mathbb{K} \rightarrow \mathbb{C}$ et donc la liste $\sigma_1(x), \dots, \sigma_n(x)$ fait apparaître chaque racine de P d fois. Finalement, puisque

$$\prod_{k=1}^m x_k = (-1)^m a_0 \text{ et } \sum_{k=1}^m x_k = -a_{m-1},$$

on trouve

$$\begin{aligned} \prod_{\sigma \in G} \sigma(x) &= \prod_{k=1}^m x_k^d = \left(\prod_{k=1}^m x_k \right)^d = ((-1)^m a_0)^d, \\ \sum_{\sigma \in G} \sigma(x) &= \sum_{k=1}^m dx_k = d \sum_{k=1}^m x_k = -da_{m-1}. \end{aligned}$$

Cela conclut. □

Définition 2.1.23 (Norme). Soit $\mathbb{K}$ un corps de nombres et $G := \text{Hom}(\mathbb{K}, \mathbb{C})$. Pour $x \in \mathbb{K}$, on définit sa *norme* comme

$$\begin{aligned} N_{\mathbb{K}} : \mathbb{K} &\rightarrow \mathbb{Q} \\ x &\mapsto \prod_{\sigma \in G} \sigma(x) \end{aligned}$$

En particulier, si $x \in \mathbb{Q}$, alors $N_{\mathbb{K}}(x) = x^n$ où $n = [\mathbb{K} : \mathbb{Q}]$.

Proposition 2.1.24. *La norme est multiplicative.*

Démonstration. Cela suit directement de la définition. □

Définition 2.1.25 (Trace). Soit $\mathbb{K}$ un corps de nombres et $G = \text{Hom}(\mathbb{K}, \mathbb{C})$. Pour $x \in \mathbb{K}$, on définit sa *trace* comme

$$\begin{aligned} \text{Tr}_{\mathbb{K}}(x) : \mathbb{K} &\rightarrow \mathbb{Q} \\ x &\mapsto \sum_{\sigma \in G} \sigma(x) \end{aligned}$$

En particulier, si $x \in \mathbb{Q}$, alors $\text{Tr}_{\mathbb{K}}(x) = nx$ où $n = [\mathbb{K} : \mathbb{Q}]$.

Proposition 2.1.26. *Soit $\mathbb{K}$ un corps de nombres, la trace est $\mathbb{Q}$ -linéaire.*

Démonstration. Le fait que la trace est additive suit de la définition. Ensuite pour $q \in \mathbb{Q}$ et $x \in \mathbb{K}$ on a que

$$\text{Tr}_{\mathbb{K}}(qx) = \sum_{\sigma \in G} \sigma(qx) = \sum_{\sigma \in G} \sigma(q)\sigma(x) = \sum_{\sigma \in G} q\sigma(x) = q \sum_{\sigma \in G} \sigma(x) = q\text{Tr}_{\mathbb{K}}(x),$$

où $G = \text{Hom}(\mathbb{K}, \mathbb{C})$. □

Les propositions 2.1.24, 2.1.26 et 2.1.22 permettent de calculer en pratique la norme et la trace d'un élément.

Exemple 2.1.27. Le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$ est donné par $X^3 - 2$, il en suit que $N_{\mathbb{Q}(\sqrt[3]{2})}(\sqrt[3]{2}) = -2$ et $\text{Tr}_{\mathbb{Q}(\sqrt[3]{2})}(\sqrt[3]{2}) = 0$.

Proposition 2.1.28. *Soit $\mathbb{K}$ un corps de nombres. Si $x \in \mathcal{O}_{\mathbb{K}}$, on a $N_{\mathbb{K}}(x), \text{Tr}_{\mathbb{K}}(x) \in \mathbb{Z}$.*

Démonstration. Soit $P(X) = X^m + a_{m-1}X^{m-1} + \dots + a_1X + a_0$ le polynôme minimal de x sur $\mathbb{Q}$, puisque x est un entier algébrique d'après 2.1.16, la proposition 2.1.9 nous dit que $P \in \mathbb{Z}[X]$. On conclut par la proposition 2.1.22 qui nous dit que $N_{\mathbb{K}}(x) = ((-1)^m a_0)^{[\mathbb{K}:\mathbb{Q}(x)]} \in \mathbb{Z}$ et $\text{Tr}_{\mathbb{K}}(x) = -[\mathbb{K}:\mathbb{Q}(x)]a_{m-1} \in \mathbb{Z}$. $\square$

La multiplicativité de la norme nous dit que pour $a, b \in \mathcal{O}_{\mathbb{K}}^*$, si a divise b dans $\mathcal{O}_{\mathbb{K}}$ alors $N_{\mathbb{K}}(a)$ divise $N_{\mathbb{K}}(b)$ dans $\mathbb{Z}$.

Proposition 2.1.29. *Soit $x \in \mathcal{O}_{\mathbb{K}}$, on a que $x \in \mathcal{O}_{\mathbb{K}}^\times$ si et seulement si $N_{\mathbb{K}}(x) = \pm 1$.*

Démonstration. Premièrement, si $x \in \mathcal{O}_{\mathbb{K}}^\times$, alors il existe $y \in \mathcal{O}_{\mathbb{K}}^\times$ tel que $xy = 1$ et puisque la norme est multiplicative, on a $N_{\mathbb{K}}(x)$ qui divise 1 dans $\mathbb{Z}$ et donc $N_{\mathbb{K}}(x) = \pm 1$.

Réciproquement, on sait que $\mathbb{K}$ est isomorphe à un sous-corps $\mathbb{L}$ de $\mathbb{C}$, notons $\lambda : \mathbb{K} \rightarrow \mathbb{L}$ cet isomorphisme. Remarquons que $N_{\mathbb{K}}(x) = N_{\mathbb{L}}(\lambda(x))$ pour tout $x \in \mathbb{K}$:

$$N_{\mathbb{L}}(\lambda(x)) = \prod_{\tau \in \text{Hom}(\mathbb{L}, \mathbb{C})} \tau(\lambda(x)) = \prod_{\sigma \in \text{Hom}(\mathbb{K}, \mathbb{C})} \sigma(x) = N_{\mathbb{K}}(x).$$

Ainsi, il suffit de montrer que $N_{\mathbb{L}}(y) = \pm 1$ implique $y \in \mathcal{O}_{\mathbb{L}}^\times$ pour tout $y \in \mathcal{O}_{\mathbb{L}}$. Notons $\iota : \mathbb{L} \hookrightarrow \mathbb{C}$ le morphisme d'inclusion et posons $G = \text{Hom}(\mathbb{L}, \mathbb{C})$ et $G^* = G \setminus \{\iota\}$. On trouve

$$N_{\mathbb{L}}(y) = \pm 1 \iff \prod_{\sigma \in G} \sigma(y) = \pm 1 \iff y \times \left(\pm \prod_{\sigma \in G^*} \sigma(y) \right) = 1.$$

Il reste donc à prouver que $z = \prod_{\sigma \in G^*} \sigma(y) \in \mathcal{O}_{\mathbb{L}}$. On a que z est un entier algébrique comme produit d'entiers algébriques, mais $z = \frac{\pm 1}{y} \in \mathbb{L}$ et donc on conclut par la proposition 2.1.16. $\square$

Proposition 2.1.30. *Soit $x \in \mathcal{O}_{\mathbb{K}}$, si $|N_{\mathbb{K}}(x)|$ est un nombre premier, alors x est irréductible.*

Démonstration. Soit $y \in \mathcal{O}_{\mathbb{K}}^*$ tel que y divise x , alors $N_{\mathbb{K}}(y)$ divise $N_{\mathbb{K}}(x)$ dans $\mathbb{Z}$ et puisque $\pm N_{\mathbb{K}}(x)$ est premier, on a soit que $N_{\mathbb{K}}(y) = \pm 1$ et est donc inversible par la proposition 2.1.29, soit que $N_{\mathbb{K}}(y) = \pm N_{\mathbb{K}}(x)$ et donc $N_{\mathbb{K}}(\frac{x}{y}) = \pm 1$, c'est-à-dire que $\frac{x}{y}$ est inversible par la proposition 2.1.29 et donc x et y sont associés. $\square$

Définition 2.1.31 (Polynôme cyclotomique). Soit p un nombre premier impair. Le $p^{\text{ième}}$ polynôme cyclotomique est défini comme

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1.$$

On rappelle le résultat de théorie de Galois suivant. Une preuve est donnée dans le cours LMAT1361 [3].

Proposition 2.1.32. *Soit p un nombre premier impair. Le $p^{\text{ième}}$ polynôme cyclotomique est irréductible et ses racines sont les racines $p^{\text{ième}}$ de l'unité différentes de 1.*

Proposition 2.1.33. *Soit p un nombre premier impair et $\zeta = e^{i\frac{2\pi}{p}}$. On a que $N_{\mathbb{Z}[\zeta]}(1 - \zeta) = p$, en particulier $1 - \zeta$ est irréductible.*

Démonstration. On évalue le $p^{\text{ième}}$ polynôme cyclotomique en 1

$$\begin{aligned}\Phi_p(X) &= \sum_{k=0}^{p-1} X^k = \prod_{k=1}^{p-1} (X - \zeta^k) \\ \Rightarrow \Phi_p(1) &= p = \prod_{k=1}^{p-1} (1 - \zeta^k) = \prod_{\sigma \in G} (\sigma(1) - \sigma(\zeta)) = \prod_{\sigma \in G} \sigma(1 - \zeta) = N_{\mathbb{Q}(\zeta)}(1 - \zeta),\end{aligned}$$

où $G = \text{Hom}(\mathbb{Q}(\zeta), \mathbb{C})$.

Le fait que $1 - \zeta$ soit irréductible découle de la proposition 2.1.30. □

Proposition 2.1.34. *Soit p un nombre premier impair et notons $\zeta = e^{i\frac{2\pi}{p}}$, on a $\text{Tr}_{\mathbb{Q}(\zeta)}(\zeta) = -1$.*

Démonstration. Le polynôme minimal de ζ est le $p^{\text{ième}}$ polynôme cyclotomique d'après 2.1.32, on conclut alors par la proposition 2.1.22. □

Proposition 2.1.35. *Soit $\mathbb{A}$ un sur-anneau de $\mathbb{Z}$ et $a, b \in \mathbb{Z}$ coprimiers. Tout idéal propre de $\mathbb{A}$ qui contient a ne contient pas b .*

Démonstration. D'après le théorème de Bézout 1.2.27, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$. Ainsi, un idéal qui contient à la fois a et b contient aussi $au + bv = 1$, il ne peut donc pas être propre. □

Définition 2.1.36. Soit $\mathbb{K}$ un corps de nombres. On dit qu'un idéal premier P de $\mathcal{O}_{\mathbb{K}}$ est *au-dessus* d'un nombre premier p si $p\mathcal{O}_{\mathbb{K}} \subset P$.

Proposition 2.1.37. *Soit $\mathbb{K}$ un corps de nombres. Un idéal premier P de $\mathcal{O}_{\mathbb{K}}$ est au dessus de p si et seulement si $P \cap \mathbb{Z} = p\mathbb{Z}$.*

Démonstration. Montrons premièrement que $P \cap \mathbb{Z} = p\mathbb{Z}$ si P est au dessus de p . On a trivialement que $p\mathbb{Z} \subset P \cap \mathbb{Z}$ car $p\mathbb{Z} \subset p\mathcal{O}_{\mathbb{K}} \subset P$ par hypothèse et $p\mathbb{Z} \subset \mathbb{Z}$. Montrons maintenant que $P \cap \mathbb{Z} \subset p\mathbb{Z}$. Soit $x \in P \cap \mathbb{Z}$, on a que $x \neq \pm 1$ car P est premier non nul. Aussi, le cas $x = 0$ est trivial, on peut donc considérer que $|x| \geq 2$ afin d'utiliser le théorème fondamental de l'arithmétique pour obtenir $x = \pm \prod_{k=1}^m q_k^{e_k}$ où les q_k sont des premiers rationnels. Puisque P est premier, il existe $k \in \llbracket 1, m \rrbracket$ tel que $q_k \in P$. On a alors que $q_k = p$ d'après la proposition 2.1.35.

Réciproquement, on a que $p\mathbb{Z} = P \cap \mathbb{Z} \subset P$ nous donne que $p \in P$ et donc pour tout $x \in p\mathcal{O}_{\mathbb{K}}$, on a que $x = pr$ avec $r \in \mathcal{O}_{\mathbb{K}}$ et $pr \in P$ par propriété des idéaux. $\square$

Proposition 2.1.38. *Soit p un nombre premier impair et $\zeta = e^{i\frac{2\pi}{p}}$. Pour tout $k, k' \in \llbracket 1, p-1 \rrbracket$, on a que $1 - \zeta^k$ et $1 - \zeta^{k'}$ sont associés dans $\mathbb{Z}[\zeta]$. En particulier $1 + \zeta \in \mathbb{Z}[\zeta]^\times$.*

Démonstration. La relation d'association est une relation d'équivalence, il suffit donc de montrer que pour tout $k \in \llbracket 2, p-1 \rrbracket$, $1 - \zeta^k$ est associé à $1 - \zeta$. Notons que $\{1, \zeta, \dots, \zeta^{p-2}\}$ est une $\mathbb{Z}$ -base de $\mathbb{Z}[\zeta]$, on trouve alors par formule des séries géométriques

$$\frac{1 - \zeta^k}{1 - \zeta} = 1 + \zeta + \dots + \zeta^{k-1} \in \mathbb{Z}[\zeta].$$

Ainsi, $1 - \zeta$ divise $1 - \zeta^k$ dans $\mathbb{Z}[\zeta]$. Ensuite, puisque $k \in \llbracket 2, p-1 \rrbracket$, il existe $t \in \llbracket 2, p-1 \rrbracket$ tel que $kt \equiv 1 [p]$. On trouve finalement

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

On conclut que $1 - \zeta^k$ divise $1 - \zeta$ dans $\mathbb{Z}[\zeta]$, ils sont donc bien associés.

On a que $1 + \zeta = \frac{1 - \zeta^2}{1 - \zeta}$, il est donc inversible puisque c'est un quotient de deux éléments associés. $\square$

Lemme 2.1.39. *Soit p un nombre premier impair et $\zeta = e^{i\frac{2\pi}{p}}$. Pour tout $x \in \mathcal{O}_{\mathbb{Q}(\zeta)}$, on a que $\text{Tr}_{\mathbb{Q}(\zeta)}((1 - \zeta)x) \in p\mathbb{Z}$.*

Démonstration. Puisque $(1 - \zeta)\mathcal{O}_{\mathbb{Q}(\zeta)} \cap \mathbb{Z} = p\mathbb{Z}$ d'après la proposition 2.1.37 et que $\text{Tr}_{\mathbb{Q}(\zeta)}((1 - \zeta)x) \in \mathbb{Z}$ d'après la proposition 2.1.28, il suffit alors de montrer que $\text{Tr}_{\mathbb{Q}(\zeta)}((1 - \zeta)x) \in (1 - \zeta)\mathcal{O}_{\mathbb{Q}(\zeta)}$. Pour tout $\sigma \in \text{Hom}(\mathbb{Q}(\zeta), \mathbb{C})$, il existe $k \in \llbracket 1, p-1 \rrbracket$ tel que

$$\sigma((1 - \zeta)x) = \sigma(1 - \zeta)\sigma(x) = (\sigma(1) - \sigma(\zeta))\sigma(x) = (1 - \zeta^k)\sigma(x).$$

Puisque l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est normale, on a que $\sigma(x) \in \mathcal{O}_{\mathbb{Q}(\zeta)}$. Aussi, $1 - \zeta$ est associé à $1 - \zeta^k$ d'après la proposition 2.1.38. Il en suit que $\sigma((1 - \zeta)x) \in (1 - \zeta)\mathcal{O}_{\mathbb{Q}(\zeta)}$ pour tout $\sigma \in \text{Hom}(\mathbb{Q}(\zeta), \mathbb{C})$, et donc $\text{Tr}_{\mathbb{Q}(\zeta)}((1 - \zeta)x) \in (1 - \zeta)\mathcal{O}_{\mathbb{Q}(\zeta)}$ par somme, ce qui conclut. $\square$

Proposition 2.1.40. Soit p un nombre premier impair et $\zeta = e^{i\frac{2\pi}{p}}$. L'anneau des entiers de $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$.

Démonstration. Soit $x \in \mathbb{Q}(\zeta)$ satisfaisant une équation de dépendance intégrale sur $\mathbb{Z}$. Par définition il existe $a_0, a_1, \dots, a_{p-3}, a_{p-2} \in \mathbb{Q}$ tels que

$$x = a_{p-2}\zeta^{p-2} + a_{p-3}\zeta^{p-3} + \dots + a_1\zeta + a_0,$$

on doit alors montrer que ces a_k sont des entiers rationnels. Considérons

$$(1 - \zeta)x = a_{p-2}(\zeta^{p-2} - \zeta^{p-1}) + a_{p-3}(\zeta^{p-3} - \zeta^{p-2}) + \dots + a_1(\zeta - \zeta^2) + a_0(1 - \zeta),$$

par additivité de la trace 2.1.26 et d'après la proposition 2.1.34 on a que $\text{Tr}_{\mathbb{Q}(\zeta)}(1 - \zeta) = \text{Tr}_{\mathbb{Q}(\zeta)}(1) - \text{Tr}_{\mathbb{Q}(\zeta)}(\zeta) = p - 1 - (-1) = p$ et aussi $\text{Tr}_{\mathbb{Q}(\zeta)}(\zeta^k - \zeta^{k+1}) = \text{Tr}_{\mathbb{Q}(\zeta)}(\zeta^k) - \text{Tr}_{\mathbb{Q}(\zeta)}(\zeta^{k+1}) = -1 - (-1) = 0$. On déduit par $\mathbb{Q}$ -linéarité de la trace 2.1.26 que $\text{Tr}_{\mathbb{Q}(\zeta)}((1 - \zeta)x) = a_0p$. Mais le lemme 2.1.39 nous dit alors que $\text{Tr}_{\mathbb{Q}(\zeta)}((1 - \zeta)x) = a_0p \in p\mathbb{Z}$ et donc $a_0 \in \mathbb{Z}$. Maintenant, on considère $(x - a_0)\zeta^{-1} = a_{p-2}\zeta^{p-3} + a_{p-3}\zeta^{p-4} + \dots + a_2\zeta + a_1$ qui est un élément de $\mathcal{O}_{\mathbb{Q}(\zeta)}$ car $x - a_0 \in \mathcal{O}_{\mathbb{Q}(\zeta)}$ et $\zeta^{-1} = \zeta^{p-1} \in \mathcal{O}_{\mathbb{Q}(\zeta)}$. On peut alors appliquer le même raisonnement sur $(x - a_0)\zeta^{-1}$ pour prouver que $a_1 \in \mathbb{Z}$. Ainsi de suite, on prouve que $a_k \in \mathbb{Z}$ pour tout $k \in \llbracket 0, p-2 \rrbracket$. $\square$

2.1.3 Discriminant d'un corps de nombres

Définition 2.1.41 (Discriminant). Soit $\mathbb{K}$ un corps de nombres de degré n et $x = (x_1, \dots, x_n) \in \mathbb{K}^n$ un vecteur de taille n . On définit son *discriminant* comme

$$\Delta(x) := \det((\sigma_i(x_j))_{i,j \in \llbracket 1, n \rrbracket})^2$$

où $\sigma_i \in \text{Hom}(\mathbb{K}, \mathbb{C})$.

Proposition 2.1.42. Soit $\mathbb{K}$ un corps de nombre de degré n , $B \in \mathcal{M}_n(\mathbb{Q})$ et $x, y \in \mathbb{K}^n$ deux vecteurs tels que $xB = y$. On a $\Delta(y) = \det(B)^2 \Delta(x)$.

Démonstration. Disons que $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ et $B = (b_{ij})_{i,j \in \llbracket 1, n \rrbracket}$ alors $y_j = \sum_{k=1}^n x_k b_{kj}$ pour tout $j \in \llbracket 1, n \rrbracket$. Pour tout $i \in \llbracket 1, n \rrbracket$, on a que σ_i est un morphisme de corps et donc

$$\sigma_i(y_j) = \sigma_i\left(\sum_{k=1}^n x_k b_{kj}\right) = \sum_{k=1}^n \sigma_i(x_k b_{kj}) = \sum_{k=1}^n \sigma_i(x_k) \sigma_i(b_{kj}) = \sum_{k=1}^n \sigma_i(x_k) b_{kj}$$

et on a alors l'égalité matricielle $(\sigma_i(y_j))_{i,j \in \llbracket 1, n \rrbracket} = (\sigma_i(x_j))_{i,j \in \llbracket 1, n \rrbracket} \times B$. On applique alors le déterminant qui est multiplicatif puis on met au carré pour obtenir l'égalité souhaitée. $\square$

Proposition 2.1.43. Soit $\mathbb{Q}(\theta)$ un corps de nombres de degré $n \geq 2$, P le polynôme minimal de θ sur $\mathbb{Q}$ et P' sa dérivée formelle. Notons σ_i les morphismes de corps $\mathbb{Q}(\theta) \rightarrow \mathbb{C}$, alors

$$\Delta(1, \theta, \dots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\sigma_i(\theta) - \sigma_j(\theta)) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{K}}(P'(\theta)).$$

Démonstration. On a par définition que

$$\Delta(1, \theta, \dots, \theta^{n-1}) = \det((\sigma_i(\theta^j))_{i,j \in \llbracket 1, n \rrbracket})^2 = \det((\sigma_i(\theta)^j)_{i,j \in \llbracket 1, n \rrbracket})^2$$

car les σ_i sont des morphismes de corps. On reconnaît alors une matrice de Vandermonde et on obtient

$$\det((\sigma_i(\theta)^j)_{i,j \in \llbracket 1, n \rrbracket})^2 = \left(\prod_{i < j} (\sigma_i(\theta) - \sigma_j(\theta)) \right)^2 = \prod_{i < j} (\sigma_i(\theta) - \sigma_j(\theta))^2 \quad (2.4)$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\sigma_i(\theta) - \sigma_j(\theta)). \quad (2.5)$$

Ensuite, on a $P(X) = \prod_i (X - \sigma_i(\theta))$ et donc $P'(X) = \sum_i \prod_{j \neq i} (X - \sigma_j(\theta))$, ainsi on a pour tout $i \in \llbracket 1, n \rrbracket$ que $\sigma_i(P'(\theta)) = P'(\sigma_i(\theta)) = \prod_{j \neq i} (\sigma_i(\theta) - \sigma_j(\theta))$. On obtient finalement

$$\begin{aligned} \det((\sigma_i(\theta)^j)_{i,j \in \llbracket 1, n \rrbracket})^2 &= (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\sigma_i(\theta) - \sigma_j(\theta)) = (-1)^{\frac{n(n-1)}{2}} \prod_i \prod_{j \neq i} (\sigma_i(\theta) - \sigma_j(\theta)) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i \sigma_i(P'(\theta)) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{K}}(P'(\theta)). \end{aligned}$$

□

Ce discriminant est non nul car les $\sigma_i(\theta)$ sont distincts et c'est un nombre rationnel par la seconde formule.

Exemple 2.1.44. Si on prend $\mathbb{Q}(\zeta)$ avec $\zeta = e^{i\frac{2\pi}{3}}$, on a que le polynôme minimal de ζ est $X^2 + X + 1$ et $2X + 1$ est le polynôme dérivé. On calcule alors $N_{\mathbb{Q}(\zeta)}(2\zeta + 1) = 3$. Finalement, on trouve $\Delta(1, \zeta) = (-1)^{\frac{2(2-1)}{2}} \cdot 3 = -3$.

Proposition 2.1.45. Soit $\mathbb{K}$ un corps de nombres et $x = (x_1, \dots, x_n) \in \mathbb{K}^n$. On a que x est une $\mathbb{Q}$ -base de $\mathbb{K}$ si et seulement si $\Delta(x) \neq 0$.

Démonstration. Soit θ un élément primitif de $\mathbb{K}$ alors $(1, \theta, \dots, \theta^{n-1})$ est une $\mathbb{Q}$ -base de $\mathbb{K}$ et donc pour tout $j \in \llbracket 1, n \rrbracket$, il existe $(b_{ij})_{i \in \llbracket 1, n \rrbracket}$ tel que $x_j = \sum_{i=1}^n \theta^{i-1} b_{ij}$. On obtient alors une matrice $B = (b_{ij})_{i,j \in \llbracket 1, n \rrbracket}$ telle que $x = (1, \theta, \dots, \theta^{n-1})B$ et donc par la proposition

2.1.42, on a que $\Delta(x) = \det(B)^2 \Delta(1, \theta, \dots, \theta^{n-1})$. Puisque $\Delta(1, \theta, \dots, \theta^{n-1}) \neq 0$ par la proposition 2.1.43, on a que $\Delta(x) \neq 0$ si et seulement si $\det(B) \neq 0$, c'est-à-dire si et seulement si x est une base. $\square$

Cette démonstration montre aussi que le discriminant d'une base est un nombre rationnel.

Proposition 2.1.46. *Soit $\mathbb{K}$ un corps de nombres et $\alpha \in \mathbb{K}$, il existe $b \in \mathbb{Z}^*$ tel que $b\alpha \in \mathcal{O}_{\mathbb{K}}$.*

Démonstration. Soit $P(X) = X^n + \frac{a_{n-1}}{b_{n-1}}X^{n-1} + \dots + \frac{a_1}{b_1}X + \frac{a_0}{b_0}$ le polynôme minimal de α sur $\mathbb{Q}$, en prenant $b = \prod_{k=0}^{n-1} b_k$ (ou le PPCM à la place du produit), on a alors que $b^n P \in \mathbb{Z}[X]$. On pose ensuite $c_k = a_k b^{n-k}$ pour $k \in \llbracket 0, n-1 \rrbracket$ et alors le polynôme $X^n + c_{n-1}X^{n-1} + \dots + c_1X + c_0$ donne une équation de dépendance intégrale de $b\alpha$ sur $\mathbb{Z}$. $\square$

Corollaire 2.1.47. *Soit $\mathbb{K}$ un corps de nombres, on a que $\mathbb{K} = \mathbb{Q}(\theta)$ avec $\theta \in \mathcal{O}_{\mathbb{K}}$.*

Démonstration. Par le théorème de l'élément primitif 2.1.20, il existe $\alpha \in \mathbb{K}$ tel que $\mathbb{K} = \mathbb{Q}(\alpha)$ mais alors la proposition 2.1.46 nous dit qu'il existe $b \in \mathbb{Z}^*$ tel que $b\alpha \in \mathcal{O}_{\mathbb{K}}$, et on a bien $\mathbb{Q}(\alpha) = \mathbb{Q}(b\alpha)$. $\square$

Proposition 2.1.48. *Tout anneau factoriel est intégralement clos.*

Démonstration. Soit $\mathbb{A}$ un anneau factoriel et $\mathbb{K}$ son corps des fractions, et soit $\frac{a}{b} \in \mathbb{K}$ avec a et b premiers entre eux, satisfaisant l'équation de dépendance intégrale sur $\mathbb{A}$ suivante : $(\frac{b}{c})^n + a_{n-1}(\frac{b}{c})^{n-1} + \dots + a_1 \frac{b}{c} + a_0 = 0$. En multipliant cette égalité par c^n , on obtient $b^n + ca_{n-1}b^{n-1} + c^2a_{n-2}b^{n-2} + \dots + c^{n-1}a_1b + c^na_0 = 0$, ce que l'on peut réécrire comme $c(a_{n-1}b^{n-1} + ca_{n-2}b^{n-2} + \dots + c^{n-2}a_1b + c^{n-1}a_0) = -b^n$ et donc c divise $-b^n$. Mais c divise aussi c et donc c divise le PGCD de c et b qui est 1 car ils sont premiers entre eux. Finalement, c est inversible et on trouve que $\frac{b}{c} \in \mathbb{A}$. $\square$

Corollaire 2.1.49. *L'anneau des entiers de $\mathbb{Q}$ est $\mathbb{Z}$.*

Démonstration. On a que $\mathbb{Z}$ est factoriel donc intégralement clos par la proposition 2.1.48, et puisque $\mathbb{Q}$ est son corps de fractions, la fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}$ est sa clôture intégrale. $\square$

Définition 2.1.50 (Base intégrale). On appelle *base intégrale* d'un corps de nombres $\mathbb{K}$ une $\mathbb{Z}$ -base du groupe abélien $(\mathcal{O}_{\mathbb{K}}, +, 0)$ (vu comme $\mathbb{Z}$ -module).

Lemme 2.1.51. *Soit $\mathbb{K}$ un corps de nombres, alors $\mathcal{O}_{\mathbb{K}} \cap \mathbb{Q} = \mathbb{Z}$.*

Démonstration. On a déjà $\mathbb{Z} \subset \mathcal{O}_{\mathbb{K}} \cap \mathbb{Q}$, prenons alors $x \in \mathcal{O}_{\mathbb{K}} \cap \mathbb{Q}$, on a donc que x est un nombre rationnel satisfaisant une équation de dépendance intégrale sur $\mathbb{Z}$, et donc $x \in \mathcal{O}_{\mathbb{Q}} \cap \mathbb{Q} = \mathbb{Z} \cap \mathbb{Q} = \mathbb{Z}$. $\square$

Lemme 2.1.52. *Le discriminant d'une $\mathbb{Q}$ -base de $\mathbb{K}$ ne consistant que d'entiers de $\mathbb{K}$ est un entier rationnel non nul.*

Démonstration. Cela suit du fait que le discriminant d'une $\mathbb{Q}$ -base de $\mathbb{K}$ est un nombre rationnel non nul d'après la proposition 2.1.45. Ensuite, puisque le déterminant ne fait intervenir que des multiplications, des sommes et des différences d'éléments de la matrice, le discriminant appartient aussi à $\mathcal{O}_{\mathbb{K}}$. On conclut par le lemme 2.1.51. $\square$

Proposition 2.1.53. *Tout corps de nombres possède une base intégrale.*

Démonstration. Tout corps de nombre peut s'écrire comme $\mathbb{Q}(\theta)$ avec $\theta \in \mathcal{O}_{\mathbb{K}}$ d'après le corollaire 2.1.47. Ainsi il admet une $\mathbb{Q}$ -base n'ayant que des entiers de $\mathbb{K}$ car on peut considérer $(1, \theta, \dots, \theta^{n-1})$ par exemple. Considérons alors $\alpha = (\alpha_1, \dots, \alpha_n)$ une $\mathbb{Q}$ -base du corps ne consistant que d'entiers du corps, qui minimise la fonction $|\Delta(-)|$ (restreinte aux bases consistant d'entiers de $\mathbb{K}$), ce que l'on peut faire par le lemme précédent 2.1.52. Supposons par l'absurde que ce n'est pas une base intégrale, alors il existe $x \in \mathcal{O}_{\mathbb{K}}$ tel que $x = \sum_{k=1}^n c_k \alpha_k$ avec un $c_k \in \mathbb{Q} \setminus \mathbb{Z}$, et sans perte de généralité, on peut supposer que $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$. Il existe donc $c \in \mathbb{Z}$ et $r \in]0, 1[$ tels que $c_1 = c + r$, on définit alors $a_1 = x - c_1 \alpha_1$ et $a_k = c_k$ pour $k \in \llbracket 2, n \rrbracket$. On obtient alors une base $(a_1, \dots, a_n)$ consistant d'entiers de $\mathbb{K}$ et le déterminant de changement de base de $(\alpha_1, \dots, \alpha_n)$ à $(a_1, \dots, a_n)$ est le suivant

$$\begin{vmatrix} c_1 - c & c_2 & c_3 & \cdots & c_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = r.$$

Par la proposition 2.1.42, on a alors $\Delta(a_1, \dots, a_n) = r^2 \Delta(\alpha_1, \dots, \alpha_n)$, ce qui contredit la minimalité de $|\Delta(\alpha_1, \dots, \alpha_n)|$ car $0 < r^2 < 1$. $\square$

Corollaire 2.1.54. *L'anneau des entiers d'un corps de nombres $\mathbb{K}$ est un $\mathbb{Z}$ -module de rang égal à $[\mathbb{K} : \mathbb{Q}]$.*

Démonstration. Il suit de la proposition 2.1.46 qu'une base intégrale de $\mathbb{K}$ est aussi une $\mathbb{Q}$ -base et une telle base existe toujours par la proposition 2.1.53. $\square$

Proposition 2.1.55. *Toutes les bases intégrales d'un corps de nombres $\mathbb{K}$ ont le même discriminant.*

Démonstration. Soit $x, y \in \mathbb{K}^n$ deux bases intégrales de $\mathbb{K}$, alors il existe $B \in \text{GL}_n(\mathbb{Z})$ telle que $y = xB$ et puisque $\det(B)^2 = (\pm 1)^2 = 1$, on conclut par la proposition 2.1.42. $\square$

On appelle ce discriminant le *discriminant* de $\mathbb{K}$ et on le note $\Delta_{\mathbb{K}}$.

Proposition 2.1.56. *Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique où d est sans facteurs carrés. Le discriminant de $\mathbb{Q}(\sqrt{d})$ vaut $4d$ si $d \equiv 2, 3 \pmod{4}$ et d si $d \equiv 1 \pmod{4}$.*

Démonstration. Faisons une disjonction de cas.

- $d \equiv 2, 3 \pmod{4}$: on a que $(1, \sqrt{d})$ est une base intégrale de $\mathbb{Q}(\sqrt{d})$, donc d'après la proposition 2.1.43, on a que $\Delta_{\mathbb{Q}(\sqrt{d})} = (-1)^{\frac{2 \times 1}{2}} N_{\mathbb{Q}(\sqrt{d})}(P'(\sqrt{d})) = -N_{\mathbb{Q}(\sqrt{d})}(P'(\sqrt{d}))$ où P est le polynôme minimal de $\sqrt{d}$. Et puisque $P(X) = X^2 - d$, on a $P'(X) = 2X$ et donc $-N_{\mathbb{Q}(\sqrt{d})}(P'(\sqrt{d})) = -N_{\mathbb{Q}(\sqrt{d})}(2\sqrt{d}) = -N_{\mathbb{Q}(\sqrt{d})}(2)N_{\mathbb{Q}(\sqrt{d})}(\sqrt{d}) = 4d$.
- $d \equiv 1 \pmod{4}$: on a que $(1, \frac{1+\sqrt{d}}{2})$ est une base intégrale de $\mathbb{Q}(\sqrt{d})$, donc d'après la proposition 2.1.43, on a que $\Delta_{\mathbb{Q}(\sqrt{d})} = (-1)^{\frac{2 \times 1}{2}} N_{\mathbb{Q}(\sqrt{d})}(P'(\frac{1+\sqrt{d}}{2})) = -N_{\mathbb{Q}(\sqrt{d})}(P'(\frac{1+\sqrt{d}}{2}))$ où P est le polynôme minimal de $\frac{1+\sqrt{d}}{2}$. Et puisque $P(X) = X^2 - X + \frac{1-d}{4}$, on a $P'(X) = 2X - 1$ et donc $-N_{\mathbb{Q}(\sqrt{d})}(P'(\frac{1+\sqrt{d}}{2})) = -N_{\mathbb{Q}(\sqrt{d})}(2\frac{1+\sqrt{d}}{2} - 1) = -N_{\mathbb{Q}(\sqrt{d})}(\sqrt{d}) = d$.

$\square$

Proposition 2.1.57. *Prenons $\zeta = e^{i\frac{2\pi}{p}}$ où p est un nombre premier impair, le discriminant de $\mathbb{Q}(\zeta)$ est $(-1)^{\frac{p-1}{2}} p^{p-2}$.*

Démonstration. On a que $\mathbb{Q}(\zeta)$ est de degré $p-1$ et $(1, \zeta, \zeta^2, \dots, \zeta^{p-2})$ est une base intégrale, on va donc utiliser la proposition 2.1.43. Le polynôme minimal de ζ est $P(X) = \frac{X^p-1}{X-1}$ et la dérivée formelle de ce polynôme est $P'(X) = \frac{pX^{p-1}(X-1) - X^{p+1}}{(X-1)^2}$. En évaluant ce dernier en ζ , on obtient

$$P'(\zeta) = \frac{p\zeta^{p-1}(\zeta-1) - \zeta^p + 1}{(\zeta-1)^2} = \frac{p\zeta^{p-1}}{\zeta-1} = -\frac{p\zeta^{p-1}}{1-\zeta}.$$

En appliquant la norme, on trouve par la proposition 2.1.33,

$$N_{\mathbb{Q}(\zeta)}(P'(\zeta)) = N_{\mathbb{Q}(\zeta)}\left(-\frac{p\zeta^{p-1}}{1-\zeta}\right) = N_{\mathbb{Q}(\zeta)}(-1) \frac{N_{\mathbb{Q}(\zeta)}(p)N_{\mathbb{Q}(\zeta)}(\zeta^{p-1})}{N_{\mathbb{Q}(\zeta)}(1-\zeta)} = \frac{p^{p-1}}{p} = p^{p-2}.$$

Pour le signe, il suffit de montrer que $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{(p-1)(p-2)}{2}}$, c'est-à-dire que $\frac{p-1}{2} \equiv \frac{(p-1)(p-2)}{2} \pmod{2}$ [2]. Cela suit de la congruence $p-1 \equiv p^2-3p+2 = (p-1)(p-2) \pmod{4}$. Remarquons que $p^2 \equiv 1 \pmod{4}$ puisque p est impair. Il en suit

$$p^2 \equiv 1 \pmod{4} \iff p^2-4p+2 \equiv -1 \pmod{4} \iff p^2-3p+2 \equiv p-1 \pmod{4} \iff (p-1)(p-2) \equiv p-1 \pmod{4}$$

$$\implies \frac{(p-1)(p-2)}{2} \equiv \frac{p-1}{2} [2].$$

□

2.2 Anneaux de Dedekind

2.2.1 Propriétés des anneaux de Dedekind

Avant d'entamer cette section, on rappelle le théorème suivant dont une preuve est donnée dans le cours d'algèbre commutative LMAT1331 [23].

Théorème 2.2.1 (Krull). *Soit $\mathbb{A}$ un anneau commutatif unitaire, tout idéal propre de $\mathbb{A}$ est contenu dans un idéal maximal.*

Définition 2.2.2 (Anneau de Dedekind). Un anneau est dit de *Dedekind* s'il est noethérien, intégralement clos et si tous ses idéaux premiers non nuls sont maximaux.

Proposition 2.2.3. *Tout anneau principal est de Dedekind.*

Démonstration. Un anneau principal est noethérien d'après la proposition 1.2.5. Il est aussi factoriel donc intégralement clos par la proposition 2.1.48.

La preuve que les idéaux premiers non nuls sont maximaux dans un anneau principal peut être trouvée dans le cours d'algèbre commutative LMAT1331 [23]. □

Proposition 2.2.4. *Soit $\mathbb{A}$ un anneau, $I_1, \dots, I_n \trianglelefteq \mathbb{A}$ et P un idéal premier non nul de $\mathbb{A}$. Si $I_1 \cdots I_n \subset P$, alors il existe $i \in \llbracket 1, n \rrbracket$ tel que $I_i \subset P$.*

Démonstration. Supposons par l'absurde que pour tout $i \in \llbracket 1, n \rrbracket$, $I_i \not\subset P$, cela veut dire qu'il existe $a_i \in I_i \setminus P$ pour tout $i \in \llbracket 1, n \rrbracket$. Par hypothèse, $\prod_{i=1}^n a_i \in P$, mais puisque P est premier, il existe $i \in \llbracket 1, n \rrbracket$ tel que $a_i \in P$, ce qui est une contradiction. □

Lemme 2.2.5. *Soit $\mathbb{A}$ un anneau noethérien et $0 \neq I \trianglelefteq \mathbb{A}$. Il existe $P_1, \dots, P_k \in \text{Spec}(\mathbb{A})$ tel que $P_1 \cdots P_k \subset I$.*

Démonstration. Soit S l'ensemble des idéaux non nuls de $\mathbb{A}$ qui ne contiennent pas un produit d'idéaux premiers non nuls et supposons par l'absurde que $S \neq \emptyset$. Puisque $\mathbb{A}$ est noethérien, S admet un élément maximal, disons J . Cet idéal n'est pas premier car $J \subset J$ et $J \in S$, et donc il existe $a, b \in \mathbb{A} \setminus J$ tels que $ab \in J$. Ainsi, J est contenu strictement dans $J + a\mathbb{A}$ et $J + b\mathbb{A}$. Ces deux derniers idéaux n'appartiennent pas à S , donc par maximalité de J , cela veut dire qu'ils contiennent chacun un produit d'idéaux premiers non nuls. De même pour leur produit, or $(J + a\mathbb{A}) \cdot (J + b\mathbb{A}) = J^2 + aJ + bJ + ab\mathbb{A} \subset J$, ce qui contredit $J \in S$. $\square$

Lemme 2.2.6. *Soit $\mathbb{A}$ un anneau noethérien dont tous les idéaux premiers non nuls sont maximaux, $\mathbb{K}$ son corps des fractions et I un idéal propre non nul de $\mathbb{A}$. Il existe $\omega \in \mathbb{K} \setminus \mathbb{A}$ tel que $\omega I \subset \mathbb{A}$.*

Démonstration. Soit $a \in I$ non nul, par le lemme 2.2.5, $a\mathbb{A}$ contient un produit d'idéaux premiers non nuls, soit $P_1 \cdots P_k$ un tel produit avec k minimal. Par le théorème de Krull 2.2.1, il existe un idéal maximal M qui contient I , et donc il contient en particulier $a\mathbb{A}$ et donc aussi $P_1 \cdots P_k$. Grâce à la proposition 2.2.4, on sait qu'il existe $i \in \llbracket 1, k \rrbracket$ tel que $P_i \subset M$. Sans perte de généralité, disons que $P_1 \subset M$, par hypothèse P_1 est aussi maximal et donc $P_1 = M$. Aussi, puisque $a\mathbb{A}$ ne contient pas de produit de $k - 1$ idéaux premiers non nuls (car $a\mathbb{A} \subset I$), il existe $b \in P_2 \cdots P_k \setminus a\mathbb{A}$. En posant $\omega = \frac{b}{a}$, on a que $\omega \notin \mathbb{A}$ car $b \notin a\mathbb{A}$ et on a bien que $\omega I \subset \mathbb{A}$: soit $c \in I$, alors $\omega c = \frac{bc}{a}$ mais $c \in P_1$ et $b \in P_2 \cdots P_k$ donc $bc \in P_1 P_2 \cdots P_k \subset a\mathbb{A}$ et donc $\omega c \in \mathbb{A}$. $\square$

Proposition 2.2.7. *Soit $\mathbb{A}$ un anneau de Dedekind, $\mathbb{K}$ son corps de fractions et soit $I \trianglelefteq \mathbb{A}$ non nul. Il existe $J \trianglelefteq \mathbb{A}$ non nul tel que IJ soit principal.*

Démonstration. Soit $a \in I$ non nul, on pose $J := \{x \in \mathbb{A} \mid xI \subset a\mathbb{A}\}$, c'est un idéal non nul car $a \in J$ et par définition on a $IJ \subset a\mathbb{A}$. Soit $H = \frac{1}{a}IJ$, montrons que $H = \mathbb{A}$ pour avoir $IJ = a\mathbb{A}$. Supposons par l'absurde que $H \neq \mathbb{A}$, alors par le lemme 2.2.6, il existe $\omega \in \mathbb{K} \setminus \mathbb{A}$ tel que $\omega H \subset \mathbb{A}$. Puisque $a \in I$, on a $J \subset H$ et donc $\omega J \subset \omega H \subset \mathbb{A}$. On va montrer maintenant que $\omega J \subset J$: soit $b \in J$ et $c \in I$, on a par définition de J que $bc \in a\mathbb{A}$, il existe donc $d \in \mathbb{A}$ tel que $bc = ad$. On a alors que $d \in H$ et donc que $\omega d \in \mathbb{A}$. On obtient finalement $\omega bc = \omega da \in a\mathbb{A}$ et on conclut que $\omega b \in J$ et donc $\omega J \subset J$. Puisque $\mathbb{A}$ est noethérien, J est un $\mathbb{A}$ -module de type fini et donc $\mathbb{A}[\omega]$ est un $\mathbb{A}$ -module de type fini. Par la proposition 2.1.4, ω est entier sur $\mathbb{A}$ sauf que $\mathbb{A}$ est de Dedekind donc intégralement clos, on conclut que $\omega \in \mathbb{A}$, une contradiction. $\square$

Proposition 2.2.8. *Soit $\mathbb{A}$ un anneau de Dedekind et $I, J, H \trianglelefteq \mathbb{A}$ avec $H \neq 0$. Si $HI = HJ$ alors $I = J$.*

Démonstration. Par la proposition précédente 2.2.7, il existe T un idéal non nul de $\mathbb{A}$ tel que $TH = a\mathbb{A}$ pour $a \in \mathbb{A}^*$, on a alors que $THI = THJ$, c'est-à-dire $aI = aJ$ et donc $I = J$. $\square$

Définition 2.2.9. Soit $\mathbb{A}$ un anneau de Dedekind et I, J des idéaux non nuls de $\mathbb{A}$, on dit que J *divise* I s'il existe H un idéal non nul de $\mathbb{A}$ tel que $JH = I$.

Proposition 2.2.10. Soit $\mathbb{A}$ un anneau de Dedekind et $I, J \trianglelefteq \mathbb{A}$ non nuls. On a que J divise I si et seulement si $I \subset J$.

Démonstration. On a toujours que J divise I implique $I \subset J$. Faisons la réciproque, si $I \subset J$, prenons H un idéal non nul de $\mathbb{A}$ tel que $JH = a\mathbb{A}$ pour $a \in \mathbb{A}^*$, ce que l'on peut faire par la proposition 2.2.7. Posons $T = \frac{1}{a}HI$, c'est un idéal de $\mathbb{A}$ car $I \subset J$ et on obtient $JT = \frac{1}{a}JHI = I$ donc J divise I . $\square$

Théorème 2.2.11. Soit $\mathbb{A}$ un anneau de Dedekind, on a que tout idéal non nul de $\mathbb{A}$ se décompose en produit d'idéaux premiers de façon unique à l'ordre près des facteurs.

Démonstration. Soit S l'ensemble des idéaux non nuls de $\mathbb{A}$ qui ne se décomposent pas en produit d'idéaux premiers et supposons par l'absurde que $S \neq \emptyset$. Puisque $\mathbb{A}$ est noethérien, S admet un élément maximal I . Par le théorème de Krull 2.2.1, il existe un idéal maximal P tel que $I \subset P$ et par la proposition 2.2.10, on a alors qu'il existe un idéal non nul J tel que $I = PJ$. On a alors aussi que $I \subset J$ mais $I \neq J$ car sinon, on aurait $P = \mathbb{A}$ par la proposition 2.2.8. Ainsi, la maximalité de I dans S nous dit que $J \notin S$ et donc il se décompose en produit d'idéaux premiers non nuls, et $I = PJ$ nous donne alors une contradiction. Pour l'unicité, supposons que $I = P_1 \cdots P_k = Q_1 \cdots Q_t$ avec chaque P_i et Q_i premier, alors on a que P_1 divise $Q_1 \cdots Q_t$ et donc par la proposition 2.2.10, $Q_1 \cdots Q_t \subset P_1$. La proposition 2.2.4 nous dit qu'il existe $i \in \llbracket 1, t \rrbracket$ tel que $Q_i \subset P_1$. Or, $\mathbb{A}$ est de Dedekind et donc Q_i est maximal et donc $P_1 = Q_i$. En appliquant la proposition 2.2.8, on obtient $\prod_{j=2}^k P_j = \prod_{j \neq i} Q_j$, on refait alors le même raisonnement sur cette dernière égalité pour trouver le résultat escompté. $\square$

2.2.2 Cas des anneaux d'entiers et norme d'un idéal

Proposition 2.2.12. Si $\mathbb{A}$ un anneau de Dedekind, alors $\mathbb{A}$ est factoriel si et seulement s'il est principal.

Démonstration. Un anneau principal est toujours factoriel d'après la proposition 1.2.26. Soit I un idéal propre non nul de $\mathbb{A}$ et $0 \neq a \in I$, puisque $\mathbb{A}$ est factoriel alors il existe $p_1, \dots, p_k \in \mathbb{A}$ irréductibles tels que $a = p_1 \cdots p_k$, en particulier, cela donne une décomposition de l'idéal principal engendré par a en produit d'idéaux premiers : $a\mathbb{A} = p_1\mathbb{A} \cdots p_k\mathbb{A}$. Puisque $a \in I$ alors $a\mathbb{A} \subset I$ et donc I divise $a\mathbb{A}$ par la proposition 2.2.10. Par le théorème 2.2.11, on a que I est un produit de $p_i\mathbb{A}$, c'est donc un idéal principal comme produits d'idéaux principaux. $\square$

Proposition 2.2.13. *Les idéaux non nuls d'un anneau d'entiers d'un corps de nombres $\mathbb{K}$ sont d'indice fini dans $\mathcal{O}_{\mathbb{K}}$.*

Démonstration. Comme pour la preuve de la proposition 2.1.29, on note $G = \text{Hom}(\mathbb{L}, \mathbb{C})$ et $G^* = G \setminus \{\iota\}$ où $\mathbb{L}$ est un sous-corps de $\mathbb{C}$ isomorphe à $\mathbb{K}$ et $\iota : \mathbb{L} \hookrightarrow \mathbb{C}$ est le morphisme d'inclusion. On note λ l'isomorphisme $\mathbb{K} \rightarrow \mathbb{L}$. Soit $I \trianglelefteq \mathcal{O}_{\mathbb{K}}$ non nul, alors il existe $a \in I$ non nul. On a par définition d'un idéal que

$$|N_{\mathbb{L}}(\lambda(a))| = \lambda(a) \times (\pm 1) \times \prod_{\sigma \in G^*} \sigma(\lambda(a)) \in \lambda(I)$$

car $\prod_{\sigma \in G^*} \sigma(\lambda(a)) \in \mathcal{O}_{\mathbb{L}}$. Le fait que $\prod_{\sigma \in G^*} \sigma(\lambda(a)) \in \mathcal{O}_{\mathbb{L}}$ se prouve comme dans la proposition 2.1.29 grâce à la proposition 2.1.16. Il suit alors du corollaire 1.2.34 que $\mathcal{O}_{\mathbb{L}}/|N_{\mathbb{L}}(\lambda(a))|\mathcal{O}_{\mathbb{L}}$ est fini car c'est un groupe abélien de torsion et de type fini. On conclut car

$$|N_{\mathbb{L}}(\lambda(a))| \in \lambda(I) \implies \#\mathcal{O}_{\mathbb{K}}/I = \#\mathcal{O}_{\mathbb{L}}/\lambda(I) \leq \#\mathcal{O}_{\mathbb{L}}/|N_{\mathbb{L}}(\lambda(a))|\mathcal{O}_{\mathbb{L}} < +\infty.$$

□

Corollaire 2.2.14. *Tous les idéaux non nuls d'un anneau d'entiers d'un corps de nombres $\mathbb{K}$ sont des $\mathbb{Z}$ -modules du même rang que $\mathcal{O}_{\mathbb{K}}$.*

Théorème 2.2.15 (Petit théorème de Wedderburn). *Un anneau fini intègre non trivial est un corps.*

Démonstration. Soit $\mathbb{A}$ un tel anneau et $x \in \mathbb{A}^*$. L'application $m_x : \mathbb{A} \rightarrow \mathbb{A} : a \mapsto xa$ est un endomorphisme du groupe additif sous-jacent, qui a un noyau trivial car $\mathbb{A}$ est intègre. On en déduit que m_x est injectif mais puisque $\mathbb{A}$ est fini, il est aussi surjectif, il existe donc $y \in \mathbb{A}$ tel que $m_x(y) = 1_{\mathbb{A}}$, c'est-à-dire $xy = 1_{\mathbb{A}}$. □

Proposition 2.2.16. *L'anneau des entiers d'un corps de nombres est un anneau de Dedekind.*

Démonstration. • L'anneau des entiers d'un corps de nombres est noethérien : par le corollaire 2.1.54, on a que le groupe additif de $\mathcal{O}_{\mathbb{K}}$ est abélien de type fini. En particulier le groupe est noethérien d'après le corollaire 1.2.32, donc tous ses sous groupes sont de type fini, en particulier les idéaux de $\mathcal{O}_{\mathbb{K}}$. Les $\mathbb{Z}$ -bases des idéaux forment aussi une partie génératrice en tant qu'idéal.

- L'anneau des entiers d'un corps de nombres est intégralement clos : on a que $\mathbb{K}$ est le corps des fractions de $\mathcal{O}_{\mathbb{K}}$ par la proposition 2.1.46. Soit $x \in \mathbb{K}$ dans la fermeture intégrale de $\mathcal{O}_{\mathbb{K}}$, on veut montrer que $x \in \mathcal{O}_{\mathbb{K}}$, c'est-à-dire qu'il est entier sur $\mathbb{Z}$. Par définition, x est entier sur $\mathcal{O}_{\mathbb{K}}$ donc il existe un polynôme unitaire $T \in \mathcal{O}_{\mathbb{K}}[X]$ tel que $T(x) = 0$. Disons que $T(X) = X^m + a_{m-1}X^{m-1} + \dots + a_1X + a_0$ avec

$a_k \in \mathcal{O}_{\mathbb{K}}$ pour tout $k \in \llbracket 0, m-1 \rrbracket$ alors ces a_k sont par définition entiers sur $\mathbb{Z}$ et donc $\mathbb{Z}[a_1, \dots, a_{m-1}]$ est un $\mathbb{Z}$ -module de type fini par la proposition 2.1.4. Or, l'équation de dépendance intégrale $T(x) = 0$ de x sur $\mathcal{O}_{\mathbb{K}}$ est aussi une équation de dépendance intégrale de x sur $\mathbb{Z}[a_1, \dots, a_{m-1}]$, donc x est entier sur $\mathbb{Z}[a_1, \dots, a_{m-1}]$. Toujours par la proposition 2.1.4, on a que $\mathbb{Z}[a_1, \dots, a_{m-1}][x]$ est un $\mathbb{Z}[a_1, \dots, a_{m-1}]$ -module de type fini. Par la proposition 1.2.6, on obtient que $\mathbb{Z}[a_1, \dots, a_{m-1}][x] \cong \mathbb{Z}[a_1, \dots, a_{m-1}, x]$ est un $\mathbb{Z}$ -module de type fini. On conclut avec la proposition 2.1.4.

- Les idéaux premiers non nuls d'un anneau des entiers d'un corps de nombres sont maximaux : soit P un idéal premier non nul de $\mathcal{O}_{\mathbb{K}}$, alors $\mathcal{O}_{\mathbb{K}}/P$ est un anneau intègre non trivial mais fini par la proposition 2.2.13. Le petit théorème de Wedderburn 2.2.15 nous dit alors que $\mathcal{O}_{\mathbb{K}}/P$ est un corps et donc P est maximal. $\square$

Définition 2.2.17. Deux idéaux I, J non nuls de $\mathbb{A}$ sont dit *premiers entre eux* ou *relativement premiers* lorsque $I + J = \mathbb{A}$.

On utilisera même parfois le terme *copremiers*.

Définition 2.2.18 (Norme d'un idéal). Soit $\mathbb{K}$ un corps de nombres et $0 \neq I \leq \mathcal{O}_{\mathbb{K}}$ un idéal, on définit sa *norme* comme $N_{\mathbb{K}}(I) = |\mathcal{O}_{\mathbb{K}}/I|$.

Cette norme est une fonction ayant $\mathbb{N}^*$ pour codomaine par la proposition 2.2.13. L'usage du terme de norme et l'abus de notation avec la norme d'un entier algébrique est motivé par l'égalité $|N_{\mathbb{K}}(\alpha)| = N_{\mathbb{K}}(\alpha\mathcal{O}_{\mathbb{K}})$. Ce sera vu en détail dans la proposition 2.2.22.

Proposition 2.2.19. *Cette norme est multiplicative.*

Démonstration. Si I et J sont premiers entre eux, alors le théorème des restes chinois nous dit que $\mathcal{O}_{\mathbb{K}}/IJ \cong \mathcal{O}_{\mathbb{K}}/I \times \mathcal{O}_{\mathbb{K}}/J$ et donc

$$N_{\mathbb{K}}(IJ) = |\mathcal{O}_{\mathbb{K}}/IJ| = |\mathcal{O}_{\mathbb{K}}/I \times \mathcal{O}_{\mathbb{K}}/J| = |\mathcal{O}_{\mathbb{K}}/I| \times |\mathcal{O}_{\mathbb{K}}/J| = N_{\mathbb{K}}(I) \times N_{\mathbb{K}}(J).$$

Par le théorème 2.2.11, il suffit alors de montrer que $N_{\mathbb{K}}(P^m) = N_{\mathbb{K}}(P)^m$ pour $P \in \text{Spec}(\mathcal{O}_{\mathbb{K}})$. Par le troisième théorème d'isomorphisme, on a

$$N_{\mathbb{K}}(P^m) = |\mathcal{O}_{\mathbb{K}}/P^m| = |\mathcal{O}_{\mathbb{K}}/P| \times |P/P^2| \times |P^2/P^3| \times \dots \times |P^{m-1}/P^m|.$$

Il reste alors à montrer l'isomorphisme de groupes $\mathcal{O}_{\mathbb{K}}/P \cong P^k/P^{k+1}$ pour $k \in \llbracket 1, m-1 \rrbracket$. Soit $k \in \llbracket 1, m-1 \rrbracket$ et $x \in P^k \setminus P^{k+1}$, et posons $t_x : \mathcal{O}_{\mathbb{K}} \rightarrow P^k : y \mapsto xy$. On a que $\text{Im}(t_x) = x\mathcal{O}_{\mathbb{K}} \subset P^k$ mais $P^{k+1} \subset P^k$ aussi, il en suit que $x\mathcal{O}_{\mathbb{K}} + P^{k+1} \subset P^k$. On a alors la chaîne d'inclusion $P^{k+1} \subset x\mathcal{O}_{\mathbb{K}} + P^{k+1} \subset P^k$ où la première inclusion est stricte car $x \notin P^{k+1}$, et donc le théorème 2.2.11 induit l'égalité $x\mathcal{O}_{\mathbb{K}} + P^{k+1} = P^k$. Soit $\pi : P^k \rightarrow P^k/P^{k+1}$ le morphisme de projection canonique, l'égalité précédente nous dit

que $\pi \circ t_x$ est surjectif. Inspectons le noyau de ce morphisme : $y \in \text{Ker}(\pi \circ t_x)$ si et seulement si $xy \in P^{k+1}$ mais P^{k+1} est un idéal primaire donc soit $x \in P^{k+1}$, soit il existe $j \in \mathbb{N}^*$ tel que $y^j \in P^{k+1}$. On a pris $x \notin P^{k+1}$ donc il existe bien $j \in \mathbb{N}^*$ tel que $y^j \in P^{k+1} \subset P$, on conclut que $y \in P$ par primalité de P et donc $\text{Ker}(\pi \circ t_x) \subset P$. Aussi, puisque $x \in P^k$, on a que $xz \in P^{k+1}$ pour $z \in P$ et donc $P \subset \text{Ker}(\pi \circ t_x)$. On a alors que $P = \text{Ker}(\pi \circ t_x)$ et on conclut par le premier théorème d'isomorphisme. $\square$

Proposition 2.2.20. *Soit $\mathbb{K}$ un corps de nombres et I un idéal non nul de $\mathcal{O}_{\mathbb{K}}$. Si $N_{\mathbb{K}}(I)$ est un nombre premier alors I est un idéal maximal.*

Démonstration. Soit $J \trianglelefteq \mathcal{O}_{\mathbb{K}}$ tel que $I \subset J$, par la proposition 2.2.10, J divise I , donc il existe $H \trianglelefteq \mathcal{O}_{\mathbb{K}}$ non nul tel que $JH = I$. Par la multiplicativité des normes 2.2.19, on a $N_{\mathbb{K}}(J)N_{\mathbb{K}}(H) = N_{\mathbb{K}}(I)$. Puisque $N_{\mathbb{K}}(I)$ est premier, on a soit que $N_{\mathbb{K}}(J) = N_{\mathbb{K}}(I)$ mais alors $N_{\mathbb{K}}(H) = |\mathcal{O}_{\mathbb{K}}/H| = 1$, donc $H = \mathcal{O}_{\mathbb{K}}$ et $I = J$, soit $N_{\mathbb{K}}(J) = |\mathcal{O}_{\mathbb{K}}/J| = 1$ et $J = \mathcal{O}_{\mathbb{K}}$. $\square$

Proposition 2.2.21. *Soit $\mathbb{K}$ un corps de nombres, $0 \neq I \trianglelefteq \mathcal{O}_{\mathbb{K}}$ et $y = (y_1, \dots, y_n)$ une $\mathbb{Z}$ -base de cet idéal. On a*

$$N_{\mathbb{K}}(I) = \sqrt{\left| \frac{\Delta(y)}{\Delta_{\mathbb{K}}} \right|}.$$

Démonstration. Soit $x = (x_1, \dots, x_n)$ une $\mathbb{Z}$ -base de $\mathcal{O}_{\mathbb{K}}$, alors il existe $B = (b_{ij})_{i,j \in [1,n]}$ telle que $y = xB$. Par la proposition 1.2.35, on a que $N(I) = |\mathcal{O}_{\mathbb{K}}/I| = |\det(B)|$. Ensuite, la proposition 2.1.42 nous dit que $\Delta(y) = \det(B)^2 \Delta(x) = N(I)^2 \Delta_{\mathbb{K}}$. On obtient le résultat voulu en divisant par $\Delta_{\mathbb{K}}$ et en appliquant la racine carrée. $\square$

Le corollaire suivant justifie le fait d'utiliser le même terme de norme et la même notation pour les éléments de $\mathcal{O}_{\mathbb{K}}$ que pour ses idéaux.

Corollaire 2.2.22. *Soit $\mathbb{K}$ un corps de nombres et $x \in \mathcal{O}_{\mathbb{K}}$ alors $|N_{\mathbb{K}}(x)| = |\mathcal{O}_{\mathbb{K}}/x\mathcal{O}_{\mathbb{K}}|$.*

Démonstration. Il suffit de voir qu'une $\mathbb{Z}$ -base de $x\mathcal{O}_{\mathbb{K}}$ est $(xa_1, \dots, xa_n)$ si $(a_1, \dots, a_n)$ est une $\mathbb{Z}$ -base de $\mathcal{O}_{\mathbb{K}}$ et d'appliquer la proposition 2.2.21. $\square$

Proposition 2.2.23. *Soit $\mathbb{K}$ un corps de nombres et $0 \neq I \trianglelefteq \mathcal{O}_{\mathbb{K}}$, on a que $N_{\mathbb{K}}(I) \in I$.*

Démonstration. On a que pour tout $x \in \mathcal{O}_{\mathbb{K}}$, $N_{\mathbb{K}}(I)x \in I$. En effet, d'après la proposition 2.2.13, le groupe additif $\mathcal{O}_{\mathbb{K}}/I$ est fini, et l'ordre de ce groupe définit $N_{\mathbb{K}}(I)$. Il suit du théorème de Lagrange que $N_{\mathbb{K}}(I)x + I$ est l'élément neutre de ce groupe, c'est-à-dire que $N_{\mathbb{K}}(I)x \in I$. Il suffit alors de prendre $x = 1$ pour conclure. $\square$

Proposition 2.2.24. Soit $\mathbb{K}$ un corps de nombres, il n'y a qu'un nombre fini d'idéaux de $\mathcal{O}_{\mathbb{K}}$ d'une norme donnée.

Démonstration. Soit $N \in \mathbb{N}^*$. On a que tous les idéaux de $\mathcal{O}_{\mathbb{K}}$ admettant N comme norme contiennent l'élément N d'après la proposition 2.2.23. En particulier, l'idéal $N\mathcal{O}_{\mathbb{K}}$ est inclus dans tout idéal de norme N . Or, les idéaux de $\mathcal{O}_{\mathbb{K}}$ contenant $N\mathcal{O}_{\mathbb{K}}$ sont en bijection avec les idéaux de $\mathcal{O}_{\mathbb{K}}/N\mathcal{O}_{\mathbb{K}}$ qui est fini d'après la proposition 2.2.13. $\square$

2.2.3 Factorisation des nombres premiers dans $\mathcal{O}_{\mathbb{K}}$

Proposition 2.2.25. Soit $\mathbb{K}$ un corps de nombres et P un idéal premier non nul de $\mathcal{O}_{\mathbb{K}}$. Il existe un unique nombre premier rationnel positif $p \in P$.

Démonstration. Puisque $\mathcal{O}_{\mathbb{K}}$ est un anneau de Dedekind, on a que P est maximal et donc $\mathcal{O}_{\mathbb{K}}/P$ est un corps fini. Il en suit qu'il existe un nombre premier rationnel p et $f \in \mathbb{N}^*$ tel que $N_{\mathbb{K}}(P) = |\mathcal{O}_{\mathbb{K}}/P| = p^f$. D'après la proposition 2.2.23, $p^f \in P$, mais puisque P est premier on obtient bien $p \in P$. L'unicité suit de la proposition 2.1.35. $\square$

Définition 2.2.26. Soit p un nombre premier rationnel. D'après 2.2.11, l'idéal $p\mathcal{O}_{\mathbb{K}}$ admet une décomposition essentiellement unique en produit d'idéaux premiers

$$p\mathcal{O}_{\mathbb{K}} = \prod_{k=1}^m P_k^{e_k}.$$

- Si $m = e_m = 1$, $p\mathcal{O}_{\mathbb{K}}$ est premier, on dit alors que p est *inerte* dans $\mathcal{O}_{\mathbb{K}}$.
- Si l'un des $e_k > 1$, on dit que p est *ramifié* dans $\mathcal{O}_{\mathbb{K}}$, si de plus $m = 1$, alors on dit que p est *totalelement ramifié*.
- Si $e_k = 1$ pour tout $k \in \llbracket 1, m \rrbracket$, on dit que p est *décomposé* dans $\mathcal{O}_{\mathbb{K}}$.

Lemme 2.2.27. Soit $\mathbb{K}$ un corps de nombres de degré n , $\alpha \in \mathcal{O}_{\mathbb{K}}$ et $T \in \mathbb{Z}[X]$ son polynôme minimal. Pour tout nombre premier rationnel p ne divisant pas l'indice $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\alpha]]$, considérons la décomposition de T en polynômes irréductibles moniques modulo p

$$T \equiv \prod_{k=1}^m T_k^{e_k} \pmod{p}.$$

On a alors que pour tout $k \in \llbracket 1, m \rrbracket$, soit $p\mathcal{O}_{\mathbb{K}} + T_k(\alpha) = \mathcal{O}_{\mathbb{K}}$, soit $\mathcal{O}_{\mathbb{K}}/(p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})$ est un corps fini d'ordre p^{f_k} où $f_k = \deg(T_k)$.

Démonstration. Soit $k \in \llbracket 1, m \rrbracket$, on a premièrement que $(\mathbb{Z}/p\mathbb{Z})[X]/T_k(\mathbb{Z}/p\mathbb{Z})[X] \cong \mathbb{F}_{p^{f_k}}$ car T_k est un polynôme irréductible modulo p de degré f_k . Il en suit de théorèmes d'isomorphismes que $\mathbb{Z}[X]/(p\mathbb{Z}[X] + T_k\mathbb{Z}[X]) \cong \mathbb{F}_{p^{f_k}}$ et donc $p\mathbb{Z}[X] + T_k\mathbb{Z}[X]$ est un

idéal maximal de $\mathbb{Z}[X]$. Soit $\varepsilon : \mathbb{Z}[X] \rightarrow \mathbb{Z}[\alpha]$ le morphisme d'évaluation et $\pi : \mathcal{O}_{\mathbb{K}} \rightarrow \mathcal{O}_{\mathbb{K}}/(p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})$ le morphisme de projection canonique, puisque $\mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}}$, on peut considérer la composition $\psi = \pi \circ \varepsilon$. Montrons que ψ est surjectif, c'est-à-dire que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha] + p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}}$. La surjectivité de ψ se traduit ainsi car

$$\text{Im}(\psi) = \mathcal{O}_{\mathbb{K}}/(p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}}) \iff \text{Im}(\pi|_{\text{Im}(\varepsilon)}) = \mathcal{O}_{\mathbb{K}}/(p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})$$

$$\iff \text{Im}(\pi|_{\mathbb{Z}[\alpha]}) = \mathcal{O}_{\mathbb{K}}/(p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}}) \iff \forall y \in \mathcal{O}_{\mathbb{K}}, \exists x \in \mathbb{Z}[\alpha] : x - y \in p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}}.$$

On peut alors montrer la surjectivité de ψ en montrant que

$$[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\alpha] + p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}}] = 1.$$

Puisque $\mathbb{Z}[\alpha] + p\mathcal{O}_{\mathbb{K}}$ est un sous-groupe de $\mathbb{Z}[\alpha] + p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}}$, on obtient alors que $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\alpha] + p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}}]$ divise $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\alpha] + p\mathcal{O}_{\mathbb{K}}]$. Ce dernier divise $\text{PGCD}([\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\alpha]], [\mathcal{O}_{\mathbb{K}} : p\mathcal{O}_{\mathbb{K}}])$ mais $[\mathcal{O}_{\mathbb{K}} : p\mathcal{O}_{\mathbb{K}}] = N_{\mathbb{K}}(p) = p^n$ et l'hypothèse nous dit que p ne divise pas $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\alpha]]$, on conclut que le PGCD vaut 1 et on obtient bien que ψ est surjectif. Par le premier théorème d'isomorphisme, on obtient $\mathbb{Z}[X]/\text{Ker}(\psi) \cong \mathcal{O}_{\mathbb{K}}/(p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})$. Enfin, remarquons que l'idéal maximal $p\mathbb{Z}[X] + T_k\mathbb{Z}[X]$ est inclut dans $\text{Ker}(\psi)$, ce qui implique que soit $\text{Ker}(\psi) = p\mathbb{Z}[X] + T_k\mathbb{Z}[X]$, soit $\text{Ker}(\psi) = \mathbb{Z}[X]$. Ainsi, on a soit $\mathcal{O}_{\mathbb{K}}/(p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}}) \cong \mathbb{Z}[X]/(p\mathbb{Z}[X] + T_k\mathbb{Z}[X]) \cong \mathbb{F}_{p^{f_k}}$, soit $\mathcal{O}_{\mathbb{K}}/(p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})$ est trivial, ce qui veut dire que $p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}}$. $\square$

Théorème 2.2.28 (Dedekind–Kummer). *Soit $\mathbb{K}$ un corps de nombres, $\alpha \in \mathcal{O}_{\mathbb{K}}$ et $T \in \mathbb{Z}[X]$ son polynôme minimal. Pour tout nombre premier rationnel p ne divisant pas l'indice $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\alpha]]$, considérons la décomposition de T en polynômes irréductibles moniques modulo p*

$$T \equiv \prod_{k=1}^m T_k^{e_k} [p].$$

On a alors que

$$p\mathcal{O}_{\mathbb{K}} = \prod_{k=1}^m (p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})^{e_k}.$$

Démonstration. Procédons par double inclusion.

- $\prod_{k=1}^m (p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})^{e_k} \subset p\mathcal{O}_{\mathbb{K}}$: cette inclusion est une conséquence de la suivante

$$\prod_{k=1}^m (p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})^{e_k} \subset p\mathcal{O}_{\mathbb{K}} + \prod_{k=1}^m T_k^{e_k}(\alpha)\mathcal{O}_{\mathbb{K}} \subset p\mathcal{O}_{\mathbb{K}}.$$

La première inclusion est obtenu par distributivité. Pour la seconde inclusion, on a par définition que $(\prod_{k=1}^m T_k^{e_k}) - T \in p\mathbb{Z}[X]$, donc en évaluant en α , on obtient $\prod_{k=1}^m T_k^{e_k}(\alpha) \in p\mathbb{Z}[\alpha] \subset p\mathcal{O}_{\mathbb{K}}$ car T est le polynôme minimal de α .

- $p\mathcal{O}_{\mathbb{K}} \subset \prod_{k=1}^m (p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})^{e_k}$: D'après le lemme 2.2.27, on peut réarranger les indices de façon à obtenir $p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}} \neq \mathcal{O}_{\mathbb{K}}$ pour tout $k \in \llbracket 1, l \rrbracket$ et $p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}}$ pour tout $k \in \llbracket l, m \rrbracket$ (pour un certain $l \in \llbracket 1, m \rrbracket$). Ce même lemme nous dit alors que les idéaux $p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}}$ pour $k \in \llbracket 1, l \rrbracket$ sont maximaux, puisque l'anneau quotient est un corps. En particulier ils sont premiers, montrons alors qu'ils sont premiers entre eux. On a que les polynômes T_k et $T_{k'}$ sont premiers entre eux dans $\mathbb{F}_p[X]$, il existe donc d'après le théorème de Bézout 1.2.27 $U, V \in \mathbb{Z}[X]$ tels que $UT_k + VT_{k'} \equiv 1 \pmod{p}$. C'est-à-dire qu'il existe $W \in \mathbb{Z}[X]$ tel que $UT_k + VT_{k'} = 1 + pW$, en évaluant cette égalité polynomiale en α , et en retranchant $pW(\alpha)$, on obtient $1 = U(\alpha)T_k(\alpha) + V(\alpha)T_{k'}(\alpha) - pW(\alpha)$. Il en suit que

$$\begin{aligned} 1 &\in p\mathbb{Z}[\alpha] + T_k(\alpha)\mathbb{Z}[\alpha] + T_{k'}(\alpha)\mathbb{Z}[\alpha] \subset p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}} + T_{k'}(\alpha)\mathcal{O}_{\mathbb{K}} \\ &= p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}} + p\mathcal{O}_{\mathbb{K}} + T_{k'}(\alpha)\mathcal{O}_{\mathbb{K}}. \end{aligned}$$

On en déduit bien que $p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}} + p\mathcal{O}_{\mathbb{K}} + T_{k'}(\alpha)\mathcal{O}_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}}$. En outre, le point précédent et la proposition 2.2.10 nous disent que $p\mathcal{O}_{\mathbb{K}}$ divise $\prod_{k=1}^m (p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})^{e_k} = \prod_{k=1}^l (p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})^{e_k}$, mais le théorème 2.2.11 nous dit alors que $p\mathcal{O}_{\mathbb{K}} = \prod_{k=1}^l (p\mathcal{O}_{\mathbb{K}} + T_k(\alpha)\mathcal{O}_{\mathbb{K}})^{s_k}$ pour certain $s_k \in \llbracket 1, e_k \rrbracket$ car ces idéaux sont premiers entre eux. Enfin, on a d'une part que $n = \sum_{k=1}^l s_k f_k$, mais on a aussi d'autre part que $\deg(T) = n = \sum_{k=1}^m e_k f_k$, et donc on conclut que $l = m$ et $s_k = e_k$ pour tout $k \in \llbracket 1, m \rrbracket$. $\square$

Exemple 2.2.29. • 2 est totalement ramifié dans $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$: $X^2 + 5 \equiv X^2 + 1 \equiv (X + 1)^2 \pmod{2}$ donc d'après le théorème de Dedekind–Kummer 2.2.28, on a que $2\mathbb{Z}[\sqrt{-5}] = (2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}])^2$. L'idéal $2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ a pour norme 2, s'il était principal, cela impliquerait l'existence d'un élément $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ de norme ± 2 d'après 2.2.22. Or, $N_{\mathbb{Q}(\sqrt{-5})}(a + b\sqrt{-5}) = a^2 + 5b^2$ et l'équation diophantienne $a^2 + 5b^2 = \pm 2$ n'a pas de solutions, donc $2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ n'est pas principal.

- 2 est totalement ramifié dans $\mathbb{Z}[\sqrt{6}]$: $X^2 - 6 \equiv X^2 \pmod{2}$ donc d'après le théorème de Dedekind–Kummer 2.2.28, on a que $2\mathbb{Z}[\sqrt{6}] = (2\mathbb{Z}[\sqrt{6}] + \sqrt{6}\mathbb{Z}[\sqrt{6}])^2$. Remarquons que $N_{\mathbb{Q}(\sqrt{6})}(2 + \sqrt{6}) = 2^2 - 6 \cdot 1^2 = -2$ donc d'après les propositions 2.2.23 et 2.1.30, on a $2\mathbb{Z}[\sqrt{6}] + \sqrt{6}\mathbb{Z}[\sqrt{6}] = (2 + \sqrt{6})\mathbb{Z}[\sqrt{6}]$.
- 2 et 3 sont totalement ramifiés dans $\mathbb{Z}[\sqrt{-6}]$: $X^2 + 6 \equiv X^2 \pmod{2}$ et $X^2 + 6 \equiv X^2 \pmod{3}$ donc d'après le théorème de Dedekind–Kummer 2.2.28, on a que $2\mathbb{Z}[\sqrt{-6}] = (2\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}])^2$ et $3\mathbb{Z}[\sqrt{-6}] = (3\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}])^2$. L'idéal $2\mathbb{Z}[\sqrt{-6}] + (1 + \sqrt{-6})\mathbb{Z}[\sqrt{-6}]$ a pour norme 2, s'il était principal, cela impliquerait l'existence d'un élément $a + b\sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]$ de norme ± 2 d'après 2.2.22. Or, $N_{\mathbb{Q}(\sqrt{-6})}(a + b\sqrt{-6}) = a^2 + 6b^2$ et l'équation diophantienne $a^2 + 6b^2 = \pm 2$ n'a pas de solutions, donc $2\mathbb{Z}[\sqrt{-6}] + (1 + \sqrt{-6})\mathbb{Z}[\sqrt{-6}]$ n'est pas principal. On peut faire le même argument

avec 3.

- 2 est totalement ramifié dans $\mathbb{Z}[\sqrt{7}]$: $X^2 - 7 \equiv X^2 - 1 \equiv (X + 1)^2$ donc d'après le théorème de Dedekind–Kummer 2.2.28, on a que $2\mathbb{Z}[\sqrt{7}] = (2\mathbb{Z}[\sqrt{7}] + (1 + \sqrt{7})\mathbb{Z}[\sqrt{7}])^2$. Remarquons que $N_{\mathbb{Q}(\sqrt{7})}(3 + \sqrt{7}) = 3^2 - 7 \cdot 1^2 = 2$ donc d'après les propositions 2.2.23 et 2.1.30, $2\mathbb{Z}[\sqrt{7}] + (1 + \sqrt{7})\mathbb{Z}[\sqrt{7}] = (3 + \sqrt{7})\mathbb{Z}[\sqrt{7}]$.

Un autre exemple de ramification est donné par la proposition suivante.

Proposition 2.2.30. *Soit p un nombre premier impair et $\zeta = e^{i\frac{2\pi}{p}}$. On a que $p = u(1 - \zeta)^{p-1}$ où $u \in \mathbb{Z}[\zeta]^\times$. En particulier, p est totalement ramifié dans $\mathbb{Z}[\zeta]$.*

Démonstration. D'après la proposition 2.1.38, pour tout $k \in \llbracket 1, p-1 \rrbracket$, il existe $u_k \in \mathbb{Z}[\zeta]^\times$ tels que $1 - \zeta^k = u_k(1 - \zeta)$. En évaluant le $p^{\text{ième}}$ polynôme cyclotomique en 1, on obtient

$$\begin{aligned} \Phi_p(X) &= \sum_{k=0}^{p-1} X^k = \prod_{k=1}^{p-1} (X - \zeta^k) \\ \implies \Phi_p(1) &= p = \prod_{k=1}^{p-1} (1 - \zeta^k) = \prod_{k=1}^{p-1} u_k(1 - \zeta) = (1 - \zeta)^{p-1} \times \prod_{k=1}^{p-1} u_k. \end{aligned}$$

On obtient le résultat escompté en posant $u = \prod_{k=1}^{p-1} u_k$.

En outre, puisque $1 - \zeta$ est irréductible d'après la proposition 2.1.33, on a que $(1 - \zeta)\mathbb{Z}[\zeta]$ est un idéal maximal. On obtient finalement que p est totalement ramifié :

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

□

2.3 Groupe des classes d'idéaux

Le but de cette section est de définir un groupe abélien spécifique, qui sera propre à chaque corps de nombres. Ce groupe mesurera à quel point l'anneau des entiers du corps des nombres est factoriel. On montrera par ailleurs que c'est un groupe fini, ce qui le rend relativement abordable d'après le théorème de Kronecker 1.2.33.

Définition 2.3.1 (Idéal fractionnaire). Soit $\mathbb{A}$ un anneau intègre et $\mathbb{K}$ son corps de fractions. Un *idéal fractionnaire* I de $\mathbb{A}$ est un sous- $\mathbb{A}$ -module non trivial de $\mathbb{K}$ tel qu'il existe $d \in \mathbb{A}^*$ satisfaisant $I \subset \frac{1}{d}\mathbb{A}$. L'ensemble des idéaux fractionnaires de $\mathbb{A}$ est noté $\mathcal{I}_{\mathbb{A}}$.

Il suit de cette définition que les idéaux classiques de $\mathbb{A}$ sont aussi des idéaux fractionnaires, c'est pourquoi on les appellera parfois des idéaux entiers pour éviter toute confusion.

Proposition 2.3.2. *Soit $\mathbb{A}$ un anneau intègre et $\mathbb{K}$ son corps des fractions. Si $\mathbb{A}$ est noethérien, alors un sous- $\mathbb{A}$ -module de $\mathbb{K}$ est de type fini si et seulement si c'est un idéal fractionnaire.*

Démonstration. Si I est un sous- $\mathbb{A}$ -module de type fini, il existe une famille génératrice $(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_n}{b_n})$ de I où $a_k, b_k \in \mathbb{A}^*$ pour tout $k \in \llbracket 1, n \rrbracket$. En posant $b = \prod_{k=1}^n b_k$, on trouve que $bI \subset \mathbb{A}$. Réciproquement, si I est un idéal fractionnaire, il existe $d \in \mathbb{A}^*$ tel que $I \subset \frac{1}{d}\mathbb{A}$. Or $\frac{1}{d}\mathbb{A}$ est un $\mathbb{A}$ -module isomorphe à $\mathbb{A}$, il est donc noethérien, on conclut alors avec la proposition 1.2.3. $\square$

Définition 2.3.3 (Idéal fractionnaire principal). Soit $\mathbb{A}$ un anneau intègre et $\mathbb{K}$ son corps de fractions. Un idéal fractionnaire de $\mathbb{A}$ est dit *principal* s'il est de la forme $s\mathbb{A}$ avec $s \in \mathbb{K}^*$. L'ensemble des idéaux fractionnaires principaux de $\mathbb{A}$ est noté $\mathcal{P}_{\mathbb{A}}$.

Définition 2.3.4. Pour I, J deux idéaux fractionnaires de $\mathbb{A}$, on définit leur produit comme pour les idéaux entiers, c'est-à-dire

$$I \cdot J := \left\{ \sum_{k=1}^m x_k y_k \mid x_k \in I, y_k \in J \forall k \in \llbracket 1, m \rrbracket \right\}.$$

Cette opération munit les ensembles $\mathcal{I}_{\mathbb{A}}$ et $\mathcal{P}_{\mathbb{A}}$ d'une structure de monoïde commutatif où l'élément neutre est donné par l'idéal fractionnaire $\mathbb{A}$.

Proposition 2.3.5. *On a que le monoïde $\mathcal{P}_{\mathbb{A}}$ est un groupe. Dans le cas où $\mathbb{K}$ est un corps de nombres et $\mathbb{A} = \mathcal{O}_{\mathbb{K}}$, on a que $\mathcal{I}_{\mathbb{A}}$ aussi est un groupe.*

Démonstration. On a que $\mathcal{P}_{\mathbb{A}}$ est un groupe car $s\mathbb{A} \cdot \frac{1}{s}\mathbb{A}$ pour tout $s \in \mathbb{K}^*$. Ensuite, si I est un idéal fractionnaire de $\mathcal{O}_{\mathbb{K}}$, alors il existe $d \in \mathcal{O}_{\mathbb{K}}^*$ tel que dI soit un idéal entier de $\mathcal{O}_{\mathbb{K}}$. La proposition 2.2.7 nous dit alors qu'il existe un autre idéal entier de $\mathcal{O}_{\mathbb{K}}$ tel que dIJ soit principal. Ainsi, il existe $s \in \mathcal{O}_{\mathbb{K}}$ tel que $I \cdot d\mathcal{O}_{\mathbb{K}} \cdot J = s\mathcal{O}_{\mathbb{K}}$ et donc l'idéal fractionnaire I est inversible, d'inverse $\frac{d}{s}J$. $\square$

Définition 2.3.6 (Groupe de Picard). Le *groupe de Picard*, ou *groupe des classes d'idéaux* d'un corps de nombres $\mathbb{K}$ est le groupe quotient

$$\text{Pic}(\mathcal{O}_{\mathbb{K}}) := \mathcal{I}_{\mathcal{O}_{\mathbb{K}}} / \mathcal{P}_{\mathcal{O}_{\mathbb{K}}}.$$

Il suit de cette définition que le groupe est trivial exactement quand $\mathcal{O}_{\mathbb{K}}$ est principal, et donc quand il est factoriel d'après la proposition 1.2.26. De cette façon, ce groupe mesure à quel point l'anneau n'est pas factoriel. La relation d'équivalence sur $\mathcal{I}_{\mathcal{O}_{\mathbb{K}}}$ correspondant au sous-groupe $\mathcal{P}_{\mathcal{O}_{\mathbb{K}}}$ est la suivante : I est équivalent à J si et seulement s'il existe $d \in \mathbb{K}^*$ tel que $I = dJ$.

2.3.1 Réseaux

Définition 2.3.7 (Réseau). Soit $(v_1, \dots, v_n)$ une base de $\mathbb{R}^n$. On appelle le sous-groupe du groupe additif de $\mathbb{R}^n$ engendré par cette famille de vecteurs un *réseau* de $\mathbb{R}^n$.

Définition 2.3.8 (Discret). Un sous-ensemble X de $\mathbb{R}^n$ est dit *discret* si pour tout $r \in \mathbb{R}_+^*$, on a $|X \cap B_r(0)| < +\infty$, où B_r désigne la boule ouverte de rayon r dans $\mathbb{R}^n$.

Proposition 2.3.9. *Un réseau de $\mathbb{R}^n$ est un sous groupe discret de $\mathbb{R}^n$.*

Démonstration. Soit Γ un réseau de $\mathbb{R}^n$ pour la base $(v_1, \dots, v_n)$, alors pour $x = \sum_{k=1}^n x_k v_k$ on définit $f(x) := (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$. On a que $f(B_r(0))$ est borné pour tout $r \in \mathbb{R}_+^*$, c'est-à-dire qu'il existe $T > 0$ tel que $\|f(y)\| \leq T$ pour tout $y \in B_r(0)$. Ainsi, si $y = \sum_{k=1}^n y_k v_k \in B_r(0)$ avec $y_k \in \mathbb{Z}$, on obtient $|y_k| \leq \|(y_1, \dots, y_n)\| \leq k$ pour tout $k \in \llbracket 1, n \rrbracket$, et donc on trouve un nombre fini de solutions à $y \in \Gamma \cap B_r(0)$.

□

Définition 2.3.10 (Domaine fondamental). Pour $(v_1, \dots, v_n)$ une base de $\mathbb{R}^n$, on définit l'ensemble

$$D := \left\{ \sum_{k=1}^n a_k v_k \mid a_k \in [0, 1[\right\}.$$

On appelle cette ensemble le *domaine fondamental* de la base $(v_1, \dots, v_n)$ ou du réseau engendré par cette base.

On peut voir que ce domaine fondamental permet de construire une partition de $\mathbb{R}^n$ comme l'énonce la proposition suivante qu'on admet.

Proposition 2.3.11. *Soit $(v_1, \dots, v_n)$ une base de $\mathbb{R}^n$, Γ un réseau engendré par cette base et D le domaine fondamental de ce réseau. On a la partition suivante*

$$\mathbb{R}^n = \bigsqcup_{a \in \Gamma} D + a$$

(où $D + a$ désigne la translation de D par le vecteur a).

Définition 2.3.12 (Tore). On définit le *tore* de dimension $n \in \mathbb{N}^*$ comme le groupe produit $\mathbb{T}^n$ où $\mathbb{T}$ est le groupe du cercle.

Proposition 2.3.13. *On a un isomorphisme de groupes $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.*

Démonstration. Il suffit de prendre le revêtement $\varphi : \mathbb{R} \rightarrow \mathbb{T} : x \mapsto e^{i2\pi x}$ qui est un morphisme surjectif ayant $\mathbb{Z}$ pour noyau, on conclut donc par le premier théorème d'isomorphisme. $\square$

Proposition 2.3.14. *Soit Γ un réseau de $\mathbb{R}^n$, on a l'isomorphisme de groupes suivant : $\mathbb{R}^n/\Gamma \cong \mathbb{T}^n$.*

Démonstration. Soit $(v_1, \dots, v_n)$ la base sur laquelle Γ est engendré, alors $\phi : \mathbb{R}^n \rightarrow \mathbb{T}^n : (x_1 v_1, \dots, x_n v_n) \mapsto (e^{i2\pi x_1}, \dots, e^{i2\pi x_n})$ est un morphisme surjectif ayant Γ pour noyau, on conclut donc par le premier théorème d'isomorphisme. $\square$

Corollaire 2.3.15. *Soit Γ un réseau et D son domaine fondamental. On a que le morphisme $\phi : \mathbb{R}^n \rightarrow \mathbb{T}^n : (x_1 v_1, \dots, x_n v_n) \mapsto (e^{i2\pi x_1}, \dots, e^{i2\pi x_n})$ est une bijection si on le restreint au domaine fondamental. On note cette restriction γ .*

Démonstration. Cela suit de la partition donnée à la proposition 2.3.11. $\square$

Définition 2.3.16 (Volume). Pour $X \subset \mathbb{T}^n$, si $v(\gamma^{-1}(X))$ existe, on définit le volume de X comme $\nu(X) := v(\gamma^{-1}(X))$ où v est le volume usuel dans $\mathbb{R}^n$.

Proposition 2.3.17. *Soit Γ un réseau de $\mathbb{R}^n$, $\phi : \mathbb{R}^n \rightarrow \mathbb{T}^n : (x_1 v_1, \dots, x_n v_n) \mapsto (e^{i2\pi x_1}, \dots, e^{i2\pi x_n})$ et X un sous-ensemble borné de $\mathbb{R}^n$ tel que $v(X)$ existe. Si $\nu(\phi(X)) \neq v(X)$ alors $\phi|_X$ n'est pas injectif.*

Démonstration. Nous allons prouver la contraposée et donc supposer que $\phi|_X$ est injectif. Soit D un domaine fondamental de Γ et soit $A = \{a \in \Gamma \mid X \cap (D+a) \neq \emptyset\}$, puisque X est borné, cet ensemble est fini par la proposition 2.3.9. Pour $a \in A$, on pose $X_a = X \cap (D+a)$ et $Y_a = X_a - a$, on a alors que $Y_a \cap Y_b = \emptyset$ pour $a \neq b$. En effet, si $y \in Y_a \cap Y_b = (X_a - a) \cap (X_b - b)$, alors il existe $\alpha \in X_a$ et $\beta \in X_b$ tel que $y = \alpha - a = \beta - b$, mais alors on trouve $\phi(\alpha) = \phi(\beta)$ car $a, b \in \Gamma = \text{Ker}(\phi)$. Ce n'est pas possible car $\alpha, \beta \in X$ et $\alpha \neq \beta$ mais $\phi|_X$ est injectif. Ensuite, le volume est stable par translation dans $\mathbb{R}^n$ donc $v(X_a) = v(Y_a)$ pour $a \in A$. Aussi, remarquons $\phi(X_a) = \gamma(Y_a)$ pour $a \in A$, on conclut alors par le calcul suivant

$$\begin{aligned}
\nu(\phi(X)) &= \nu\left(\phi\left(\bigcup_{a \in A} X_a\right)\right) = \nu\left(\bigcup_{a \in A} \phi(X_a)\right) = \nu\left(\bigcup_{a \in A} \gamma(Y_a)\right) = \nu\left(\bigsqcup_{a \in A} \gamma(Y_a)\right) \\
&= \sum_{a \in A} \nu(\gamma(Y_a)) = \sum_{a \in A} \nu(\gamma^{-1}(\gamma(Y_a))) = \sum_{a \in A} \nu(Y_a) = \sum_{a \in A} \nu(X_a) = \nu(X).
\end{aligned}$$

□

Définition 2.3.18 (Symétrique). Un sous-ensemble X de $\mathbb{R}^n$ est dit *symétrique* lorsque $x \in X$ implique $-x \in X$.

Théorème 2.3.19 (Minkowski). Soit Γ un réseau engendré par une base de $\mathbb{R}^n$ ayant D comme domaine fondamental, et soit X un sous-ensemble borné symétrique convexe de $\mathbb{R}^n$. Si $v(X) > 2^n v(D)$, alors X contient un élément non nul de Γ .

Démonstration. Si on double la taille de notre réseau, il n'est pas compliqué de voir que le volume du domaine fondamental de ce nouveau réseau est $v(2D) = 2^n v(D)$. On considère alors le tore obtenu par ce nouveau réseau $\mathbf{T}^n = \mathbb{R}^n / 2\Gamma$ et on a par définition que $\nu(\mathbf{T}^n) = v(2D) = 2^n v(D)$. Soit $\phi : \mathbb{R}^n \rightarrow \mathbf{T}^n : (2x_1v_1, \dots, 2x_nv_n) \mapsto (e^{i2\pi x_1}, \dots, e^{i2\pi x_n})$, cette fonction ne préserve pas le volume de X car $\nu(\phi(X)) \leq \nu(\mathbf{T}^n) = 2^n v(D) < v(X)$. Par la proposition 2.3.17, $\pi|_X$ n'est pas injectif, il existe donc $x, y \in X$ tels que $x \neq y$ et $\pi(x) = \pi(y)$, c'est-à-dire tels que $x - y \in 2\Gamma$. Puisque X est symétrique, $-y \in X$ et puisque X est convexe, $\frac{x-y}{2} \in X$. Or $x - y \in 2\Gamma$ implique $\frac{x-y}{2} \in \Gamma$ et donc on trouve bien $0 \neq \frac{x-y}{2} \in X \cap \Gamma$. □

2.3.2 Borne de Minkowski

Définition 2.3.20. Soit $\mathbb{K}$ un corps de nombres de degré n . Un morphisme de corps $\tau : \mathbb{K} \rightarrow \mathbb{C}$ est dit *réel* si $\tau(\mathbb{K}) \subset \mathbb{R}$ et *imaginaire* sinon.

Maintenant qu'on a un outil puissant sur les réseaux de $\mathbb{R}^n$, on aimerait trouver une fonction qui permettrait de plonger un corps de nombres $\mathbb{K}$ de degré n dans $\mathbb{R}^n$ tout en envoyant les idéaux non nuls de $\mathcal{O}_{\mathbb{K}}$ dans les réseaux de $\mathbb{R}^n$. On considère l'ensemble $\text{Hom}(\mathbb{K}, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$, et puisque la conjugaison complexe est un automorphisme de $\mathbb{C}$, on a que $\overline{\sigma_k} \in \text{Hom}(\mathbb{K}, \mathbb{C})$ pour tout $k \in \llbracket 1, n \rrbracket$, et plus précisément $\overline{\sigma_k} = \sigma_k$ si et seulement si σ_k est réel. Les morphismes de corps $\mathbb{K} \rightarrow \mathbb{C}$ imaginaires viennent donc en paires. Soit s le nombre de morphismes de corps $\mathbb{K} \rightarrow \mathbb{C}$ réels et t le nombre de paires de morphismes de corps $\mathbb{K} \rightarrow \mathbb{C}$ imaginaires, on peut renommer les indices de ces morphismes pour avoir le n -uplet de morphismes $(\sigma_1, \dots, \sigma_s, \sigma_{s+1}, \overline{\sigma_{s+1}}, \dots, \sigma_{s+t}, \overline{\sigma_{s+t}})$ où les s premiers sont réels. On peut alors définir la fonction

$$\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$$

$$\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_s(\alpha), \Re(\sigma_{s+1}(\alpha)), \Im(\sigma_{s+1}(\alpha)), \dots, \Re(\sigma_{s+t}(\alpha)), \Im(\sigma_{s+t}(\alpha))).$$

Proposition 2.3.21. *Soit $\mathbb{K}$ un corps de nombres de degré $n = s + 2t$ et $\alpha = (\alpha_1, \dots, \alpha_n)$ une $\mathbb{Q}$ -base de $\mathbb{K}$. On a que $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ sont des vecteurs linéairements indépendants de $\mathbb{R}^n$.*

Démonstration. Pour $k \in \llbracket 1, n \rrbracket$, on définit

$$(\tau_1(\alpha_k), \tau_2(\alpha_k), \dots, \tau_s(\alpha_k), \tau_{s+1}(\alpha_k), \tau_{s+2}(\alpha_k), \dots, \tau_{s+2t-1}(\alpha_k), \tau_{s+2t}(\alpha_k)) := \sigma(\alpha_k)$$

et on pose $T = (\tau_i(\alpha_j))_{i,j \in \llbracket 1, n \rrbracket}$, on doit alors démontrer $\det(T) \neq 0$. En choisissant les indices correctement, on peut remarquer, par multilinéarité du déterminant, que $\det(T) = (2i)^{-t} \det((\sigma_i(\alpha_j))_{i,j \in \llbracket 1, n \rrbracket})$. Enfin, α est une $\mathbb{Q}$ -base de $\mathbb{K}$, donc d'après la proposition 2.1.45, $\det((\sigma_i(\alpha_j))_{i,j \in \llbracket 1, n \rrbracket})^2 = \Delta(\alpha) \neq 0$, ce qui conclut. $\square$

Il suit de cette proposition que σ envoie les idéaux de $\mathcal{O}_{\mathbb{K}}$ sur des réseaux de $\mathbb{R}^{s+2t}$.

Proposition 2.3.22. *Soit $(v_1, \dots, v_n)$ une base de $\mathbb{R}^n$, Γ un réseau engendré par cette base et P une matrice de changement de base. Le volume du domaine fondamental de la base $(v_1, \dots, v_n)$ est donné par $|\det(P)|^2$.*

Démonstration. La preuve peut être trouvée dans le cours LMAT1221 [18]. $\square$

Il suit de cette proposition que le volume du domaine fondamental ne dépend pas de la base choisie car les matrices de changement de base sont ici dans $\mathrm{GL}_n(\mathbb{Z})$.

Proposition 2.3.23. *Soit $\mathbb{K}$ un corps de nombres de degré $n = s + 2t$ et $0 \neq I \subseteq \mathcal{O}_{\mathbb{K}}$. Le volume du domaine fondamental de $\sigma(I)$ dans $\mathbb{R}^{s+2t}$ est donné par*

$$\frac{N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|}}{2^t}.$$

Démonstration. Soit $\alpha = (\alpha_1, \dots, \alpha_n)$ une $\mathbb{Z}$ -base de I et D le domaine fondamental de la base $(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$, alors d'après la proposition 2.3.22, on a $v(D) = |\det(T)|$ où T est défini comme dans 2.3.21. On a alors

$$\det(T) = (2i)^{-t} \det((\sigma_i(x_j))_{i,j \in \llbracket 1, n \rrbracket})$$

et donc

$$|\det(T)| = \left| \frac{\det((\sigma_i(x_j))_{i,j \in \llbracket 1, n \rrbracket})}{(2i)^t} \right| = \frac{\sqrt{|\Delta(\alpha)|}}{2^t} = \frac{N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|}}{2^t}$$

par la proposition 2.2.21. $\square$

Lemme 2.3.24. Soit Γ un réseau de $\mathbb{R}^n$ où $n = s + 2t$, et D un domaine fondamental de ce réseau de volume V . Si $a_1, \dots, a_{s+t}$ sont des nombres réels strictement positifs tels que $\prod_{k=1}^{s+t} a_k > \left(\frac{4}{\pi}\right)^t V$ alors il existe $0 \neq (x_1, \dots, x_s, x_{s+1}, x'_{s+1}, \dots, x_{s+t}, x'_{s+t}) \in \Gamma$ tel que $|x_k| < a_k$ pour tout $k \in \llbracket 1, s \rrbracket$ et $x_k^2 + x_k'^2 < a_k$ pour tout $k \in \llbracket s+1, s+t \rrbracket$.

Démonstration. Soit X l'ensemble des points de $\mathbb{R}^{s+2t}$ qui satisfont la conclusion, on a alors $v(X)$ qui vaut

$$\begin{aligned} & \int_{-a_1}^{a_1} dx_1 \times \dots \times \int_{-a_s}^{a_s} dx_s \times \iint_{x_{s+1}^2 + x_{s+1}'^2 < a_{s+1}} dx_{s+1} dx'_{s+1} \times \dots \times \iint_{x_{s+t}^2 + x_{s+t}'^2 < a_{s+t}} dx_{s+t} dx'_{s+t} \\ &= 2a_1 \times 2a_2 \times \dots \times 2a_s \times \pi a_{s+1} \times \pi a_{s+2} \times \dots \times \pi a_{s+t} = 2^s \pi^t \prod_{k=1}^{s+t} a_k. \end{aligned}$$

On a que X est borné, symétrique et convexe puisque c'est le produit cartésien de segments et de disques centrés en l'origine. On peut donc appliquer le théorème de Minkowski 2.3.19 pour conclure car

$$v(X) > 2^{s+2t} V \iff 2^s \pi^t \prod_{k=1}^{s+t} a_k > 2^{s+2t} V \iff \prod_{k=1}^{s+t} a_k > \left(\frac{4}{\pi}\right)^t V.$$

$\square$

Proposition 2.3.25. Soit $\mathbb{K}$ un corps de nombres de degré $n = s + 2t$ et $0 \neq I \subseteq \mathcal{O}_{\mathbb{K}}$. Il existe $a \in I$ non nul tel que

$$|N_{\mathbb{K}}(a)| \leq \left(\frac{2}{\pi}\right)^t N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|}.$$

Démonstration. Soit $\varepsilon > 0$, il existe $a_1, \dots, a_{s+t} > 0$ tels que

$$\prod_{k=1}^{s+t} a_k = \left(\frac{2}{\pi}\right)^t N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|} + \varepsilon.$$

Par la proposition 2.3.21, on a que $\sigma(I)$ est un réseau de $\mathbb{R}^{s+2t}$, et il a un domaine fondamental de volume $V = \frac{N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|}}{2^t}$ d'après la proposition 2.3.23. On obtient alors

$$\prod_{k=1}^{s+t} a_k = \left(\frac{2}{\pi}\right)^t 2^t V + \varepsilon = \left(\frac{4}{\pi}\right)^t V + \varepsilon \implies \prod_{k=1}^{s+t} a_k > \left(\frac{4}{\pi}\right)^t V.$$

D'après le lemme 2.3.24, il existe $\alpha \in I$ non nul tel que

$\sigma(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_s(\alpha), \Re(\sigma_{s+1}(\alpha)), \Im(\sigma_{s+1}(\alpha)), \dots, \Re(\sigma_{s+t}(\alpha)), \Im(\sigma_{s+t}(\alpha)))$ satisfait

$|\sigma_k(\alpha)| < a_k$ pour $k \in \llbracket 1, s \rrbracket$ et $|\sigma_k(\alpha)|^2 < a_k$ pour $k \in \llbracket s+1, s+t \rrbracket$. On multiplie toutes ces inégalités pour obtenir

$$\begin{aligned} |N_{\mathbb{K}}(\alpha)| &= \left| \prod_{\sigma \in \text{Hom}(\mathbb{K}, \mathbb{C})} \sigma(\alpha) \right| = \prod_{\sigma \in \text{Hom}(\mathbb{K}, \mathbb{C})} |\sigma(\alpha)| \\ &= |\sigma_1(\alpha)| \cdot |\sigma_2(\alpha)| \cdots |\sigma_s(\alpha)| \cdot |\sigma_{s+1}(\alpha)|^2 \cdot |\sigma_{s+2}(\alpha)|^2 \cdots |\sigma_{s+t}(\alpha)|^2 \\ &< a_1 \cdot a_2 \cdots a_{s+t} = \left(\frac{2}{\pi}\right)^t N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|} + \varepsilon. \end{aligned}$$

Posons

$$A_\varepsilon = \{b \in \mathbb{R}^n \mid \exists \beta \in I \setminus \{0\} ; N_{\mathbb{K}}(\beta) < \left(\frac{2}{\pi}\right)^t N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|} + \varepsilon \wedge \sigma(\beta) = b\}.$$

Puisque un réseau est discret d'après la proposition 2.3.9, A_ε est fini, et il est non vide car $\alpha \in A_\varepsilon$. Remarquons que si $\varepsilon < \varepsilon'$, alors $A_\varepsilon \subset A_{\varepsilon'}$, on obtient alors une chaîne d'ensembles non vides indexée par $\varepsilon \in \mathbb{R}_+^*$. Il en suit que

$$A = \bigcap_{\varepsilon \in \mathbb{R}_+^*} A_\varepsilon \neq \emptyset.$$

Ainsi, on peut prendre $a \in A$ et conclure. □

Corollaire 2.3.26. *Soit $\mathbb{K}$ un corps de nombres de degré $n = s + 2t$. Tout idéal non nul $I \trianglelefteq \mathcal{O}_{\mathbb{K}}$ est équivalent à un idéal de norme inférieure ou égale à $\left(\frac{2}{\pi}\right)^t \sqrt{|\Delta_{\mathbb{K}}|}$.*

Démonstration. Il existe un idéal entier J de $\mathcal{O}_{\mathbb{K}}$ équivalent à l'idéal fractionnaire I^{-1} , on a alors $IJ \sim \mathcal{O}_{\mathbb{K}}$. D'après la proposition 2.3.25, il existe un entier $a \in J$ tel que $|N_{\mathbb{K}}(a)| \leq \left(\frac{2}{\pi}\right)^t N_{\mathbb{K}}(J) \sqrt{|\Delta_{\mathbb{K}}|}$. Puisque $a \in J$, on a que $a\mathcal{O}_{\mathbb{K}} \subset J$ et donc J divise $a\mathcal{O}_{\mathbb{K}}$ d'après la proposition 2.2.10. Soit $H \trianglelefteq \mathcal{O}_{\mathbb{K}}$ tel que $JH = a\mathcal{O}_{\mathbb{K}}$, alors $H \sim J^{-1} \sim (I^{-1})^{-1} \sim I$. Par multiplicativité de la norme (proposition 2.2.19), on obtient $N_{\mathbb{K}}(J)N_{\mathbb{K}}(H) = N_{\mathbb{K}}(JH) = N_{\mathbb{K}}(a\mathcal{O}_{\mathbb{K}}) = |N_{\mathbb{K}}(a)|$ par le corollaire 2.2.22. Finalement,

$$|N_{\mathbb{K}}(a)| \leq \left(\frac{2}{\pi}\right)^t N_{\mathbb{K}}(J) \sqrt{|\Delta_{\mathbb{K}}|} \iff N_{\mathbb{K}}(J)N_{\mathbb{K}}(H) \leq \left(\frac{2}{\pi}\right)^t N_{\mathbb{K}}(J) \sqrt{|\Delta_{\mathbb{K}}|} \quad (2.6)$$

$$\iff N_{\mathbb{K}}(H) \leq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta_{\mathbb{K}}|}. \quad (2.7)$$

□

Proposition 2.3.27. *Le groupe de Picard d'un corps de nombres est fini.*

Démonstration. C'est une conséquence du corollaire 2.3.26 et de la proposition 2.2.24. $\square$

On rappelle la célèbre inégalité suivante, qu'on admet.

Proposition 2.3.28 (Inégalité arithmético-géométrique). *Étant donné un vecteur de nombres positifs $(x_1, \dots, x_n) \in (\mathbb{R}^+)^n$, on a l'inégalité suivante*

$$\sqrt[n]{x_1 \cdots x_n} \leq \frac{x_1 + \cdots + x_n}{n}.$$

Lemme 2.3.29. *Soit $\delta > 0$, l'ensemble des points $(x_1, x_2, \dots, x_s, x_{s+1}, x'_{s+1}, \dots, x_{s+t}, x'_{s+t}) \in \mathbb{R}^{s+2t}$ satisfaisant*

$$|x_1| + |x_2| + \cdots + |x_s| + 2\sqrt{x_{s+1}^2 + x_{s+1}'^2} + \cdots + 2\sqrt{x_{s+t}^2 + x_{s+t}'^2} < \delta$$

qu'on note X_δ a pour volume

$$2^s \left(\frac{\pi}{2}\right)^t \frac{\delta^n}{n!},$$

où $n = s + 2t$.

Démonstration. Appelons le volume de cet ensemble $V(s, t, \delta)$ et procédons par double récurrence sur s et t .

- Initialisation : on a que $V(1, 0, \delta) = 2\delta$ car c'est le volume de $]-\delta, \delta[$, et $V(0, 1, \delta) = \frac{\pi}{4}\delta^2$ car c'est le volume d'un disque de rayon $\frac{\delta}{2}$.
- Hérité : fixons premièrement t et supposons que $V(s, t, \delta) = 2^s \left(\frac{\pi}{2}\right)^t \frac{\delta^{s+2t}}{(s+2t)!}$ pour un certain $s \in \mathbb{N}$, montrons alors que $V(s+1, t, \delta) = 2^{s+1} \left(\frac{\pi}{2}\right)^t \frac{\delta^{s+1+2t}}{(s+1+2t)!}$. On a

$$V(s+1, t, \delta) = \int_{\mathbb{R}} V(s, t, \delta - |x|) dx = \int_{-\delta}^{\delta} V(s, t, \delta - |x|) dx,$$

l'hypothèse de récurrence nous donne alors

$$V(s+1, t, \delta) = 2 \int_0^{\delta} 2^s \left(\frac{\pi}{2}\right)^t \frac{(\delta - x)^{s+2t}}{(s+2t)!} dx = 2^{s+1} \left(\frac{\pi}{2}\right)^t \frac{\delta^{s+1+2t}}{(s+1+2t)!}.$$

Maintenant, fixons s et supposons que $V(s, t, \delta) = 2^s \left(\frac{\pi}{2}\right)^t \frac{\delta^{s+2t}}{(s+2t)!}$ pour un certain

$t \in \mathbb{N}$, montrons alors que $V(s, t+1, \delta) = 2^s \left(\frac{\pi}{2}\right)^{t+1} \frac{\delta^{s+2t+2}}{(s+2t+2)!}$. On a

$$\begin{aligned} V(s, t+1, \delta) &= \iint_{\mathbb{R}^2} V(s, t, \delta - 2\sqrt{x^2 + x'^2}) dx dx' \\ &= \iint_{\sqrt{x^2 + x'^2} \leq \frac{\delta}{2}} V(s, t, \delta - 2\sqrt{x^2 + x'^2}) dx dx'. \end{aligned}$$

On effectue alors le changement de variables $(x, x') = \rho e^{i\theta}$ avec $\rho \in \mathbb{R}^+$ et $\theta \in [0, 2\pi]$, et on obtient par l'hypothèse de récurrence

$$\begin{aligned} V(s, t+1, \delta) &= \int_0^{\frac{\delta}{2}} \int_0^{2\pi} 2^s \left(\frac{\pi}{2}\right)^t \frac{(\delta - 2\rho)^{s+2t}}{(s+2t)!} \rho d\theta \\ &= 2^s \left(\frac{\pi}{2}\right)^t \frac{2\pi}{(s+2t)!} \int_0^{\frac{\delta}{2}} (\delta - 2\rho)^{s+2t} \rho d\rho. \end{aligned}$$

En faisant le changement de variable $\rho = \frac{y}{2}$, on obtient en intégrant par parties

$$\int_0^{\frac{\delta}{2}} (\delta - 2\rho)^{s+2t} \rho d\rho = \frac{\delta^{s+2t+2}}{4(s+2t+1)(s+2t+2)}.$$

On conclut bien que

$$V(s, t+1, \delta) = 2^s \left(\frac{\pi}{2}\right)^{t+1} \frac{\delta^{s+2t+2}}{(s+2t+2)!}.$$

□

Théorème 2.3.30. Soit $\mathbb{K}$ un corps de nombres de degré $n = s + 2t$. Tout idéal non nul $I \subseteq \mathcal{O}_{\mathbb{K}}$ contient un élément $a \neq 0$ tel que

$$|N_{\mathbb{K}}(a)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|} N_{\mathbb{K}}(I).$$

Démonstration. Soit $\delta > 0$ et X_{δ} définit comme dans le lemme 2.3.29, et D un domaine fondamental pour le réseau $\sigma(I)$. Pour $\alpha \in I \subseteq \mathcal{O}_{\mathbb{K}}$ non nul, on obtient grâce à l'inégalité arithmético-géométrique 2.3.28 une majoration de $|N_{\mathbb{K}}(\alpha)|$:

$$\begin{aligned} &|\sigma_1(\alpha)| \cdot |\sigma_2(\alpha)| \cdots |\sigma_s(\alpha)| \cdot |\sigma_{s+1}(\alpha)| \cdot |\overline{\sigma_{s+1}(\alpha)}| \cdot |\sigma_{s+2}(\alpha)| \cdot |\overline{\sigma_{s+2}(\alpha)}| \cdots |\sigma_{s+t}(\alpha)| \cdot |\overline{\sigma_{s+t}(\alpha)}| \\ &\leq \\ &\frac{(|\sigma_1(\alpha)| + \cdots + |\sigma_s(\alpha)| + 2\sqrt{\Re(\sigma_{s+1}(\alpha))^2 + \Im(\sigma_{s+1}(\alpha))^2} + \cdots + 2\sqrt{\Re(\sigma_{s+t}(\alpha))^2 + \Im(\sigma_{s+t}(\alpha))^2})^n}{n^n}. \end{aligned}$$

Ainsi, si $\sigma(\alpha) \in X_\delta$, alors $|N_{\mathbb{K}}(\alpha)| \leq \frac{\delta^n}{n^n}$, d'après la définition de X_δ donnée dans le lemme 2.3.29. Puisque X_δ est un ensemble borné symétrique convexe, on a par le théorème de Minkowski 2.3.19 qu'il existe un $\alpha \in I$ non nul tel que $\sigma(\alpha) \in X_\delta$ si $v(X_\delta) > 2^n v(D)$. Par le lemme 2.3.29, on a que $v(X_\delta) = 2^s \left(\frac{\pi}{2}\right)^t \frac{1}{n!} \delta^n$, et par la proposition 2.3.23, on a que $v(D) = \frac{N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|}}{2^t}$. On trouve alors

$$v(X_\delta) > 2^n v(D) \iff 2^s \left(\frac{\pi}{2}\right)^t \frac{1}{n!} \delta^n > 2^{s+2t} \frac{N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|}}{2^t} \iff \delta^n > \left(\frac{4}{\pi}\right)^t n! N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|}.$$

Posons $A = \{\delta \in \mathbb{R}_+^* \mid \delta^n > \left(\frac{4}{\pi}\right)^t n! N_{\mathbb{K}}(I) \sqrt{|\Delta_{\mathbb{K}}|}\}$, le théorème de Minkowski 2.3.19 nous donne donc un $\alpha \in I$ non nul tel que $|N_{\mathbb{K}}(\alpha)| \leq \frac{\varepsilon^n}{n^n}$ pour tout $\varepsilon \in A$. Posons alors

$$B_\varepsilon = \{b \in \mathbb{R}^n \mid \exists \alpha \in I \setminus \{0\} ; |N_{\mathbb{K}}(\alpha)| \leq \frac{\varepsilon^n}{n^n} \wedge \sigma(\alpha) = b\}.$$

Puisque un réseau est discret par la proposition 2.3.9, l'ensemble B_ε est fini. Remarquons que si $\varepsilon < \varepsilon'$, alors $B_\varepsilon \subset B_{\varepsilon'}$, on obtient alors une chaîne d'ensembles finis non vide indexée par $\varepsilon \in A$. Il en suit que $B = \bigcap_{\varepsilon \in A} B_\varepsilon \neq \emptyset$. On peut alors choisir $\alpha \in I$ tel que $\sigma(\alpha) \in B$ pour obtenir

$$|N_{\mathbb{K}}(\alpha)| \leq \frac{\delta^n}{n^n}$$

pour tout $\delta \in A$. Finalement, on conclut que pour un tel α , on a

$$|N_{\mathbb{K}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|} N_{\mathbb{K}}(I).$$

□

Corollaire 2.3.31. *Soit $\mathbb{K}$ un corps de nombres de degré $n = s + 2t$. Toute classe d'idéaux fractionnaire de $\mathcal{O}_{\mathbb{K}}$ contient un idéal entier H tel que*

$$N_{\mathbb{K}}(H) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|}.$$

Démonstration. Soit I un idéal fractionnaire, il existe un idéal entier J de $\mathcal{O}_{\mathbb{K}}$ équivalent à l'idéal fractionnaire I^{-1} , on a alors $IJ \sim \mathcal{O}_{\mathbb{K}}$. D'après la proposition 2.3.30, il existe un entier $a \in J$ tel que $|N_{\mathbb{K}}(a)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|} N_{\mathbb{K}}(J)$. Puisque $a \in J$, on a que $a\mathcal{O}_{\mathbb{K}} \subset J$ et donc J divise $a\mathcal{O}_{\mathbb{K}}$ d'après la proposition 2.2.10. Soit $H \leq \mathcal{O}_{\mathbb{K}}$ tel que $JH = a\mathcal{O}_{\mathbb{K}}$, alors $H \sim J^{-1} \sim (I^{-1})^{-1} \sim I$. Par multiplicativité de la norme (2.2.19), on obtient $N_{\mathbb{K}}(J)N_{\mathbb{K}}(H) = N_{\mathbb{K}}(JH) = N_{\mathbb{K}}(a\mathcal{O}_{\mathbb{K}}) = |N_{\mathbb{K}}(a)|$ par la proposition 2.2.22. Finalement,

$$\begin{aligned}
|N_{\mathbb{K}}(a)| &\leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|} N_{\mathbb{K}}(J) \\
\iff N_{\mathbb{K}}(J) N_{\mathbb{K}}(H) &\leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|} N_{\mathbb{K}}(J) \\
\iff N_{\mathbb{K}}(H) &\leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|}.
\end{aligned}$$

□

Définition 2.3.32 (Borne de Minkowski). Soit $\mathbb{K}$ un corps de nombres de degré $n = s + 2t$. La *borne de Minkowski* de $\mathbb{K}$ est définie comme

$$\mu_{\mathbb{K}} = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|}.$$

Proposition 2.3.33. Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique avec d sans facteurs carrés.

1. Si $d > 0$ et $d \equiv 2, 3 \pmod{4}$ alors $\mu_{\mathbb{Q}(\sqrt{d})} = \sqrt{d}$.
2. Si $d > 0$ et $d \equiv 1 \pmod{4}$ alors $\mu_{\mathbb{Q}(\sqrt{d})} = \frac{\sqrt{d}}{2}$.
3. Si $d < 0$ et $d \equiv 2, 3 \pmod{4}$ alors $\mu_{\mathbb{Q}(\sqrt{d})} = \frac{4}{\pi} \sqrt{-d}$.
4. Si $d < 0$ et $d \equiv 1 \pmod{4}$ alors $\mu_{\mathbb{Q}(\sqrt{d})} = \frac{2}{\pi} \sqrt{-d}$.

Démonstration. On rappelle que le degré d'un corps quadratique est 2.

1. Si $d > 0$, alors $t = 0$, et d'après la proposition 2.1.56, on a $\Delta_{\mathbb{Q}(\sqrt{d})} = 4d$ car $d \equiv 2, 3 \pmod{4}$. On trouve alors

$$\mu_{\mathbb{Q}(\sqrt{d})} = \left(\frac{4}{\pi}\right)^0 \frac{2!}{2^2} \sqrt{4d} = \frac{1}{2} 2\sqrt{d} = \sqrt{d}.$$

2. On a ici aussi que $t = 0$ mais par contre, d'après la proposition 2.1.56, $\Delta_{\mathbb{Q}(\sqrt{d})} = d$ puisque $d \equiv 1 \pmod{4}$. On trouve alors

$$\mu_{\mathbb{Q}(\sqrt{d})} = \left(\frac{4}{\pi}\right)^0 \frac{2!}{2^2} \sqrt{d} = \frac{\sqrt{d}}{2}.$$

3. Si $d < 0$, alors $t = 1$, et d'après la proposition 2.1.56, on a $\Delta_{\mathbb{Q}(\sqrt{d})} = 4d$ car $d \equiv 2, 3 \pmod{4}$. On trouve alors

$$\mu_{\mathbb{Q}(\sqrt{d})} = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2} \sqrt{-4d} = \frac{4}{\pi} \frac{1}{2} 2\sqrt{-d} = \frac{4}{\pi} \sqrt{-d}.$$

4. On a ici aussi que $t = 1$ mais par contre, d'après la proposition 2.1.56, $\Delta_{\mathbb{Q}(\sqrt{d})} = d$ puisque $d \equiv 1 \pmod{4}$. On trouve alors

$$\mu_{\mathbb{Q}(\sqrt{d})} = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2} \sqrt{-d} = \frac{4}{\pi} \frac{1}{2} \sqrt{-d} = \frac{2}{\pi} \sqrt{-d}.$$

□

Proposition 2.3.34. *Soit p un nombre premier impair, notons $\zeta = e^{i\frac{2\pi}{p}}$, on a que*

$$\mu_{\mathbb{Q}(\zeta)} = \left(\frac{4}{\pi}\right)^{\frac{p-1}{2}} \frac{(p-1)!}{(p-1)^{p-1}} \sqrt{p^{p-2}}.$$

Démonstration. Le degré de $\mathbb{Q}(\zeta)$ est $p-1$, et pour tout $\sigma \in \text{Hom}(\mathbb{Q}(\zeta), \mathbb{C})$, on a que $\sigma(\zeta) = \zeta^k \notin \mathbb{R}$ pour un certain $k \in \llbracket 1, p-1 \rrbracket$. On en déduit qu'il n'y a aucun morphisme de corps réels $\mathbb{Q}(\zeta) \rightarrow \mathbb{C}$ et donc $0 \times s + 2t = p-1$. D'après la proposition 2.1.57, le discriminant de $\mathbb{Q}(\zeta)$ vaut p^{p-2} , on trouve donc le résultat escompté. □

Proposition 2.3.35. *Soit $\mathbb{K}$ un corps de nombres de degré $n = s + 2t$. Si pour tout nombre premier rationnel positif p tel que $p \leq \mu_{\mathbb{K}}$, les idéaux premiers divisant $p\mathcal{O}_{\mathbb{K}}$ sont principaux, alors $\mathcal{O}_{\mathbb{K}}$ est principal.*

Démonstration. Soit $I \trianglelefteq \mathcal{O}_{\mathbb{K}}$ non nul, par le corollaire 2.3.31, il existe $J \trianglelefteq \mathcal{O}_{\mathbb{K}}$ un idéal équivalent à I tel que $N_{\mathbb{K}}(J) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|}$. Supposons par l'absurde que J n'est pas principal, alors en particulier $J \neq \mathcal{O}_{\mathbb{K}}$ et donc $N_{\mathbb{K}}(J) > 1$. Soit $N_{\mathbb{K}}(J) = p_1 \cdots p_k$ la décomposition en facteurs premiers qu'on obtient grâce au théorème fondamental de l'arithmétique, on a alors que $p_j \leq N_{\mathbb{K}}(J) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|}$ pour tout $j \in \llbracket 1, k \rrbracket$. L'hypothèse nous dit que les idéaux premiers qui divisent les $p_j \mathcal{O}_{\mathbb{K}}$ sont principaux. Aussi, par la proposition 2.2.23, on a $N_{\mathbb{K}}(I) \in I$, ce qui peut être reformulé comme I divise $N_{\mathbb{K}}(I)\mathcal{O}_{\mathbb{K}}$ d'après la proposition 2.2.10. Finalement, on obtient par le théorème 2.2.11 que I est le produit d'idéaux principaux et est donc lui-même principal. □

Corollaire 2.3.36. *Soit $\mathbb{K}$ un corps de nombres de degré $n = s + 2t$. Si*

$$\left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta_{\mathbb{K}}|} < 2,$$

alors $\mathcal{O}_{\mathbb{K}}$ est principal.

On a maintenant les outils nécessaires pour calculer des groupes de Picard.

Exemple 2.3.37. 1. D'après la proposition 2.3.33, on a que les bornes de Minkowski de $\mathbb{Q}(\sqrt{d})$ pour $d \in \{-1, \pm 2, \pm 3, 5, -7, 13\}$ sont strictement inférieures à 2. D'après 2.3.36, leur groupe de Picard est trivial.

2. D'après la proposition 2.3.33, on a que les bornes de Minkowski de $\mathbb{Q}(\sqrt{6})$ et $\mathbb{Q}(\sqrt{7})$ valent respectivement $\sqrt{6} \simeq 2,45$ et $\sqrt{7} \simeq 2,65$. D'après la proposition 2.3.35 et le calcul fait dans le deuxième et quatrième exemple de 2.2.29, leur groupe de Picard est trivial.
3. D'après la proposition 2.3.33, on a que la borne de Minkowski de $\mathbb{Q}(\sqrt{-5})$ vaut $\frac{4}{\pi}\sqrt{5} \simeq 2,85$. Or, le premier exemple de 2.2.29 nous dit que $2\mathbb{Z}[\sqrt{-5}] = (2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}])^2$ et que $2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ n'est pas principal. Il en suit que le groupe de Picard de $\mathbb{Q}(\sqrt{-5})$ est d'ordre 2 par le corollaire 2.3.31, et la classe $[2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]]$ est l'élément non neutre du groupe.
4. D'après la proposition 2.3.33, on a que la borne de Minkowski de $\mathbb{Q}(\sqrt{-6})$ vaut $\frac{4}{\pi}\sqrt{6} \simeq 3,12$. Le troisième exemple de 2.2.29 nous dit que $2\mathbb{Z}[\sqrt{-6}] = (2\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}])^2$ et $3\mathbb{Z}[\sqrt{-6}] = (3\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}])^2$, le groupe de Picard est donc engendré par $[2\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}]]$ et $[3\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}]]$ par le corollaire 2.3.31. Montrons que ces deux idéaux sont dans la même classe. Puisque $[3\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}]]$ est d'ordre 2, c'est son propre inverse, il suffit alors de montrer que $(2\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}])(3\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}])$ est principal. On a

$$\begin{aligned}
& (2\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}])(3\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}]) \\
&= 6\mathbb{Z}[\sqrt{-6}] + 2\sqrt{-6}\mathbb{Z}[\sqrt{-6}] + 3\sqrt{-6}\mathbb{Z}[\sqrt{-6}] - 6\mathbb{Z}[\sqrt{-6}] \\
&= 2\sqrt{-6}\mathbb{Z}[\sqrt{-6}] + 3\sqrt{-6}\mathbb{Z}[\sqrt{-6}] - 6\mathbb{Z}[\sqrt{-6}] \\
&= \sqrt{-6}(2\mathbb{Z}[\sqrt{-6}] + 3\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}]) = \sqrt{-6}\mathbb{Z}[\sqrt{-6}].
\end{aligned}$$

La dernière égalité vient du fait que $2, 3 \in 2\mathbb{Z}[\sqrt{-6}] + 3\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}]$, on a donc pu appliquer la proposition 2.1.35. Finalement, comme pour le point précédent, le groupe de Picard de $\mathbb{Q}(\sqrt{-6})$ est d'ordre 2 et $[2\mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\mathbb{Z}[\sqrt{-6}]]$ est l'élément non neutre du groupe.

2.4 Ordre d'un corps de nombres et conducteur

On va s'intéresser dans cette section à des anneaux plus généraux que les anneaux d'entiers d'un corps de nombres, appelés ordres. Contrairement à l'anneau des entiers, ses classes d'idéaux fractionnaires ne sont pas toutes inversibles, ce qui va rajouter de la difficulté dans les calculs. On s'en sort malgré tout dans le cas quadratique.

2.4.1 Groupe de Picard d'un ordre

Définition 2.4.1 (Ordre). Pour $\mathbb{K}$ un corps de nombres de degré n , un *ordre* de $\mathbb{K}$ est un sous-anneau de $\mathcal{O}_{\mathbb{K}}$ ayant une $\mathbb{Z}$ -base de taille n . Un *ordre quadratique* est un ordre d'un corps quadratique.

Pour $\mathcal{O}$ un ordre d'un corps de nombres $\mathbb{K}$, il suit de cette définition que $\mathbb{K}$ est le corps de fractions de $\mathcal{O}$ et donc $\mathcal{O}_{\mathbb{K}}$ est la fermeture intégrale de $\mathcal{O}$. Ainsi, $\mathcal{O}_{\mathbb{K}}$ est l'unique ordre de $\mathbb{K}$ à être un anneau de Dedekind car c'est le seul à être intégralement clos. Pour autant, les deux propositions suivantes montrent qu'être intégralement clos est l'unique propriété qui peut manquer à un ordre pour être de Dedekind.

Proposition 2.4.2. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. Tout idéal non nul de $\mathcal{O}$ est d'indice fini.*

Démonstration. Soit $I \trianglelefteq \mathcal{O}$ non nul, il existe $\alpha \in I$ non nul. On va d'abord montrer qu'il existe $b \in I \cap \mathbb{Z}^*$. Puisque $\alpha \in I \subset \mathcal{O} \subset \mathcal{O}_{\mathbb{K}}$, α admet une équation de dépendance intégrale sur $\mathbb{Z}$. Il existe donc $b_0, b_1, \dots, b_{m-1} \in \mathbb{Z}$ tels que

$$\alpha^m + b_{m-1}\alpha^{m-1} + b_{m-2}\alpha^{m-2} + \dots + b_1\alpha + b_0 = 0.$$

Ce qui peut se réécrire comme

$$b_0 = -\alpha(\alpha^{m-1} + b_{m-1}\alpha^{m-2} + b_{m-2}\alpha^{m-3} + \dots + b_2\alpha + b_1).$$

Étant donné que $\alpha \in I$, les propriétés d'idéaux impliquent que $b_0 \in I$. En outre, on trouve que $b_0\mathcal{O} \subset I \subset \mathcal{O}$ mais $b_0\mathcal{O}$ est de même rang que $\mathcal{O}$ et donc I est aussi de même rang que $\mathcal{O}$. On en conclut que $[\mathcal{O} : I]$ est fini. $\square$

Proposition 2.4.3. *Tout ordre d'un corps de nombres est un anneau noethérien et tous ses idéaux premiers non nuls sont maximaux.*

Démonstration. Par définition, un ordre d'un corps de nombres est un groupe abélien de type fini, on peut donc utiliser les mêmes arguments que pour $\mathcal{O}_{\mathbb{K}}$ dans la proposition 2.2.16 pour dire que tout ordre d'un corps de nombres est noethérien. De même, on peut imiter la preuve de la proposition 2.2.16 pour montrer que tout idéal premier non nul est maximal, car la proposition 2.4.2 nous dit que les idéaux non nuls d'un ordre d'un corps de nombres sont d'indice fini. $\square$

Définition 2.4.4 (Monoïde des classes d'idéaux). Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. On définit de façon similaire au groupe de Picard de $\mathbb{K}$, le *monoïde des classes d'idéaux* de $\mathcal{O}$ comme

$$\mathrm{ICM}(\mathcal{O}) := \mathcal{I}_{\mathcal{O}} / \mathcal{P}_{\mathcal{O}}.$$

On parle bien ici uniquement de monoïde, car la proposition 2.4.17 nous dira que ce n'est jamais un groupe lorsque $\mathcal{O} \neq \mathcal{O}_{\mathbb{K}}$. La classe d'équivalence correspondante est similaire à ce qu'on a déjà vu : I et J sont équivalents si et seulement s'il existe $d \in \mathbb{K}^*$ tel que $I = dJ$. On a une autre caractérisation de cette équivalence donnée par la proposition suivante.

Proposition 2.4.5. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. On a que deux idéaux fractionnaires de $\mathcal{O}$ sont équivalents si et seulement s'ils sont isomorphes en tant que $\mathcal{O}$ -modules.*

Démonstration. Soient I et J deux idéaux fractionnaires de $\mathcal{O}$, supposons d'abord qu'ils sont équivalents. Il existe donc $d \in \mathbb{K}^*$ tel que $I = dJ$, et ainsi, on peut définir le morphisme de $\mathcal{O}$ -modules $m : J \rightarrow I : x \mapsto dx$, qui est surjectif par hypothèse. L'injectivité suit du fait que J est un sous-ensemble de $\mathbb{K}$ qui est un corps et que $d \neq 0$.

Réciproquement, supposons qu'il existe un isomorphisme de $\mathcal{O}$ -modules $\varphi : J \rightarrow I$. Prenons $s \in J \setminus \{0\}$, on a que $\frac{\varphi(s)}{s} \in \mathbb{K}^*$, montrons alors que $I = \frac{\varphi(s)}{s}J$. Soit $y \in I$, puisque φ est surjectif, il existe $x \in J$ tel que $y = \varphi(x)$. Remarquons que $\frac{x}{s} \in \mathbb{K}$, il existe donc $a \in \mathcal{O}$ et $b \in \mathcal{O}^*$ tel que $\frac{x}{s} = \frac{a}{b}$, puisque $\mathbb{K}$ est le corps des fractions de $\mathcal{O}$. Cette dernière égalité peut se réécrire comme $bx = as$, et puisque $as \in J$ par propriété de $\mathcal{O}$ -module, on peut appliquer l'isomorphisme φ . On trouve alors $b\varphi(x) = a\varphi(s)$ et donc $y = \varphi(x) = \frac{a}{b}\varphi(s) = \frac{\varphi(s)}{s}x$, ce qui conclut. $\square$

Définition 2.4.6. Soit $\mathbb{A}$ un anneau intègre et $\mathbb{K}$ son corps de fractions. Pour I, J deux idéaux fractionnaires, on définit l'idéal fractionnaire

$$(I : J) = \{x \in \mathbb{K} \mid xJ \subset I\}.$$

Cela définit bien un idéal fractionnaire. Si $x, y \in (I : J)$ et $a \in \mathbb{A}$ alors pour tout $z \in J$, $xz, yz \in I$ et donc $(x + y)z \in I$. Aussi, $az \in J$ donc $axz = xaz \in I$, on a donc que $(I : J)$ est bien un sous- $\mathbb{A}$ -module de $\mathbb{K}$. Ensuite, on a $dI \subset \mathbb{A}$ et $d'J \subset \mathbb{A}$ pour certains $d, d' \in \mathbb{A}^*$, et puisque J est non nul, il existe $j \in J$ non nul. On trouve alors $d'j \in J \cap \mathbb{A}^*$ et $dd'j(I : J) \subset \mathbb{A}$. En effet, soit $x \in (I : J)$, on a $d'jx \in I$ car $d'j \in J$, et donc $dd'jx \in \mathbb{A}$.

Proposition 2.4.7. *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et I un idéal fractionnaire de $\mathcal{O}$. On a que $(I : I)$ est un sous-anneau de $\mathcal{O}_{\mathbb{K}}$ contenant $\mathcal{O}$. En particulier, I est aussi un idéal fractionnaire de $(I : I)$.*

Démonstration. Pour $x \in \mathcal{O}$, les propriétés de modules nous donnent que $xI \subset I$ et donc $\mathcal{O} \subset (I : I)$. Ensuite, étant donné $y, z \in (I : I)$, on a que $yI \subset I$ et $zI \subset I$ et donc $yzI \subset yI \subset I$. Aussi, $1 \cdot I \subset I$ donc $1 \in (I : I)$. C'est donc bien un anneau. Enfin, si $x \in (I : I)$, alors $x \in \mathbb{K}$, en vue de la proposition 2.1.16, on doit montrer que x est un entier algébrique. D'après la proposition 2.1.4, il faut montrer que $\mathbb{Z}[x]$ est un $\mathbb{Z}$ -module de type fini. Puisque $xI \subset I$, on a que $x^k I \subset I$ pour tout $k \in \mathbb{N}$. Prenons alors $a \in I$ non nul, on a $ax^k \in I$ pour tout $k \in \mathbb{N}$ et donc $a\mathbb{Z}[x] \subset I$. Il en suit que $a\mathbb{Z}[x]$ est un $\mathbb{Z}$ -module de type fini, on peut alors conclure car $a\mathbb{Z}[x] \cong \mathbb{Z}[x]$. $\square$

On appelle $(I : I)$ l'anneau des multiplicateurs de I .

Corollaire 2.4.8. *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et I un idéal fractionnaire de $\mathcal{O}$. On a que l'anneau des multiplicateurs de I est un ordre de $\mathbb{K}$.*

Démonstration. D'après la proposition 2.4.7, on a $\mathcal{O} \subset (I : I) \subset \mathcal{O}_{\mathbb{K}}$. Il en suit que le rang de $(I : I)$ est égal à celui de $\mathcal{O}$ (et de $\mathcal{O}_{\mathbb{K}}$), c'est donc bien un ordre de $\mathbb{K}$. $\square$

Proposition 2.4.9. *L'anneau des multiplicateurs est un invariant de classes d'idéaux fractionnaires.*

Démonstration. Soient I, J deux idéaux fractionnaires d'un ordre $\mathcal{O}$ qui sont équivalents, cela veut dire qu'il existe $d \in \mathbb{K}^*$ tel que $I = dJ$, on trouve alors

$$(I : I) = (dJ : dJ) = d(J : dJ) = d \frac{1}{d} (J : J) = (J : J).$$

$\square$

Définition 2.4.10 (Conducteur). Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. On définit le *conducteur* de $\mathcal{O}$ comme

$$\mathfrak{f} := (\mathcal{O} : \mathcal{O}_{\mathbb{K}}).$$

Puisque $1 \in \mathcal{O}_{\mathbb{K}}$, on remarque que le conducteur est à la fois un idéal entier de $\mathcal{O}$ et de $\mathcal{O}_{\mathbb{K}}$.

Proposition 2.4.11. *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et $\mathfrak{f}$ son conducteur. Pour $I \trianglelefteq \mathcal{O}_{\mathbb{K}}$, on a que $I \subset \mathcal{O}$ si et seulement si $I \subset \mathfrak{f}$.*

Démonstration. Puisque I est un idéal de $\mathcal{O}_{\mathbb{K}}$, on a que $I = I\mathcal{O}_{\mathbb{K}}$ et donc par définition du conducteur on obtient $I \subset \mathfrak{f}$ si $I = I\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}$. L'autre inclusion provient du fait que $\mathfrak{f} \subset \mathcal{O}$. $\square$

On a donc que le conducteur de $\mathcal{O}$ est le plus grand idéal entier qui est à la fois dans $\mathcal{O}$ et dans $\mathcal{O}_{\mathbb{K}}$. La proposition suivante explique l'importance du conducteur d'un ordre.

Proposition 2.4.12. *Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique avec d sans facteurs carrés, notons $d' = \sqrt{d}$ si $d \equiv 2, 3 \pmod{4}$ et $d' = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1 \pmod{4}$, de façon à obtenir $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[d']$.*

1. *Tous les ordres de $\mathbb{Q}(\sqrt{d})$ sont de la forme $\mathbb{Z}[cd']$ pour $c \in \mathbb{N}^*$ et $[\mathbb{Z}[d'] : \mathbb{Z}[cd']] = c$.*
2. *Le conducteur de l'ordre $\mathbb{Z}[cd']$ est $c\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.*

Démonstration. 1. Par définition, un ordre d'un corps quadratique doit être un $\mathbb{Z}$ -module de rang 2. On a $1 \in \mathcal{O}$ et d'après une généralisation de la proposition 1.2.17 aux groupes abéliens libres de type fini qu'on admet, 1 peut être complété pour former une $\mathbb{Z}$ -base. Il existe donc $\alpha \in \mathcal{O} \setminus \mathbb{Z}$ tel que $\mathcal{O} = \mathbb{Z} + \alpha\mathbb{Z}$. Puisque $\mathcal{O} \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[d']$ par définition, on a que $\alpha = a + cd'$ avec $a, c \in \mathbb{Z}$. De plus, $c \neq 0$ car $\alpha \notin \mathbb{Z}$. Remarquons alors qu'on a une matrice de changement de base

$$\begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

qui envoie la base $(1, a + cd')$ sur la base $(1, cd')$. On a donc $\mathbb{Z} = \mathbb{Z} + cd'\mathbb{Z} = \mathbb{Z} \pm cd'\mathbb{Z} = \mathbb{Z}[|c|d']$. Ensuite, puisque $(1, d')$ est une $\mathbb{Z}$ -base de $\mathbb{Z}[d']$ et que

$$(1, |c|d') = (1, d') \begin{pmatrix} 1 & 0 \\ 0 & |c| \end{pmatrix},$$

on conclut par la proposition 1.2.35 que $[\mathbb{Z}[d'] : \mathbb{Z}[|c|d']] = |c|$.

2. Procédons par double inclusion. Premièrement, on a

$$c\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = c\mathbb{Z}[d'] = c\mathbb{Z} + cd'\mathbb{Z} \subset \mathbb{Z} + cd'\mathbb{Z} = \mathbb{Z}[cd'],$$

on en déduit par la proposition 2.4.11 que $c\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \subset \mathfrak{f}$. Pour l'autre inclusion, considérons $x \in \mathfrak{f}$, puisque $\mathfrak{f} \subset \mathbb{Z}[cd']$, on a que $x = a + bcd'$ pour $a, b \in \mathbb{Z}$, il faut

alors montrer que $a \in c\mathbb{Z}$. Remarquons que $a = x - bcd' \in \mathfrak{f} \subset \mathbb{Z}[cd']$ et donc $ad' \in \mathbb{Z}[cd']$, on conclut que c divise a car $(1, cd')$ est une $\mathbb{Z}$ -base de $\mathbb{Z}[cd']$. $\square$

Proposition 2.4.13. *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et $\mathfrak{f}$ son conducteur. Si I est un idéal non nul de $\mathcal{O}$ relativement premier à $\mathfrak{f}$, alors $(I : I) = \mathcal{O}$.*

Démonstration. Les propriétés d'idéaux nous donnent $\mathcal{O} \subset (I : I)$. Pour l'autre inclusion, prenons $x \in (I : I)$, par définition, $x \in \mathbb{K}$ et $xI \subset I$. Cette dernière inclusion et le fait que I soit un $\mathbb{Z}$ -module de type fini nous donne que $\mathbb{Z}[x]$ est un $\mathbb{Z}$ -module de type fini. D'après la proposition 2.1.4, x est entier sur $\mathbb{Z}$ et donc $x \in \mathcal{O}_{\mathbb{K}}$. Ensuite, puisque I est relativement premier avec $\mathfrak{f}$, il existe $a \in I$ et $b \in \mathfrak{f}$ tels que $a + b = 1$. Il en suit que $x = 1 \times x = (a + b)x = ax + bx$, mais $ax \in I \subset \mathcal{O}$ car $x \in (I : I)$, et $bx \in \mathcal{O}$ puisque $b \in \mathfrak{f} = (\mathcal{O} : \mathcal{O}_{\mathbb{K}})$ et $x \in \mathcal{O}_{\mathbb{K}}$. Finalement on a bien $x = ax + bx \in \mathcal{O}$. $\square$

Proposition 2.4.14. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. Si I est un idéal fractionnaire inversible de $\mathcal{O}$ alors son inverse est $(\mathcal{O} : I)$.*

Démonstration. Puisque $I^{-1} \cdot I = \mathcal{O}$, on a $I^{-1} \subset (\mathcal{O} : I)$. De plus, en multipliant cette dernière inclusion par I , on obtient

$$\mathcal{O} = I \cdot I^{-1} \subset I(\mathcal{O} : I) \subset \mathcal{O},$$

ce qui conclut. $\square$

Proposition 2.4.15. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. Si I est un idéal fractionnaire inversible de $\mathcal{O}$ alors $(I : I) = \mathcal{O}$.*

Démonstration. Par définition d'idéal fractionnaire, on a que $\mathcal{O} \subset (I : I)$. Pour l'autre inclusion, considérons $x \in (I : I)$, alors $xI \subset I$, mais puisque I est inversible, on peut multiplier cette dernière inclusion par I^{-1} pour obtenir $x\mathcal{O} \subset \mathcal{O}$, ce qui conclut. $\square$

Définition 2.4.16 (Gorenstein). Un ordre est dit de *Gorenstein* si on a l'autre implication dans la proposition 2.4.15.

Corollaire 2.4.17. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$ différent de $\mathcal{O}_{\mathbb{K}}$. On a que le conducteur de $\mathcal{O}$ n'est pas un idéal fractionnaire inversible de $\mathcal{O}$.*

Démonstration. Notons $\mathfrak{f}$ le conducteur de $\mathcal{O}$, on sait que c'est un idéal entier de $\mathcal{O}_{\mathbb{K}}$. En particulier, $(\mathfrak{f} : \mathfrak{f}) = \mathcal{O}_{\mathbb{K}}$ d'après la proposition 2.4.7. Par hypothèse, $\mathcal{O} \neq \mathcal{O}_{\mathbb{K}}$, on conclut alors par la contraposée de la proposition 2.4.15. $\square$

Puisqu'être inversible est une propriété de classe, il suit du corollaire 2.4.17 que $\text{ICM}(\mathcal{O})$ n'est jamais un groupe lorsque $\mathcal{O} \neq \mathcal{O}_{\mathbb{K}}$. Cela motive la définition suivante.

Définition 2.4.18 (Groupe de Picard). Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. On définit le *groupe de Picard* de $\mathcal{O}$ comme le sous-monoïde de $\text{ICM}(\mathcal{O})$ des classes d'idéaux fractionnaires inversibles. On le note $\text{Pic}(\mathcal{O})$.

Proposition 2.4.19. Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et P un idéal premier non nul de $\mathcal{O}$. On a que P est inversible en tant qu'idéal fractionnaire de $\mathcal{O}$ si et seulement si $(P : P) = \mathcal{O}$.

Démonstration. Le premier sens d'implication est donné par la proposition 2.4.15. Procédons par contraposée pour la réciproque. Si P n'est pas inversible en tant qu'idéal fractionnaire, alors en particulier $P \neq \mathcal{O}$. D'après le lemme 2.2.6, il existe $\omega \in \mathbb{K} \setminus \mathcal{O}$ tel que $\omega P \subset \mathcal{O}$. On a alors la chaîne d'inclusion suivante

$$P \subset (\mathcal{O} + \omega\mathcal{O})P \subset P + \omega P \subset \mathcal{O}.$$

D'après la proposition 2.4.3, P est maximal et donc soit $(\mathcal{O} + \omega\mathcal{O})P = P$, soit $(\mathcal{O} + \omega\mathcal{O})P = \mathcal{O}$. Puisque P n'est pas inversible par hypothèse, on a $(\mathcal{O} + \omega\mathcal{O})P = P$. On trouve finalement $\omega \in (P : P) \setminus \mathcal{O}$. $\square$

On rappelle un résultat d'algèbre commutative, une preuve est donnée dans [14].

Lemme 2.4.20 (Nakayama). Soit $\mathbb{A}$ un anneau commutatif, M un $\mathbb{A}$ -module de type fini, et I un idéal de $\mathbb{A}$ tel que $M \subset IM$, alors il existe un élément $a \in I$ tel que $(1 + a)M = 0$.

Proposition 2.4.21. Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et $\mathfrak{f}$ son conducteur. Tout idéal non nul de $\mathcal{O}$ relativement premier à $\mathfrak{f}$ est un produit d'idéaux premiers inversibles.

Démonstration. Soit I un idéal non nul de $\mathcal{O}$ relativement premier à $\mathfrak{f}$, d'après la proposition 2.4.13, on a que $(I : I) = \mathcal{O}$. Si I est premier, alors on conclut par la proposition 2.4.19. Sinon, on procède par récurrence forte sur $[\mathcal{O} : I]$. Le théorème de Krull 2.2.1 nous donne un idéal maximal $P \triangleleft \mathcal{O}$ tel que $I \subset P$. Puisque I est relativement premier avec $\mathfrak{f}$, on obtient $\mathcal{O} = I + \mathfrak{f} \subset P + \mathfrak{f} \subset \mathcal{O}$ et donc P est relativement premier avec $\mathfrak{f}$. On en déduit encore une fois des propositions 2.4.13 et 2.4.19 que P est inversible. Posons $J = IP^{-1}$, puisque I n'est pas premier, alors $I \neq P$ et donc $J \neq \mathcal{O}$. Remarquons maintenant que l'inclusion $I = PJ \subset J$ est stricte. En effet, si $J \subset PJ$, alors le lemme de Nakayama 2.4.20 nous dit qu'il existe $a \in P$ tel que $(1 + a)J = 0$ et puisque P est maximal, $a \neq -1$, on trouve donc une contradiction puisque $\mathcal{O}$ est intègre. Ainsi, l'inclusion stricte nous donne d'une part $[\mathcal{O} : J] < [\mathcal{O} : I]$ et d'autre part $\mathcal{O} = I + \mathfrak{f} \subset J + \mathfrak{f} \subset \mathcal{O}$.

Ainsi, J est relativement premier avec $\mathfrak{f}$ et donc l'hypothèse de récurrence nous dit que J est un produit d'idéaux premiers inversibles. On conclut car $I = PJ$. $\square$

Corollaire 2.4.22. *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et $\mathfrak{f}$ son conducteur. Tout idéal non nul de $\mathcal{O}$ relativement premier à $\mathfrak{f}$ est inversible.*

Proposition 2.4.23. *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et $\mathfrak{f}$ son conducteur. On a une bijection entre les idéaux de $\mathcal{O}$ relativement premiers à $\mathfrak{f}$ et les idéaux de $\mathcal{O}_{\mathbb{K}}$ relativement premiers à $\mathfrak{f}$ donné par $\kappa : I \mapsto I\mathcal{O}_{\mathbb{K}}$ et $\chi : J \mapsto J \cap \mathcal{O}$. De plus κ et χ sont multiplicatifs.*

Démonstration. Montrons d'abord que notre candidat de bijection envoie les idéaux relativement premiers à $\mathfrak{f}$ vers des idéaux relativement premiers à $\mathfrak{f}$. Premièrement, si $I + \mathfrak{f} = \mathcal{O}$, alors $1 \in I + \mathfrak{f}$, mais $\mathcal{O} \subset \mathcal{O}_{\mathbb{K}}$ implique $I\mathcal{O} + \mathfrak{f} \subset I\mathcal{O}_{\mathbb{K}} + \mathfrak{f}$ et donc $1 \in I\mathcal{O}_{\mathbb{K}} + \mathfrak{f}$. On a donc bien que $I\mathcal{O}_{\mathbb{K}} + \mathfrak{f} = \mathcal{O}_{\mathbb{K}}$, c'est-à-dire que $I\mathcal{O}_{\mathbb{K}}$ est relativement premier à $\mathfrak{f}$. Ensuite, si $J + \mathfrak{f} = \mathcal{O}_{\mathbb{K}}$, alors

$$\mathcal{O} = \mathcal{O}_{\mathbb{K}} \cap \mathcal{O} = (I + \mathfrak{f}) \cap \mathcal{O} \subset I \cap \mathcal{O} + \mathfrak{f} \subset \mathcal{O},$$

d'où $I \cap \mathcal{O} + \mathfrak{f} = \mathcal{O}$ et donc $I \cap \mathcal{O}$ est relativement premier à $\mathfrak{f}$.

Montrons maintenant que κ est bijectif et d'inverse χ . Puisque $\chi(J) + \mathfrak{f} = \mathcal{O}$, on a

$$\begin{aligned} J &= J\mathcal{O} = J(\chi(J) + \mathfrak{f}) = J(J \cap \mathcal{O} + \mathfrak{f}) \\ &\subset J(J \cap \mathcal{O}) + J\mathfrak{f} \subset \mathcal{O}_{\mathbb{K}}(J \cap \mathcal{O}) + (J \cap \mathcal{O})\mathcal{O}_{\mathbb{K}} = (J \cap \mathcal{O})\mathcal{O}_{\mathbb{K}} \subset J. \end{aligned}$$

On en déduit que $\kappa(\chi(J)) = (J \cap \mathcal{O})\mathcal{O}_{\mathbb{K}} = J$. Aussi, on trouve

$$I \subset I\mathcal{O}_{\mathbb{K}} \cap \mathcal{O} = (I\mathcal{O}_{\mathbb{K}} \cap \mathcal{O})\mathcal{O} \subset I(I + \mathfrak{f}) \subset I.$$

On en conclut que $\chi(\kappa(I)) = I\mathcal{O}_{\mathbb{K}} \cap \mathcal{O} = I$.

Enfin, puisque κ et χ sont inverses l'un de l'autre, il suffit de remarquer que κ est multiplicatif. $\square$

Proposition 2.4.24. *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et $\mathfrak{f}$ son conducteur. Si J est un idéal non nul de $\mathcal{O}_{\mathbb{K}}$ relativement premier à $\mathfrak{f}$, alors on a un isomorphisme d'anneaux canonique $\mathcal{O}/J \cap \mathcal{O} \cong \mathcal{O}_{\mathbb{K}}/J$. Si I est un idéal non nul de $\mathcal{O}$ relativement premier à $\mathfrak{f}$, alors on a un isomorphisme d'anneaux canonique $\mathcal{O}/I \cong \mathcal{O}_{\mathbb{K}}/I\mathcal{O}_{\mathbb{K}}$.*

Démonstration. • Le morphisme $\mathcal{O} \hookrightarrow \mathcal{O}_{\mathbb{K}} \xrightarrow{\pi} \mathcal{O}_{\mathbb{K}}/J$ où π est le morphisme de projection canonique, a pour noyau $J \cap \mathcal{O}$. Ce morphisme est surjectif car $J + \mathfrak{f} = \mathcal{O}_{\mathbb{K}}$ et $\mathfrak{f} \subset \mathcal{O}$. On conclut par le premier théorème d'isomorphisme.

- Le morphisme $\mathcal{O} \hookrightarrow \mathcal{O}_{\mathbb{K}} \xrightarrow{\pi} \mathcal{O}_{\mathbb{K}}/I\mathcal{O}_{\mathbb{K}}$ où π est le morphisme de projection canonique, a pour noyau $I\mathcal{O}_{\mathbb{K}} \cap \mathcal{O} = I$. Ce morphisme est surjectif car $I\mathcal{O}_{\mathbb{K}} + \mathfrak{f} = \mathcal{O}_{\mathbb{K}}$ et $\mathfrak{f} \subset \mathcal{O}$. On conclut par le premier théorème d'isomorphisme. $\square$

Proposition 2.4.25. *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et H un idéal non nul de $\mathcal{O}$. Toute classe d'idéaux fractionnaires dans $\text{Pic}(\mathcal{O})$ contient un idéal entier relativement premier à H .*

Démonstration. Le cas où $H = \mathcal{O}$ est trivial, supposons alors maintenant que $H \neq \mathcal{O}$. Soit I un idéal fractionnaire inversible de $\mathcal{O}$, on cherche $x \in \mathbb{K}^*$ tel que $xI^{-1} \subset \mathcal{O}$ et $xI^{-1} + H = \mathcal{O}$. D'après la proposition 2.4.14, $I^{-1} = (\mathcal{O} : I)$, et donc pour tout $x \in I$, on a $xI^{-1} \subset \mathcal{O}$. Il en suit que $xI^{-1} + H \subset \mathcal{O}$. Supposons par l'absurde que pour tout $x \in I$, $xI^{-1} + H \neq \mathcal{O}$. Puisque $H \neq \mathcal{O}$, le théorème de Krull 2.2.1 nous dit qu'il existe un idéal maximal P tel que $H \subset P$. De plus, l'indice $[\mathcal{O} : H] \in \mathbb{N}^*$ d'après la proposition 2.4.2, et donc il n'y a qu'un nombre fini d'idéaux maximaux contenant H qu'on note $P_1, \dots, P_m$. Pour tout $x \in I$, il existe $k \in \llbracket 1, m \rrbracket$ tel que $xI^{-1} + H \subset P_k$ car $H \subset xI^{-1} + H$. Aussi, $H \subset P_k$ nous donne $xI^{-1} \subset P_k$ et donc $x \in P_k I$. Il suffit alors de montrer qu'il existe $x \in I$ tel que $x \notin P_k I$ pour tout $k \in \llbracket 1, m \rrbracket$ pour obtenir une contradiction. Remarquons que $P_k I \subset I$ mais $P_k I \neq I$ pour tout $k \in \llbracket 1, m \rrbracket$, il existe donc $x_k \in I \setminus P_k I$ pour tout $k \in \llbracket 1, m \rrbracket$. Enfin, le théorème des restes chinois nous donne l'existence d'un $x \in I$ tel que $x \equiv x_k$ modulo $P_k I$ pour tout $k \in \llbracket 1, m \rrbracket$, ce qui conclut. $\square$

Lemme 2.4.26. *Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et $\mathfrak{f}$ son conducteur. Pour $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}^*$, si $\alpha - \beta \in \mathfrak{f}$, alors $\alpha\mathcal{O}_{\mathbb{K}} \cap \mathcal{O} = \frac{\alpha}{\beta}(\beta\mathcal{O}_{\mathbb{K}} \cap \mathcal{O})$. En particulier, $\alpha\mathcal{O}_{\mathbb{K}} \cap \mathcal{O}$ et $\beta\mathcal{O}_{\mathbb{K}} \cap \mathcal{O}$ sont dans la même classe d'idéaux fractionnaires.*

Démonstration. Remarquons premièrement que

$$\alpha\mathcal{O}_{\mathbb{K}} \cap \mathcal{O} = \frac{\alpha}{\beta}(\beta\mathcal{O}_{\mathbb{K}} \cap \mathcal{O}) \iff \mathcal{O}_{\mathbb{K}} \cap \frac{1}{\alpha}\mathcal{O} = \mathcal{O}_{\mathbb{K}} \cap \frac{1}{\beta}\mathcal{O}.$$

Cette dernière égalité est symétrique, on peut montrer la double inclusion en montrant uniquement $\mathcal{O}_{\mathbb{K}} \cap \frac{1}{\alpha}\mathcal{O} \subset \mathcal{O}_{\mathbb{K}} \cap \frac{1}{\beta}\mathcal{O}$. Soit $a \in \mathcal{O}_{\mathbb{K}} \cap \frac{1}{\alpha}\mathcal{O}$, on a que $\alpha - \beta \in \mathfrak{f}$ nous donne l'existence de $\eta \in \mathfrak{f}$ tel que $\alpha = \beta + \eta$. Puisque $a \in \frac{1}{\alpha}\mathcal{O}$, on a $\beta a + \eta a = (\beta + \eta)a = \alpha a \in \mathcal{O}$. Or, $\eta a \in \mathfrak{f} \subset \mathcal{O}$ et donc $\beta a \in \mathcal{O}$ et donc $a \in \mathcal{O}_{\mathbb{K}} \cap \frac{1}{\beta}\mathcal{O}$. $\square$

Proposition 2.4.27. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. La séquence de morphismes de groupes abéliens*

$$(\mathcal{O}_{\mathbb{K}}/\mathfrak{f})^{\times} \xrightarrow{\iota} \text{Pic}(\mathcal{O}) \xrightarrow{\kappa} \text{Pic}(\mathcal{O}_{\mathbb{K}}) \longrightarrow 0$$

où $\iota : \alpha + \mathfrak{f} \mapsto [\alpha\mathcal{O}_{\mathbb{K}} \cap \mathcal{O}]$ et $\kappa : [I] \mapsto [I\mathcal{O}_{\mathbb{K}}]$, est exacte en $\text{Pic}(\mathcal{O})$ et $\text{Pic}(\mathcal{O}_{\mathbb{K}})$.

Démonstration. • Exactitude en $\text{Pic}(\mathcal{O}_{\mathbb{K}})$: il faut montrer que κ est surjectif. Le fait que c'est un morphisme de groupes suit de la proposition 2.4.23. Soit $\mathfrak{f}$ le conducteur de $\mathcal{O}$, c'est un idéal non nul de $\mathcal{O}_{\mathbb{K}}$, donc la proposition 2.4.25 nous dit que toute classe d'idéaux fractionnaire de $\mathcal{O}_{\mathbb{K}}$ contient un idéal entier J relativement premier à $\mathfrak{f}$. D'après la proposition 2.4.23, $J \cap \mathcal{O}$ est relativement premier à $\mathfrak{f}$ et $(J \cap \mathcal{O})\mathcal{O}_{\mathbb{K}} = J$. Il suit de la proposition 2.4.22 que $J \cap \mathcal{O}$ est inversible et donc $[J \cap \mathcal{O}] \in \text{Pic}(\mathcal{O})$ et donc on trouve $\kappa([J \cap \mathcal{O}]) = [(J \cap \mathcal{O})\mathcal{O}_{\mathbb{K}}] = [J]$.

- Exactitude en $\text{Pic}(\mathcal{O})$: le fait que ι est un morphisme de groupes suit de la multiplicativité de χ dans la proposition 2.4.23. Le conducteur $\mathfrak{f}$ est aussi un idéal non nul de $\mathcal{O}$, donc la proposition 2.4.25 nous dit que toute classe d'idéaux fractionnaire de $\mathcal{O}$ contient un idéal entier I relativement premier à $\mathfrak{f}$. On a que $[I] \in \text{Ker}(\kappa)$ si et seulement si $I\mathcal{O}_{\mathbb{K}}$ est principal, c'est-à-dire s'il existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tel que $I\mathcal{O}_{\mathbb{K}} = \alpha\mathcal{O}_{\mathbb{K}}$. D'après la proposition 2.4.23, on a d'une part que $\alpha\mathcal{O}_{\mathbb{K}}$ est relativement premier à $\mathfrak{f}$ et d'autre part $I = I\mathcal{O}_{\mathbb{K}} \cap \mathcal{O} = \alpha\mathcal{O}_{\mathbb{K}} \cap \mathcal{O}$. Il en suit que $\alpha + \mathfrak{f}$ est inversible dans $\mathcal{O}_{\mathbb{K}}/\mathfrak{f}$ et donc $\text{Ker}(\kappa) = \{[\alpha\mathcal{O}_{\mathbb{K}} \cap \mathcal{O}] \mid \alpha\mathcal{O}_{\mathbb{K}} \text{ premier avec } \mathfrak{f}\}$. On conclut par le lemme 2.4.26 que $\text{Ker}(\kappa) = \text{Im}(\iota)$.

□

Exemple 2.4.28. 1. $\text{Pic}(\mathbb{Z}[\sqrt{13}])$ est trivial : d'après la proposition 2.3.33, on a que $\mu_{\mathbb{Q}(\sqrt{13})} = \frac{\sqrt{13}}{2} \simeq 1,8$, et donc $\text{Pic}(\mathcal{O}_{\mathbb{Q}(\sqrt{13})})$ est trivial par le corollaire 2.3.36. Il en suit que $\text{Pic}(\mathbb{Z}[\sqrt{13}])$ est donné par l'image du morphisme ι de la proposition 2.4.27. La proposition 2.4.12 nous dit que le conducteur de $\mathbb{Z}[\sqrt{13}]$ est $2\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$. On trouve par la suite

$$\mathcal{O}_{\mathbb{Q}(\sqrt{13})}/\mathfrak{f} = \mathbb{Z} \left[\frac{1+\sqrt{13}}{2} \right] / 2\mathbb{Z} \left[\frac{1+\sqrt{13}}{2} \right] \cong (\mathbb{Z}/2\mathbb{Z})[X]/(X^2-X-3)(\mathbb{Z}/2\mathbb{Z})[X] \cong \mathbb{F}_4.$$

Ainsi, $(\mathcal{O}_{\mathbb{Q}(\sqrt{13})}/\mathfrak{f})^\times \cong \mathbb{Z}/3\mathbb{Z}$, il suffit alors de montrer qu'un élément non neutre de $(\mathcal{O}_{\mathbb{Q}(\sqrt{13})}/\mathfrak{f})^\times$ est dans le noyau de ι pour conclure. Considérons $1 + \frac{1+\sqrt{13}}{2} + \mathfrak{f} \in (\mathcal{O}_{\mathbb{Q}(\sqrt{13})}/\mathfrak{f})^\times$, on a alors

$$\begin{aligned} \left(1 + \frac{1+\sqrt{13}}{2}\right) \mathbb{Z} \left[\frac{1+\sqrt{13}}{2} \right] &= \left(1 + \frac{1+\sqrt{13}}{2}\right) \left\{ a + b \frac{1+\sqrt{13}}{2} \mid a, b \in \mathbb{Z} \right\} \\ &= \left\{ \frac{3a}{2} + 4b + \left(\frac{a}{2} + b\right) \sqrt{13} \right\}. \end{aligned}$$

Un élément de cet ensemble appartient à l'ordre $\mathbb{Z}[\sqrt{13}]$ si et seulement si a est

pair. On trouve finalement

$$\left(1 + \frac{1 + \sqrt{13}}{2}\right) \mathbb{Z} \left[\frac{1 + \sqrt{13}}{2} \right] \cap \mathbb{Z}[\sqrt{13}] = \{3c + 4b + (c + b)\sqrt{13} \mid c, b \in \mathbb{Z}\}.$$

Or,

$$\begin{pmatrix} 3 & 4 \\ 1 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{Z}),$$

donc $\left(1 + \frac{1 + \sqrt{13}}{2}\right) \mathbb{Z} \left[\frac{1 + \sqrt{13}}{2} \right] \cap \mathbb{Z}[\sqrt{13}] = \mathbb{Z}[\sqrt{13}]$, ce qui conclut.

2.4.2 Monoïde des classes d'idéaux d'un ordre

Définition 2.4.29 (Différente). Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et I un idéal fractionnaire de $\mathcal{O}$. On définit la *différente* de I comme

$$I^t := \{x \in \mathbb{K} \mid \text{Tr}_{\mathbb{K}}(xI) \subset \mathbb{Z}\}.$$

Proposition 2.4.30. Soit $\mathbb{K}$ un corps de nombres, $\mathcal{O}$ un ordre de $\mathbb{K}$ et I, J deux idéaux fractionnaires de $\mathcal{O}$, la différentielle a les propriétés suivantes

1. $I = (I^t)^t$
2. $I \subset J \iff J^t \subset I^t$
3. $(xI)^t = \frac{1}{x}I^t$ pour tout $x \in \mathbb{K}^*$.

Démonstration. 1. On a

$$(I^t)^t = \{x \in \mathbb{K} \mid \text{Tr}_{\mathbb{K}}(xI^t) \subset \mathbb{Z}\} = \{x \in \mathbb{K} \mid \forall y \in \mathbb{K} : \text{Tr}_{\mathbb{K}}(yI) \subset \mathbb{Z} \Rightarrow \text{Tr}_{\mathbb{K}}(xy) \in \mathbb{Z}\}.$$

Il est clair de par cette définition que $I \subset (I^t)^t$. On admet l'autre inclusion.

2. D'après le point précédent, il suffit de montrer un sens de l'implication. Supposons alors que $I \subset J$ et prenons $x \in J^t$. Par définition, on a $\text{Tr}_{\mathbb{K}}(xJ) \subset \mathbb{Z}$, mais puisque $I \subset J$, on trouve que $xI \subset xJ$ et donc $\text{Tr}_{\mathbb{K}}(xI) \subset \text{Tr}_{\mathbb{K}}(xJ) \subset \mathbb{Z}$. On conclut que $x \in I^t$.

3. Soit $x \in \mathbb{K}^*$, on a

$$(xI)^t = \{y \in \mathbb{K} \mid \text{Tr}_{\mathbb{K}}(yxI) \subset \mathbb{Z}\} = \frac{1}{x}\{y \in \mathbb{K} \mid \text{Tr}_{\mathbb{K}}(yI) \subset \mathbb{Z}\} = \frac{1}{x}I^t.$$

□

Lemme 2.4.31. Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. Si I est un idéal fractionnaire tel que $(I : I) = \mathcal{O}$, alors $II^t = \mathcal{O}^t$.

Démonstration. Montrons d'abord que $II^t \subset \mathcal{O}^t$. Soit $a \in II^t$ et $z \in \mathcal{O}$, on doit montrer que $\text{Tr}_{\mathbb{K}}(za) \in \mathbb{Z}$. Or, la définition du produit d'idéaux fractionnaires nous dit qu'il existe $m \in \mathbb{N}^*$ tel que $a = \sum_{k=1}^m x_k y_k$ avec $x_k \in I$ et $y_k \in I^t$ pour tout $k \in \llbracket 1, m \rrbracket$. Par additivité de la trace (proposition 2.1.26), il suffit de montrer que $\text{Tr}_{\mathbb{K}}(zx_k y_k) \in \mathbb{Z}$ pour tout $k \in \llbracket 1, m \rrbracket$ afin de montrer que $\text{Tr}_{\mathbb{K}}(\sum_{k=1}^m zx_k y_k) \in \mathbb{Z}$. Puisque I est un idéal fractionnaire de $\mathcal{O}$, on a que $zx_k \in I$ car $z \in \mathcal{O}$ et $x_k \in I$, et par définition de I^t , on a $\text{Tr}_{\mathbb{K}}(zx_k y_k) \in \mathbb{Z}$ car $y_k \in I^t$.

Pour l'autre inclusion, on a d'après la proposition 2.4.30 que c'est équivalent à montrer que $(II^t)^t \subset (\mathcal{O}^t)^t$, et cette même proposition nous dit qu'il suffit de montrer $(II^t)^t \subset \mathcal{O}$. Soit $x \in (II^t)^t$, alors par définition, on a que $\text{Tr}_{\mathbb{K}}(xII^t) \subset \mathbb{Z}$, il en suit que $xI^t \subset I^t$. Par la proposition 2.4.30, on a alors $I \subset (I^t)^t \subset \frac{1}{x}I$, et donc $xI \subset I$. On conclut bien que $x \in (I : I) = \mathcal{O}$. $\square$

Proposition 2.4.32. *Soit $\mathbb{K}$ un corps de nombres. Un ordre $\mathcal{O}$ de $\mathbb{K}$ est de Gorenstein si et seulement si $\mathcal{O}^t$ est inversible.*

Démonstration. Supposons que $\mathcal{O}$ soit de Gorenstein, on peut alors montrer que $(\mathcal{O}^t : \mathcal{O}^t) = \mathcal{O}$ pour prouver que $\mathcal{O}^t$ est inversible. On a $\mathcal{O} \subset (\mathcal{O}^t : \mathcal{O}^t)$ car $\mathcal{O}^t$ est un $\mathcal{O}$ -module. Pour l'autre inclusion, prenons $x \in (\mathcal{O}^t : \mathcal{O}^t)$, alors $x\mathcal{O}^t \subset \mathcal{O}^t$ et donc $\mathcal{O} = (\mathcal{O}^t)^t \subset (x\mathcal{O}^t)^t = \frac{1}{x}\mathcal{O}$ par la proposition 2.4.30. Ainsi $x\mathcal{O} \subset \mathcal{O}$ et donc $x \in \mathcal{O}$ car $1 \in \mathcal{O}$.

Réciproquement, supposons que $\mathcal{O}^t$ est inversible et qu'un idéal fractionnaire de $\mathcal{O}$ ait la propriété que $(I : I) = \mathcal{O}$. Montrons que I est inversible. D'après le lemme 2.4.31, on a que $II^t = \mathcal{O}^t$, on multiplie alors par l'inverse de $\mathcal{O}^t$ afin d'obtenir $II^t(\mathcal{O}^t)^{-1} = \mathcal{O}$, ce qui conclut. $\square$

Définition 2.4.33 (Monogène). Soit $\mathbb{K}$ un corps de nombres. Un ordre de $\mathbb{K}$ est dit *monogène* s'il est de la forme $\mathbb{Z}[\alpha]$ pour $\alpha \in \mathcal{O}_{\mathbb{K}}$.

Proposition 2.4.34. *Tout ordre monogène est de Gorenstein.*

Démonstration. On admet que $\mathbb{Z}[\alpha]^t = \frac{1}{P'(\alpha)}\mathbb{Z}[\alpha]$ où P est le polynôme minimal de α sur $\mathbb{Q}$. On conclut par la proposition 2.4.32. $\square$

Définition 2.4.35 (Bass). Soit $\mathbb{K}$ un corps de nombres. Un ordre de $\mathbb{K}$ est dit de *Bass* si tous ses sur-ordres sont de Gorenstein.

Corollaire 2.4.36. *Tout ordre quadratique est de Bass.*

Démonstration. D'après la proposition 2.4.12, tous les ordres quadratiques sont monogènes. Ils sont donc en particulier tous de Gorenstein d'après la proposition 2.4.34. $\square$

Proposition 2.4.37. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de $\mathbb{K}$. Si $\mathcal{O}$ est de Bass, alors on a l'égalité ensembliste suivante*

$$\mathrm{ICM}(\mathcal{O}) = \bigsqcup_{\mathcal{O} \subset \mathcal{R}} \mathrm{Pic}(\mathcal{R}),$$

où l'union disjointe est indexée par les sur-ordres de $\mathcal{O}$.

Démonstration. Soit I un idéal fractionnaire de $\mathcal{O}$, posons $\mathcal{R} = (I : I)$ l'anneau des multiplicateurs de I . D'après la proposition 2.4.7 et le corollaire 2.4.8, on a que $\mathcal{R}$ est un sur-ordre de $\mathcal{O}$ et I est un idéal fractionnaire de $\mathcal{R}$. Par hypothèse, $\mathcal{O}$ est de Bass, donc $\mathcal{R}$ est de Gorenstein, et donc I est inversible dans $\mathcal{R}$ et uniquement dans le sur-ordre $\mathcal{R}$ (proposition 2.4.15). L'anneau des multiplicateurs est un invariant de classes d'idéaux fractionnaires de $\mathcal{O}$. Ainsi, pour conclure, il reste à remarquer qu'étant donnés deux idéaux fractionnaires J, H de $\mathcal{O}$ ayant le même anneau des multiplicateurs $\mathcal{S}$, s'ils sont équivalents en tant qu'idéaux fractionnaires de $\mathcal{O}$, alors ils le sont aussi en tant qu'idéaux fractionnaires de $\mathcal{S}$. $\square$

Corollaire 2.4.38. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{O}$ un ordre de Bass de $\mathbb{K}$. Il n'y a qu'un nombre fini de classes d'idéaux fractionnaires.*

Démonstration. Il n'y a qu'un nombre fini de sur-ordres et chaque groupe de Picard d'un ordre est fini d'après la suite exacte donnée par la proposition 2.4.27 car le groupe des classes d'idéaux d'un corps de nombres est fini et $\mathcal{O}_{\mathbb{K}}/\mathfrak{f}$ est fini. $\square$

Exemple 2.4.39. D'après l'exemple donné dans 2.4.28 et la proposition 2.4.37, on a que les deux classes d'idéaux fractionnaires de $\mathbb{Z}[\sqrt{13}]$ sont $[\mathbb{Z}[\sqrt{13}]]$ et $[\mathbb{Z}[\frac{1+\sqrt{13}}{2}]]$.

Chapitre 3

Dernier théorème de Fermat

Lemme 3.0.1. Soit p un nombre premier impair et notons $\zeta = e^{i\frac{2\pi}{p}}$. Pour $x, y \in \mathbb{C}$, on a que

$$x^p + y^p = \prod_{k=0}^{p-1} (x + \zeta^k y).$$

Démonstration. Le cas où $y = 0$ est trivial, on suppose donc maintenant que $y \neq 0$. On évalue le polynôme $T(X) = X^p - 1$ en $\frac{x}{-y}$ pour obtenir

$$T(X) = X^p - 1 = \prod_{k=0}^{p-1} (X - \zeta^k) \quad (3.1)$$

$$\Rightarrow T\left(\frac{x}{-y}\right) = \frac{x^p}{-y^p} - 1 = \prod_{k=0}^{p-1} \left(\frac{x}{-y} - \zeta^k\right) \quad (3.2)$$

$$\Rightarrow -y^p T\left(\frac{x}{-y}\right) = x^p + y^p = \prod_{k=0}^{p-1} (x + \zeta^k y). \quad (3.3)$$

□

Lemme 3.0.2. Soit p un nombre premier impair, notons $\zeta = e^{i\frac{2\pi}{p}}$. On a que pour tout $\alpha \in \mathbb{Z}[\zeta]$, il existe $a \in \mathbb{Z}$ tel que $\alpha \equiv a$ modulo $(1 - \zeta)\mathbb{Z}[\zeta]$.

Démonstration. C'est équivalent à montrer que la surjectivité du morphisme d'anneaux $\mathbb{Z} \hookrightarrow \mathbb{Z}[\zeta] \xrightarrow{\pi} \mathbb{Z}[\zeta]/(1 - \zeta)\mathbb{Z}[\zeta]$ où π est le morphisme de projection canonique. Puisque $N_{\mathbb{Z}[\zeta]}(1 - \zeta) = p$ d'après la proposition 2.1.33, on a que $|\mathbb{Z}[\zeta]/(1 - \zeta)\mathbb{Z}[\zeta]| = p$ d'après la proposition 2.2.22. On obtient donc l'isomorphisme d'anneaux $\mathbb{Z}[\zeta]/(1 - \zeta)\mathbb{Z}[\zeta] \cong \mathbb{Z}/p\mathbb{Z}$. En appelant $\lambda : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}[\zeta]/(1 - \zeta)\mathbb{Z}[\zeta]$ cet isomorphisme et $\pi' : \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ le morphisme de projection canonique, on obtient que $\pi \circ \iota = \lambda \circ \pi'$ car $\mathbb{Z}$ est l'élément initial de la catégorie des anneaux unitaires et des morphismes d'anneaux unitaires. Il en suit que $\pi \circ \iota$ est surjectif. □

Lemme 3.0.3. Soit p un nombre premier impair, notons $\zeta = e^{i\frac{2\pi}{p}}$. On a que pour tout $\alpha \in \mathbb{Z}[\zeta]$, il existe $a \in \mathbb{Z}$ tel que $\alpha^p \equiv a^p$ modulo $p\mathbb{Z}[\zeta]$.

Démonstration. D'après le lemme 3.0.2, il existe $a \in \mathbb{Z}$ tel que $1 - \zeta$ divise $\alpha - a$. Il existe donc $\beta \in \mathbb{Z}[\zeta]$ tel que $(1 - \zeta)\beta = \alpha - a$. On a alors par la formule du binôme de Newton que

$$(1 - \zeta)^p \beta^p = (\alpha - a)^p = \alpha^p - a^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^{p-k} (-a)^k.$$

D'après la proposition 2.2.30, p divise $(1 - \zeta)^p$ et divise donc

$$\alpha^p - a^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^{p-k} (-a)^k.$$

Puisque p divise $\binom{p}{k}$ pour tout $k \in \llbracket 1, p-1 \rrbracket$, on trouve bien que p divise $\alpha^p - a^p$.

□

Définition 3.0.4 (Régulier). Un nombre premier impair positif p est dit *régulier* s'il ne divise pas l'ordre de $\text{Pic}(\mathbb{Z}[\zeta])$ où $\zeta = e^{i\frac{2\pi}{p}}$.

Lemme 3.0.5. Soit $\mathbb{K}$ un corps de nombres, b l'ordre du groupe de Picard de $\mathbb{K}$ et $q \in \mathbb{N}^*$ un nombre copremier avec b . Si un idéal fractionnaire I est tel que I^q est principal, alors I est lui-même principal.

Démonstration. On doit montrer que la classe de I est triviale. Puisque q est copremier avec b , il existe par le théorème de Bézout 1.2.27 $u, v \in \mathbb{Z}$ tels que $bu + qv = 1$. On a alors

$$[I]^1 = [I]^{bu+qv} = [I]^{bu} [I]^{qv} = ([I]^b)^u ([I]^q)^v = [\mathcal{O}_{\mathbb{K}}]^u [I^q]^v = [\mathcal{O}_{\mathbb{K}}][\mathcal{O}_{\mathbb{K}}]^v = [\mathcal{O}_{\mathbb{K}}].$$

□

Lemme 3.0.6. Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire irréductible de degré $n \geq 1$ et soient $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ ses racines. Pour tout $k \in \mathbb{N}$, on a que les coefficients de

$$P_k(X) := \prod_{j=1}^n (X - \alpha_j^k)$$

sont des entiers rationnels.

Démonstration. Soit $k \in \mathbb{N}$, remarquons que tous les α_j sont des entiers algébriques, il en est donc de même pour tous les α_j^k . Soit $\mathbb{L}$ le corps de décomposition de P , puisque P est le polynôme minimal de α_1 , on obtient en posant $G = \text{Gal}_{\mathbb{Q}}(\mathbb{L})$ que

$$P(X) = \prod_{\tau \in G} (X - \tau(\alpha_1)).$$

Les propriétés de morphismes de corps nous donnent que

$$P_k(X) = \prod_{j=1}^n (X - \alpha_j^k) = \prod_{\tau \in G} (X - \tau(\alpha_1^k)) = \prod_{\tau \in G} (X - \tau(\alpha_1^k)).$$

On a alors pour tout $\tau \in G$, que P_{k_τ} , le polynôme P_k où l'on a appliqué τ à ses coefficients, est égale à P_k . En effet,

$$P_{k_\tau}(X) = \prod_{\tau' \in G} (X - \tau'(\tau(\alpha_1^k))) = \prod_{\tau'' \in G} (X - \tau''(\alpha_1^k)) = P_k(X).$$

Soit A_1 le polynôme minimal de α_1^k sur $\mathbb{Q}$, d'après la proposition 2.1.9, on a que $A_1 \in \mathbb{Z}[X]$ car α_1^k est un entier algébrique. Puisque $P_k(\alpha_1^k) = 0$, on a que A_1 divise P_k et donc $A_1 = \prod_{j \in B} (X - \alpha_j^k)$ où $B \subset \llbracket 1, n \rrbracket$. Si $B = \llbracket 1, n \rrbracket$, alors $A_1 = P_k$ et on conclut, sinon on considère A_j le polynôme minimal de α_j^k pour un certain $j \notin B$, on a alors comme précédemment que $A_k \in \mathbb{Z}[X]$ et aussi, A_j divise $\frac{P_k}{A_1}$ car ce dernier annule α_j . On trouve alors que $A_j = \prod_{t \in C} (X - \alpha_t^k)$ où $C \subset \llbracket 1, n \rrbracket \setminus B$. Si cette dernière inclusion est une égalité, on trouve alors que $P_k = A_1 A_j$, sinon on réitère l'argument en considérant A_t le polynôme minimal de α_t^k où $t \notin B \cup C$, qui est aussi à coefficients entiers car α_t^k est un entier algébrique. Ainsi de suite, on trouve finalement que P_k est à coefficients entiers car c'est le produit de polynômes à coefficients entiers. $\square$

Lemme 3.0.7. *Étant donnés $m \in \mathbb{N}^*$ et un m -uplet $(\beta_j)_{j \in \llbracket 1, m \rrbracket} \subset \mathbb{C}$, pour un polynôme défini comme $Q_k(X) := \prod_{j=1}^m (X - \beta_j^k)$, on a que si $|\beta_j| \leq 1$ pour tout $j \in \llbracket 1, m \rrbracket$ alors les coefficients de Q_k sont bornés indépendamment de k .*

Démonstration. Procédons par récurrence sur m .

- Initialisation : si $m = 1$ alors on a bien que pour tout polynôme défini comme $X - \beta^k$ avec $\beta \in \{b \in \mathbb{C} : |b| \leq 1\}$ alors les coefficients de ce polynôme sont bornés en module. En effet, le coefficient dominant est 1 et l'autre coefficient qui est $-\beta^k$ est borné en module par 1 car : $1 \geq |\beta| \implies 1 \geq |\beta|^k = |\beta^k| = |-\beta^k|$.
- Hérité : supposons que pour tout polynôme de degré m défini comme $Q_k(X) = \prod_{j=1}^m (X - \beta_j^k)$ pour tout m -uplet $(\beta_j)_{j \in \llbracket 1, m \rrbracket} \subset \mathbb{C}$, on a la propriété : $|\beta_j| \leq 1$ pour tout $j \in \llbracket 1, m \rrbracket$ implique que les coefficients de Q_k sont bornés indépendamment de k . Montrons que cette propriété est vraie pour tout polynôme de degré $m + 1$ de la forme de Q_k (produit de monômes unitaires).

Soit $\beta_1, \beta_2, \dots, \beta_{m+1} \subset \mathbb{C}$, et soit $\tilde{Q}_k(X) := \prod_{j=1}^{m+1} (X - \beta_j^k)$. Si on nomme comme polynôme $Q_k(X) = \prod_{j=1}^m (X - \beta_j^k)$, on a que $\tilde{Q}_k(X) = (X - \beta_{m+1}^k)Q_k(X)$. Or, Q_k est un polynôme de degré m et d'après l'hypothèse d'hérédité, ses coefficients sont bornés indépendamment de k . On peut donc le réécrire de la façon suivante :

$Q_k(X) = X^m + \sum_{l=0}^{m-1} a_l X^l$ avec $a_l \in \{b \in \mathbb{C} : |b| \leq M\}$ pour tout $l \in \llbracket 0, m-1 \rrbracket$ pour un certain $M \in \mathbb{R}^+$. Ainsi, on a

$$\begin{aligned}\tilde{Q}_k(X) &= (X - \beta_{m+1}^k) Q_k(X) \\ &= (X - \beta_{m+1}^k) \left(X^m + \sum_{l=0}^{m-1} a_l X^l \right) \\ &= X^{m+1} - \beta_{m+1}^k X^m + \sum_{l=1}^m a_{l-1} X^l + \sum_{l=0}^{m-1} (-\beta_{m+1}^k) a_l X^l \\ &= X^{m+1} + (-\beta_{m+1}^k + a_{m-1}) X^m - \beta_{m+1}^k a_0 + \sum_{l=1}^{m-1} (a_{l-1} - \beta_{m+1}^k a_l) X^l\end{aligned}$$

Sachant que comme précédemment, on a $|\beta_{m+1}^k| \leq 1 \implies |-\beta_{m+1}^k| \leq 1$, on observe donc que le coefficient de $\tilde{Q}_k$ est 1, pour le coefficient devant X^m , on a $|-\beta_{m+1}^k + a_{m-1}| \leq |-\beta_{m+1}^k| + |a_{m-1}| \leq 1 + M$. Pour l'ordonnée à l'origine (coefficient devant X^0), on a $|-\beta_{m+1}^k a_0| \leq |-\beta_{m+1}^k| |a_0| \leq 1 * M = M$. Pour les coefficients devant X^l pour $l \in \llbracket 1, m-1 \rrbracket$, on a $|a_{l-1} - \beta_{m+1}^k a_l| \leq |a_{l-1}| + |-\beta_{m+1}^k a_l| \leq M + |-\beta_{m+1}^k| |a_l| \leq M + 1 * M = 2M$. On en conclut finalement que tous les coefficients de $\tilde{Q}_k$ sont bornés indépendamment de k (de borne $\max(M+1, 2M)$). $\square$

Théorème 3.0.8 (Kronecker). *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire séparable de degré $n \geq 1$ et soient $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ ses racines. Si $|\alpha_i| \in]0, 1]$ pour tout $i \in \llbracket 1, n \rrbracket$, alors α_i est une racine de l'unité pour tout $i \in \llbracket 1, n \rrbracket$.*

Démonstration. Pour $k \in \mathbb{N}^*$, prenons P_k défini comme dans 3.0.6, montrons d'abord que l'ensemble $\{P_k \mid k \in \mathbb{N}^*\}$ est fini. D'après le lemme 3.0.6, on a que $\{P_k \mid k \geq 1\} \subset \mathbb{Z}[X]$ et d'après le lemme 3.0.7, on a que les coefficients de P_k sont bornés indépendamment de k . Ainsi, si on nomme M cette borne optimale, on sait que $M \geq 1$ car les P_k sont unitaires et que c'est un entier car les coefficients de P_k sont entiers. On déduit de cette dernière information que les coefficients sont éléments de $\llbracket -M, M \rrbracket$. Or, le nombre de polynômes unitaires de degré n à coefficients dans $\llbracket -M, M \rrbracket$ est fini et vaut exactement $(2M+1)^n$.

De ce fait, si on considère la suite $u : \mathbb{N}^* \rightarrow \mathbb{Z}[X] : k \mapsto P_k$, on a que l'image de u ($\{P_k \mid k \geq 1\}$) est finie. Formellement, cela revient à dire qu'il existe $Q \in \{P_k \mid k \geq 1\}$ et $\psi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ strictement croissante tel que pour tout $k \in \mathbb{N}^*$, $u_{\psi(k)} = Q$. Nommons cette sous-suite $v : v_k = u_{\psi(k)} = Q \forall k \in \mathbb{N}^*$. Construisons maintenant une application qui à tout élément de $\{P_k \mid k \geq 1\}$ associe un vecteur de ses racines (donc de taille n car on compte la multiplicité) qui est ordonnée selon l'indexation i donnée par l'énoncé, c'est-à-dire, $\tau : \{P_k \mid k \geq 1\} \rightarrow \mathbb{Z}^n : \prod_{j=1}^n (X - \alpha_j^k) \mapsto (\alpha_1^k, \alpha_2^k, \dots, \alpha_n^k)$. On a alors que pour tout $k, k' \in \mathbb{N}^*$, $\tau(v_{k'})$ est une permutation de $\tau(v_k)$ car v_k et $v_{k'}$ étant le même

polynôme, ils ont les mêmes racines, donc seul l'ordre dans le vecteur peut changer. Ainsi, puisqu'il y a un nombre fini de permutations possibles, on peut déduire qu'il existe forcément $k, k' \in \mathbb{N}^*$ tels que $k < k'$ et $\tau(v_k) = \tau(v_{k'})$. Or, cela revient à dire qu'il existe $k < k'$ tel que $(\alpha_1^k, \alpha_2^k, \dots, \alpha_n^k) = (\alpha_1^{k'}, \alpha_2^{k'}, \dots, \alpha_n^{k'})$ ou de façon équivalente que pour tout i , $\alpha_i^k = \alpha_i^{k'}$. Mais puisque pour tout i , $|\alpha_i| \neq 0$ donc $\alpha_i \neq 0$ et aussi $\alpha_i^k \neq 0$, on peut diviser dans l'égalité par α_i^k et on trouve alors que $\alpha_i^{k'-k} = 1$ avec $k' - k \in \mathbb{N}^*$. On en conclut donc que pour tout i , α_i est une racine de l'unité. $\square$

Lemme 3.0.9 (Kummer). *Soit p un nombre premier régulier et notons $\zeta = e^{i\frac{2\pi}{p}}$. Pour tout $\varepsilon \in \mathbb{Z}[\zeta]^\times$, il existe $v \in \mathbb{R}$ et $t \in \mathbb{Z}$ tels que $\varepsilon = v\zeta^t$.*

Démonstration. On applique le théorème de Kronecker 3.0.8 à $\frac{\varepsilon}{\bar{\varepsilon}}$ afin d'obtenir $\frac{\varepsilon}{\bar{\varepsilon}} = \pm \zeta^k$ pour un certain $k \in \mathbb{Z}$ (on admet dans ce mémoire que ce sont les seules racines de l'unité dans $\mathbb{Z}[\zeta]$). Puisque p est impair, il existe $t \in \mathbb{Z}$ tel que $\frac{\varepsilon}{\bar{\varepsilon}} = \pm \zeta^{2t}$ et on obtient alors $\varepsilon \zeta^{-t} = \pm \bar{\varepsilon} \zeta^t$. On aimerait que le signe soit positif, car si c'est le cas, on aurait

$$\overline{\varepsilon \zeta^{-t}} = \bar{\varepsilon} \bar{\zeta}^{-t} = \bar{\varepsilon} \zeta^t = \varepsilon \zeta^{-t},$$

et donc $\varepsilon \zeta^{-t} \in \mathbb{R}$. Supposons par l'absurde que le signe est négatif, d'après le lemme 3.0.2, il existe $a \in \mathbb{Z}$ tel que $\varepsilon \zeta^{-t} \equiv a$ modulo $(1 - \zeta)\mathbb{Z}[\zeta]$. En appliquant la conjugaison complexe à cette congruence, on obtient $\bar{\varepsilon} \zeta^t \equiv a$ modulo $(1 - \zeta^{p-1})\mathbb{Z}[\zeta]$ mais la proposition 2.1.38 nous dit que $1 - \zeta$ est associé à $1 - \zeta^{p-1}$ et donc $(1 - \zeta^{p-1})\mathbb{Z}[\zeta] = (1 - \zeta)\mathbb{Z}[\zeta]$. Ainsi, $\varepsilon \zeta^{-t} \equiv \bar{\varepsilon} \zeta^t$ modulo $(1 - \zeta)\mathbb{Z}[\zeta]$ et donc $-\zeta^{2t} = \frac{\varepsilon}{\bar{\varepsilon}} \equiv \zeta^{2t}$ modulo $(1 - \zeta)\mathbb{Z}[\zeta]$. Finalement $1 - \zeta$ divise $2\zeta^{2t}$ et divise même 2 car ζ^{2t} est inversible, or, p est le seul nombre premier rationnel que $1 - \zeta$ divise d'après la proposition 2.2.25. $\square$

On admet le résultat suivant, une preuve détaillée est donnée dans [7].

Lemme 3.0.10 (Kummer). *Soit p un nombre premier régulier et notons $\zeta = e^{i\frac{2\pi}{p}}$. Si $\varepsilon \in \mathbb{Z}[\zeta]^\times$ est congru à un entier rationnel modulo $p\mathbb{Z}[\zeta]$, alors il existe $\omega \in \mathbb{Z}[\zeta]^\times$ tel que $\varepsilon = \omega^p$.*

Lemme 3.0.11. *Soit $x, y, z \in \mathbb{Z}$, si 3 ne divise pas xyz , alors $x^3 + y^3 + z^3 \neq 0$.*

Démonstration. Supposons par l'absurde que $x^3 + y^3 + z^3 = 0$, alors on aurait $x^3 + y^3 + z^3 \equiv 0$ [9]. Or, puisque 3 ne divise pas xyz , on a que x, y, z sont chacun congrus à 1, 2, 4, -4, -2 ou -1 modulo 9. Mais pour tout $k \in \{\pm 1, \pm 2, \pm 4\}$, on a que $k^3 \equiv \pm 1$ [9], et on obtient donc $\pm 1 \pm 1 \pm 1 \equiv 0$ [9], ce qui n'est pas possible. $\square$

Théorème 3.0.12 (Fermat–Kummer). *Soit p un nombre premier régulier, alors l'équation diophantienne $x^p + y^p = z^p$ n'admet aucune solution non triviale.*

Démonstration. Tout d'abord, remarquons qu'il est équivalent de montrer que l'équation diophantienne

$$x^p + y^p + z^p = 0 \quad (3.4)$$

n'admet aucune solution non triviale. En effet, p étant impair, si (a, b, c) est une solution non triviale de $x^p + y^p = z^p$, alors $(a, b, -c)$ est une solution non triviale de $x^p + y^p + z^p = 0$. Remarquons maintenant que si un nombre premier rationnel q divise deux de ces termes, disons sans perte de généralité x et y , alors q divise z^p et divise donc z car c 'est un nombre premier. On peut donc supposer que x, y et z sont deux à deux coprimiers car si (a, b, c) est une solution non triviale, alors $(\frac{a}{q}, \frac{b}{q}, \frac{c}{q})$ est aussi une solution non triviale pour tout nombre premier rationnel q divisant x, y et z . Maintenant qu'on a réduit le problème, on va démontrer ce théorème en faisant une disjonction de cas selon que p divise ou non xyz .

- p ne divise pas xyz : d'après le lemme 3.0.1, l'équation (3.4) se réécrit comme

$$\prod_{k=0}^{p-1} (x + \zeta^k y) = -z^p, \quad (3.5)$$

ce qui induit une équation en termes d'idéaux

$$\prod_{k=0}^{p-1} (x + \zeta^k y) \mathbb{Z}[\zeta] = z^p \mathbb{Z}[\zeta]. \quad (3.6)$$

Montrons que les idéaux $(x + \zeta^k y) \mathbb{Z}[\zeta]$ sont deux à deux coprimiers. Supposons par l'absurde que $(x + \zeta^k y) \mathbb{Z}[\zeta] + (x + \zeta^{k'} y) \mathbb{Z}[\zeta] \neq \mathbb{Z}[\zeta]$ pour $k \neq k'$, alors le théorème de Krull 2.2.1 nous dit qu'il existe un idéal maximal P contenant $(x + \zeta^k y) \mathbb{Z}[\zeta] + (x + \zeta^{k'} y) \mathbb{Z}[\zeta]$. En particulier, $x + \zeta^k y, x + \zeta^{k'} y \in P$ et donc $(1 - \zeta^{k-k'}) \zeta^k y = \zeta^k y - \zeta^{k'} y \in P$. Puisque ζ^k est inversible, $(1 - \zeta^{k-k'}) y \in P$, et puisque P est premier, on a soit $1 - \zeta^{k-k'} \in P$, soit $y \in P$. Remarquons que $z \in P$ puisque d'après la proposition 2.2.10, P divise $(x + \zeta^k y) \mathbb{Z}[\zeta]$ et divise donc $\prod_{k=0}^{p-1} (x + \zeta^k y) \mathbb{Z}[\zeta] = z^p \mathbb{Z}[\zeta]$. Ainsi, $z^p \in P$ et donc $z \in P$ car P est premier. Puisque y et z sont supposés ici être coprimiers, la proposition 2.1.35 nous dit qu'on ne peut pas avoir $y \in P$. On a alors $1 - \zeta^{k-k'} \in P$, mais d'après la proposition 2.1.38, $1 - \zeta^{k-k'}$ est associé à $1 - \zeta$ donc $(1 - \zeta) \mathbb{Z}[\zeta] \subset P$. Or, $(1 - \zeta) \mathbb{Z}[\zeta]$ est maximal d'après la proposition 2.1.33 et donc $(1 - \zeta) \mathbb{Z}[\zeta] = P$. Il en suit que $1 - \zeta$ divise z , et donc $p = N_{\mathbb{Z}[\zeta]}(1 - \zeta)$ divise $N_{\mathbb{Z}[\zeta]}(z) = z^{p-1}$. On trouve alors que p divise z ce qui contredit notre hypothèse. On a donc bien que les $(x + \zeta^k y) \mathbb{Z}[\zeta]$ sont coprimiers.

On déduit alors du théorème 2.2.11 que tous les idéaux $(x + \zeta^k y) \mathbb{Z}[\zeta] = H_k^p$ pour certains idéaux entiers H_k . D'après le lemme 3.0.5, puisque p est régulier, chaque

H_k est principal. Ainsi, pour tout $k \in \llbracket 1, p-1 \rrbracket$, il existe $h_k \in \mathbb{Z}[\zeta]$ tel que $H_k = h_k \mathbb{Z}[\zeta]$. En particulier, il existe $\nu \in \mathbb{Z}[\zeta]^\times$ tel que $x + \zeta y = \nu h_1^p$. D'après le lemme de Kummer 3.0.9, il existe $v \in \mathbb{R}$ et $t \in \mathbb{Z}$ tel que $\nu = v\zeta^t$. Aussi, le lemme 3.0.2 nous dit qu'il existe $g \in \mathbb{Z}$ tel que $g \equiv h_1^p$ modulo $p\mathbb{Z}[\zeta]$. On a alors la congruence

$$x + \zeta y \equiv v\zeta^t g \text{ modulo } p\mathbb{Z}[\zeta]. \quad (3.7)$$

En multipliant par ζ^{-t} d'une part, et en appliquant la conjugaison complexe d'autre part, on obtient

$$\zeta^{-t}(x + \zeta y) \equiv vg \text{ modulo } p\mathbb{Z}[\zeta] \quad (3.8)$$

$$\implies \zeta^t(x + \zeta^{-1}y) \equiv vg \text{ modulo } p\mathbb{Z}[\zeta]. \quad (3.9)$$

En soustrayant ces deux congruences, on trouve

$$\zeta^{-t}x + \zeta^{1-t}y - \zeta^t x - y\zeta^{t-1} \equiv 0 \text{ modulo } p\mathbb{Z}[\zeta]. \quad (3.10)$$

Cette dernière congruence implique que $2t \equiv 1 \pmod{p}$. En effet, si $t \equiv 0 \pmod{p}$, alors (3.10) nous donne

$$\zeta y - \zeta^{-1}y \equiv 0 \text{ modulo } p\mathbb{Z}[\zeta].$$

Or,

$$\zeta y - \zeta^{-1}y = -(\zeta^{-1} - \zeta)y = -\zeta^{-1}(1 - \zeta^2)y = -\zeta^{-1}(1 + \zeta)(1 - \zeta)y,$$

et la proposition 2.1.38 nous dit que $1 + \zeta$ est inversible, et donc $-\zeta^{-1}(1 + \zeta)$ l'est aussi. Il suit de cela que p divise $(1 - \zeta)y$ dans $\mathbb{Z}[\zeta]$ et donc $N_{\mathbb{Z}[\zeta]}(p) = p^{p-1}$ divise $N_{\mathbb{Z}[\zeta]}((1 - \zeta)y) = N_{\mathbb{Z}[\zeta]}(1 - \zeta)N_{\mathbb{Z}[\zeta]}(y) = py^{p-1}$. On a alors que p^{p-2} divise y^{p-1} et donc p divise y , ce qui contredit l'hypothèse. De la même façon, on obtient la même contradiction avec x à la place de y si on considère que $t \equiv 1 \pmod{p}$. La congruence (3.10) nous dit qu'il existe $\delta \in \mathbb{Z}[\zeta]$ tel que $p\delta = \zeta^{-t}x + \zeta^{1-t}y - \zeta^t x - y\zeta^{t-1}$ et donc $\delta = \frac{x}{p}\zeta^{-t} + \frac{y}{p}\zeta^{1-t} - \frac{x}{p}\zeta^t - \frac{y}{p}\zeta^{t-1}$. Or, $\{1, \zeta, \dots, \zeta^{p-2}\}$ constitue une $\mathbb{Z}$ -base de $\mathbb{Z}[\zeta]$ donc on doit avoir deux termes parmi, $t, -t, t-1, 1-t$ qui sont congrus modulo p , car sinon on aurait $\frac{x}{p}, \frac{y}{p} \in \mathbb{Z}$, ce qui contredirait l'hypothèse. Enfin, on a bien $t \equiv 1 - t \pmod{p}$ donc $2t \equiv 1 \pmod{p}$ car

- $t \equiv -t \pmod{p} \iff 2t \equiv 0 \pmod{p} \iff t \equiv 0 \pmod{p}$
- $t - 1 \equiv 1 - t \pmod{p} \iff 2t \equiv 2 \pmod{p} \iff t \equiv 1 \pmod{p}$
- $t \equiv t - 1 \pmod{p} \iff 0 \equiv -1 \pmod{p}$
- $1 - t \equiv -t \pmod{p} \iff 1 \equiv 0 \pmod{p}$.

En multipliant la congruence (3.10) par ζ^t , on trouve alors

$$\zeta^t(\zeta^{-t}x + \zeta^{1-t}y - \zeta^t x - y\zeta^{t-1}) = x + \zeta y - \zeta^{2t}x - \zeta^{2t-1}y \quad (3.11)$$

$$= x + \zeta y - \zeta x - y = (x - y)(1 - \zeta) \equiv 0 \text{ modulo } p\mathbb{Z}[\zeta]. \quad (3.12)$$

Ainsi, p divise $(x - y)(1 - \zeta)$ dans $\mathbb{Z}[\zeta]$ et donc $N_{\mathbb{Z}[\zeta]}(p) = p^{p-1}$ divise $N_{\mathbb{Z}[\zeta]}((x - y)(1 - \zeta)) = N_{\mathbb{Z}[\zeta]}(x - y)N_{\mathbb{Z}[\zeta]}(1 - \zeta) = (x - y)^{p-1}p$. Il en suit que p^{p-2} divise $(x - y)^{p-1}$ et donc p divise $x - y$ car p est premier. Finalement, $x \equiv y [p]$, mais la symétrie de (3.4) nous indique qu'on aurait pu faire exactement la même démonstration pour obtenir $x \equiv z [p]$, et donc l'équation (3.4) implique

$$0 = x^p + y^p + z^p \equiv 3x^p [p]. \quad (3.13)$$

Or, p ne divise pas x par hypothèse donc p divise 3 et vaut donc 3. On conclut alors par le lemme 3.0.11.

- p divise xyz : remarquons premièrement que p divise un seul des facteurs de xyz puisqu'on a pris x, y et z deux à deux coprimiers. La symétrie de (3.4) nous dit qu'on peut supposer sans perte de généralité que p divise z , on a donc $z = p^s z'$ avec $s \in \mathbb{N}^*$ et $z' \in \mathbb{Z} \setminus p\mathbb{Z}$. Aussi, la proposition 2.2.30 nous dit que $p = u(1 - \zeta)^{p-1}$ pour un certain $u \in \mathbb{Z}[\zeta]^\times$ donc

$$z^p = (p^s z')^p = ((u(1 - \zeta)^{p-1})^s z')^p = (u^s (1 - \zeta)^{(p-1)s} z')^p = u^{sp} (1 - \zeta)^{p(p-1)s} z'^p. \quad (3.14)$$

Ainsi, l'équation (3.4) peut se réécrire comme

$$x^p + y^p + u^{sp} (1 - \zeta)^{p(p-1)s} z'^p = 0. \quad (3.15)$$

On va alors montrer un résultat plus fort que celui de Fermat : pour tout $m \in \mathbb{N}^*$, il n'existe aucun $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta] \setminus (1 - \zeta)\mathbb{Z}[\zeta]$ tels que l'équation suivante admette une solution

$$\alpha^p + \beta^p + \varepsilon(1 - \zeta)^{pm} \gamma^p = 0, \quad \varepsilon \in \mathbb{Z}[\zeta]^\times. \quad (3.16)$$

Supposons qu'on ait une solution, alors le lemme 3.0.1 nous donne

$$\prod_{k=0}^{p-1} (\alpha + \zeta^k \beta) = -\varepsilon(1 - \zeta)^{pm} \gamma^p, \quad (3.17)$$

ce qui induit une égalité en termes d'idéaux

$$\prod_{k=0}^{p-1} (\alpha + \zeta^k \beta) \mathbb{Z}[\zeta] = (1 - \zeta)^{pm} \mathbb{Z}[\zeta] \cdot \gamma^p \mathbb{Z}[\zeta]. \quad (3.18)$$

On va d'abord montrer que $m \geq 2$. Supposons par l'absurde que $m = 1$. Puisque $1 - \zeta$ est premier d'après la proposition 2.1.33, l'égalité (3.17) nous dit que $1 - \zeta$ divise l'un des $\alpha + \zeta^k \beta$, or, $\alpha + \zeta^k \beta \equiv \alpha + \beta$ modulo $1 - \zeta$ pour tout $k \in \llbracket 0, p-1 \rrbracket$, donc $1 - \zeta$ divise tous les $\alpha + \zeta^k \beta$. Puisque $m = 1$ et que $\gamma \notin (1 - \zeta) \mathbb{Z}[\zeta]$, $1 - \zeta$ divise chaque $\alpha + \zeta^k \beta$ exactement une fois, c'est-à-dire que $(1 - \zeta)^2$ ne divise pas $\alpha + \zeta^k \beta$. Cela peut se réécrire comme $\alpha + \zeta^k \beta \not\equiv 0$ modulo $(1 - \zeta)^2$. Maintenant, on sait grâce à la preuve de la proposition 2.2.19 que $|(1 - \zeta) \mathbb{Z}[\zeta] / (1 - \zeta)^2 \mathbb{Z}[\zeta]| = p$, il y a donc exactement p multiples de $1 - \zeta$ modulo $(1 - \zeta)^2$ et donc $p - 1$ multiples non nuls modulo $(1 - \zeta)^2$. Il suit du principes des tiroirs qu'il existe $k, k' \in \llbracket 1, p-1 \rrbracket$ tels que $\alpha + \zeta^k \beta \equiv \alpha + \zeta^{k'} \beta$ modulo $(1 - \zeta)^2$. On trouve alors $(1 - \zeta^{k'-k})\beta = \zeta^k \beta - \zeta^{k'} \beta \equiv 0$ modulo $(1 - \zeta)^2$. D'après la proposition 2.1.38, $1 - \zeta^{k-k'}$ est associé à $1 - \zeta$ et donc $(1 - \zeta)\beta \equiv 0$ modulo $(1 - \zeta)^2$. Il en suit que $\beta \equiv 0$ modulo $1 - \zeta$, c'est-à-dire que $1 - \zeta$ divise β , ce qui contredit l'hypothèse. On en déduit que $m \geq 2$ et donc il existe $k \in \llbracket 1, p-1 \rrbracket$ tel que $(1 - \zeta)^2$ divise $\alpha + \zeta^k \beta$. De plus, notre dernier argument nous dit que ce k est unique.

Quitte à remplacer dans notre équation (3.16) β par $\zeta^k \beta$, on peut supposer que $k = 0$. Si on pose $I = \alpha \mathbb{Z}[\zeta] + \beta \mathbb{Z}[\zeta]$, on a que I et $(1 - \zeta) \mathbb{Z}[\zeta]$ sont relativement premiers car $\alpha \notin (1 - \zeta) \mathbb{Z}[\zeta]$ et $(1 - \zeta) \mathbb{Z}[\zeta]$ est maximal d'après la proposition 2.1.33. Ainsi, puisque $(1 - \zeta) \mathbb{Z}[\zeta]$ et I divisent $(\alpha + \zeta^k \beta) \mathbb{Z}[\zeta]$ pour tout $k \in \llbracket 0, p-1 \rrbracket$ alors $(1 - \zeta)I$ en est aussi un diviseur par la proposition 2.2.11. En particulier, il existe $S_k \leq \mathbb{Z}[\zeta]$ tel que $(1 - \zeta)IS_k = (\alpha + \zeta^k \beta) \mathbb{Z}[\zeta]$ pour tout $k \in \llbracket 1, p-1 \rrbracket$. Ainsi,

$$(1 - \zeta)^p I^p \prod_{k=0}^{p-1} S_k = \prod_{k=0}^{p-1} (\alpha + \zeta^k \beta) \mathbb{Z}[\zeta]. \quad (3.19)$$

et les S_k divisent $((1 - \zeta)^m \gamma \mathbb{Z}[\zeta])^p$ d'après (3.18). D'après le théorème 2.2.11, et que $1 - \zeta$ ne divise qu'une seule fois $\alpha + \zeta^k \beta$ pour $k \in \llbracket 1, p-1 \rrbracket$, on obtient qu'il existe des idéaux J_k non divisibles par $(1 - \zeta) \mathbb{Z}[\zeta]$ pour tout $k \in \llbracket 0, p-1 \rrbracket$ tels que

$$(\alpha + \beta) \mathbb{Z}[\zeta] = J_0^p I (1 - \zeta)^{mp-(p-1)} \quad (3.20)$$

$$\text{et } (\alpha + \zeta^k \beta) \mathbb{Z}[\zeta] = J_k^p I (1 - \zeta) \mathbb{Z}[\zeta] \text{ pour tout } k \in \llbracket 1, p-1 \rrbracket. \quad (3.21)$$

En divisant, on obtient l'équation d'idéaux fractionnaires suivante

$$\frac{\alpha + \zeta^k \beta}{\alpha + \beta} \mathbb{Z}[\zeta] = J_k^p J_0^{-p} \frac{1}{(1 - \zeta)^{p(m-1)}} \mathbb{Z}[\zeta]. \quad (3.22)$$

En multipliant par l'idéal fractionnaire $(1 - \zeta)^{p(m-1)} \mathbb{Z}[\zeta]$, on obtient que $J_k^p J_0^{-p} = (J_k J_0^{-1})^p$ est un idéal fractionnaire principal. Par le lemme 3.0.5, on a que $J_k J_0^{-1}$

est lui même principal, il existe donc $\eta_k \in \mathbb{Q}(\zeta)^*$ tel que $J_k J_0^{-1} = \eta_k \mathbb{Z}[\zeta]$. En outre, il existe $\varepsilon_k \in \mathbb{Z}[\zeta]$ tel que l'équation (3.22) d'idéaux fractionnaires donne l'équation suivante

$$\frac{\alpha + \zeta^k \beta}{\alpha + \beta} = \frac{\varepsilon_k \eta_k^p}{(1 - \zeta)^{p(m-1)}}. \quad (3.23)$$

Remarquons maintenant qu'on a l'équation

$$\zeta(\alpha + \zeta^{p-1} \beta) + (\alpha + \zeta \beta) - (1 + \zeta)(\alpha + \beta) = 0. \quad (3.24)$$

En divisant cette équation par $\alpha + \beta$, on obtient grâce à (3.23)

$$\zeta \frac{\alpha + \zeta^{p-1} \beta}{\alpha + \beta} + \frac{\alpha + \zeta \beta}{\alpha + \beta} - \frac{(1 + \zeta)(\alpha + \beta)}{\alpha + \beta} = 0 \quad (3.25)$$

$$\iff \frac{\zeta \varepsilon_{p-1} \eta_{p-1}^p}{(1 - \zeta)^{p(m-1)}} + \frac{\varepsilon_1 \eta_1^p}{(1 - \zeta)^{p(m-1)}} - (1 + \zeta) = 0 \quad (3.26)$$

$$\iff \zeta \varepsilon_{p-1} \eta_{p-1}^p + \varepsilon_1 \eta_1^p - (1 + \zeta)(1 - \zeta)^{p(m-1)} = 0. \quad (3.27)$$

Ensuite, on a $\eta_k = \frac{a'_k}{b'_k}$ avec $a'_k, b'_k \in \mathbb{Z}[\zeta]^*$, qui a la particularité que $1 - \zeta$ divise autant de fois a'_k que b'_k . En effet, on a $J_k J_0^{-1} = \eta_k \mathbb{Z}[\zeta] = a'_k \mathbb{Z}[\zeta] \frac{1}{b'_k} \mathbb{Z}[\zeta]$ qui nous donne l'équation d'idéaux entiers $b'_k J_k = a'_k J_0$. Si $1 - \zeta$ divise a'_k alors $b'_k J_k = a'_k J_0 \subset a'_k \mathbb{Z}[\zeta] \subset (1 - \zeta) \mathbb{Z}[\zeta]$, mais puisque $J_k \not\subset (1 - \zeta) \mathbb{Z}[\zeta]$, on a bien $b'_k \mathbb{Z}[\zeta] \subset (1 - \zeta) \mathbb{Z}[\zeta]$ par la proposition 2.2.4. Quitte à simplifier a'_k et b'_k par $1 - \zeta$, on trouve $\eta_k = \frac{a'_k \div (1 - \zeta)}{b'_k \div (1 - \zeta)}$, et on peut répéter l'argument afin de bien trouver que $1 - \zeta$ divise autant de fois a'_k que b'_k . On peut alors simplifier complètement la fraction des $1 - \zeta$ pour obtenir $\eta_k = \frac{a_k}{b_k}$ avec $1 - \zeta$ qui ne divise pas $a_k b_k$. Ainsi, en multipliant (3.27) par $\frac{b_1^p b_{p-1}^p}{\zeta \varepsilon_{p-1}}$, on obtient

$$(a_{p-1} b_1)^p + \frac{\varepsilon_1}{\zeta \varepsilon_{p-1}} (a_1 b_{p-1})^p - \frac{1 + \zeta}{\zeta \varepsilon_{p-1}} (1 - \zeta)^{p(m-1)} (b_1 b_{p-1})^p = 0. \quad (3.28)$$

Considérons cette équation modulo $p\mathbb{Z}[\zeta]$, par la proposition 2.2.30, p divise $(1 - \zeta)^p$. On a donc $(a_{p-1} b_1)^p + \frac{\varepsilon_1}{\zeta \varepsilon_{p-1}} (a_1 b_{p-1})^p \equiv 0$ modulo $p\mathbb{Z}[\zeta]$. Puisque $a_1 b_{p-1}$ est premier avec $1 - \zeta$, il suit de la proposition 2.2.30 que $a_1 b_{p-1}$ est inversible modulo $p\mathbb{Z}[\zeta]$. Soit $c \in \mathbb{Z}[\zeta]$ tel que $ca_1 b_{p-1} \equiv 1$ modulo $p\mathbb{Z}[\zeta]$, alors $c^p (a_1 b_{p-1})^p \equiv 1$ modulo $p\mathbb{Z}[\zeta]$ et donc

$$\frac{\varepsilon_1}{\zeta \varepsilon_{p-1}} \equiv -(a_{p-1} b_1 c)^p \text{ modulo } p\mathbb{Z}[\zeta]. \quad (3.29)$$

D'après le lemme 3.0.3, il existe un entier rationnel qui est congru à $-(a_{p-1}b_1c)^p$ modulo $p\mathbb{Z}[\zeta]$. En particulier, $\frac{\varepsilon_1}{\zeta\varepsilon_{p-1}}$ est aussi congru à un entier rationnel, et puisqu'il est inversible, le second lemme de Kummer 3.0.10 nous dit qu'il existe $\omega \in \mathbb{Z}[\zeta]^\times$ tel que $\frac{\varepsilon_1}{\zeta\varepsilon_{p-1}} = \omega^p$. Finalement, on peut réécrire (3.28) comme

$$(a_{p-1}b_1)^p + (\omega a_1b_{p-1})^p - \frac{1+\zeta}{\zeta\varepsilon_{p-1}}(1-\zeta)^{p(m-1)}(b_1b_{p-1})^p = 0, \quad (3.30)$$

mais $a_{p-1}b_1, \omega a_1b_{p-1}$ et b_1b_{p-1} ne sont pas divisibles par $1-\zeta$ car $a_1, a_{p-1}, b_1, b_{p-1}$ sont premiers avec $1-\zeta$ et ω est inversible. Aussi, la proposition 2.1.38 nous dit que $1+\zeta$ est inversible, et donc $-\frac{1+\zeta}{\zeta\varepsilon_{p-1}}$ l'est aussi. En conclusion, l'équation (3.30) est une équation du type (3.16) mais où l'on a remplacé m par $m-1$, or, $m \geq 2$ implique $m-1 \geq 1$, on a donc une contradiction par descente. □

Corollaire 3.0.13. *Soit $n \in \mathbb{N} \setminus \{0, 1, 2\}$, si un nombre premier régulier divise n , alors l'équation diophantienne $x^n + y^n = z^n$ n'admet aucune solution non triviale.*

Démonstration. Supposons par l'absurde qu'il existe une solution non triviale (a, b, c) . Soit p un nombre premier régulier qui divise n , il existe donc $m \in \mathbb{N}^*$ tel que $pm = n$. On obtient alors

$$x^n + y^n = z^n \iff x^{pm} + y^{pm} = z^{pm} \iff (x^m)^p + (y^m)^p = (z^m)^p,$$

ce qui contredit le théorème de Fermat–Kummer 3.0.12. □

Chapitre 4

Problème de conjugaison dans $\mathcal{M}_n(\mathbb{Z})$

Pour un entier algébrique α , on a que $\mathbb{Z}[\alpha]$ est un ordre de $\mathbb{Q}(\alpha)$. On a donc maintenant les outils pour attaquer le théorème de Latimer–MacDuffee.

Proposition 4.0.1. *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire irréductible de degré $n \geq 1$ et α une racine de ce polynôme. Soit $M \in \mathcal{M}_n(\mathbb{Z})$ ayant P pour polynôme caractéristique, le $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}^n$ peut être étendu en une structure de $\mathbb{Q}(\alpha)$ -espace vectoriel où le produit scalaire par α est donné par $\alpha \cdot v = Mv$ pour tout $v \in \mathbb{Q}^n$. De plus, sa dimension vaut 1.*

Démonstration. Le fait que ce produit scalaire est bien défini suit du théorème de Cayley–Hamilton.

Pour montrer que la dimension de cette espace vectoriel vaut 1, on utilise la formule des dimensions

$$n = \dim_{\mathbb{Q}}(\mathbb{Q}^n) = \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n) \times \dim_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n) \times n \implies \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n) = 1.$$

□

Théorème 4.0.2 (Latimer–MacDuffee). *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire irréductible de degré $n \geq 1$, il existe une bijection entre les classes de similitudes de matrices $n \times n$ entières ayant P comme polynôme caractéristique et les classes d'idéaux fractionnaires de $\mathbb{Z}[\alpha]$ où α est une racine de P .*

Démonstration. Soit I un idéal fractionnaire de $\mathbb{Z}[\alpha]$, on a que $m_\alpha : I \rightarrow I : x \mapsto \alpha x$ est un endomorphisme de $\mathbb{Z}$ -modules. Si on choisit une $\mathbb{Z}$ -base de I , on obtient une matrice $M \in \mathcal{M}_n(\mathbb{Z})$ représentant m_α . Ainsi, indépendamment du choix d'une $\mathbb{Z}$ -base, on peut associer à I la classe de similitude de M . Puisque le polynôme caractéristique d'une matrice est un invariant de similitude, on doit uniquement vérifier que P est le polynôme caractéristique de M . On a que $P(M) = 0_{\mathcal{M}}$ si et seulement si $P(m_\alpha) = 0$, mais $P(m_\alpha) = m_{P(\alpha)} = m_0 = 0$. Enfin, nous avons que si $I \sim J$, c'est-à-dire que $J = yI$ pour $y \in \mathbb{Q}(\alpha)^*$, alors notre processus associe à J la même classe de similitude qu'à I .

En effet, remarquons que si $(e_1, \dots, e_n)$ est une $\mathbb{Z}$ -base de I où M représente $m_\alpha : I \rightarrow I$, alors M représente $m'_\alpha : J \rightarrow J : x \mapsto \alpha x$ dans la $\mathbb{Z}$ -base $(ye_1, \dots, ye_n)$ de J . On obtient donc une fonction Ω bien définie, des classes d'idéaux fractionnaires de $\mathbb{Z}[\alpha]$ aux classes de similitudes de $\mathcal{M}_n(\mathbb{Z})$ ayant P comme polynôme caractéristique. Montrons alors que Ω est une bijection.

- Injectivité : soit I, J deux idéaux fractionnaires de $\mathbb{Z}[\alpha]$ ayant M et M' comme matrices représentant respectivement $m_\alpha : I \rightarrow I$ et $m'_\alpha : J \rightarrow J$ dans certaines $\mathbb{Z}$ -bases A et B , et supposons que M et M' sont semblables. On doit montrer que I et J sont dans la même classe d'équivalence. Soient $e_I : I \rightarrow \mathbb{Z}^n$ et $e_J : J \rightarrow \mathbb{Z}^n$ les isomorphismes de $\mathbb{Z}$ -modules envoyant respectivement A et B sur la base canonique de $\mathbb{Z}^n$. Le fait que M et M' représentent respectivement m_α et m'_α dans A et B se traduit par les diagrammes commutatifs de $\mathbb{Z}$ -modules suivants :

$$\begin{array}{ccc} I & \xrightarrow{e_I} & \mathbb{Z}^n \\ m_\alpha \downarrow & & \downarrow M \\ I & \xrightarrow{e_I} & \mathbb{Z}^n \end{array} \quad \begin{array}{ccc} J & \xrightarrow{e_J} & \mathbb{Z}^n \\ m'_\alpha \downarrow & & \downarrow M' \\ J & \xrightarrow{e_J} & \mathbb{Z}^n \end{array}$$

La similitude de M et M' nous dit qu'il existe $B \in \mathrm{GL}_n(\mathbb{Z})$ telle que $M'B = BM$, ce qui se traduit par le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{B} & \mathbb{Z}^n \\ M \downarrow & & \downarrow M' \\ \mathbb{Z}^n & \xrightarrow{B} & \mathbb{Z}^n \end{array}$$

En combinant ces 3 diagrammes, on obtient le diagramme commutatif

$$\begin{array}{ccccccc} I & \xrightarrow{e_I} & \mathbb{Z}^n & \xrightarrow{B} & \mathbb{Z}^n & \xrightarrow{e_J^{-1}} & J \\ m_\alpha \downarrow & & M \downarrow & & \downarrow M' & & \downarrow m'_\alpha \\ I & \xrightarrow{e_I} & \mathbb{Z}^n & \xrightarrow{B} & \mathbb{Z}^n & \xrightarrow{e_J^{-1}} & J \end{array}$$

On trouve alors en haut et en bas de ce diagramme un isomorphisme $I \rightarrow J$ de $\mathbb{Z}$ -modules, qui commute avec la multiplication par α , c'est donc un isomorphisme de $\mathbb{Z}[\alpha]$ -modules, ils sont donc équivalents par la proposition 2.4.5.

- Surjectivité : Soit $M \in \mathcal{M}_n(\mathbb{Z})$ tel que $P(M) = 0$, on cherche un idéal fractionnaire I de $\mathbb{Z}[\alpha]$ et une $\mathbb{Z}$ -base de I dans laquelle M représente l'endomorphisme $m_\alpha : I \rightarrow I$. D'après la proposition 4.0.1, $\mathbb{Q}^n$ peut être muni d'une structure de $\mathbb{Q}(\alpha)$ -espace vectoriel où le produit scalaire par α est défini comme $\alpha \cdot v = Mv$ pour tout $v \in \mathbb{Q}^n$. Ainsi, si $v \in \mathbb{Z}^n$, on a que $\alpha \cdot v \in \mathbb{Z}^n$ car $M \in \mathcal{M}_n(\mathbb{Z})$. Il en suit d'une part que $\mathbb{Z}^n$ est un $\mathbb{Z}[\alpha]$ -sous-module du $\mathbb{Z}[\alpha]$ -module $\mathbb{Q}^n$ de rang n . D'autre

part, le fait que $\alpha \cdot v = Mv$ pour tout $v \in \mathbb{Z}^n$ veut dire que l'endomorphisme $m_\alpha : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ est représenté par M dans la base canonique. Ensuite, remarquons que pour $v \in \mathbb{Q}^n$ un vecteur non nul, l'application $g_v : \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}^n : \beta \mapsto \beta \cdot v$ est $\mathbb{Q}(\alpha)$ -linéaire, mais puisque $\dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n) = 1$, on a que g_v est un isomorphisme car v est un vecteur non nul. On définit alors $I := g_v^{-1}(\mathbb{Z}^n)$ pour v un vecteur non nul fixé. C'est un $\mathbb{Z}[\alpha]$ -sous-module de $\mathbb{Q}(\alpha)$ de rang n car $\mathbb{Z}^n$ est un $\mathbb{Z}[\alpha]$ -sous-module du $\mathbb{Z}[\alpha]$ -module $\mathbb{Q}^n$ de rang n , c'est donc un idéal fractionnaire de $\mathbb{Z}[\alpha]$ d'après la proposition 2.3.2. Notons que la classe d'idéaux fractionnaires ainsi définie ne dépend pas du choix de v . En effet, pour $w \in \mathbb{Q}^n$ un autre vecteur non nul, puisque $\mathbb{Q}^n$ est un $\mathbb{Q}(\alpha)$ -espace vectoriel de dimension 1, il y a donc un automorphisme qui envoie w sur v et il est de la forme $u \mapsto y \cdot u$ pour un certain $y \in \mathbb{Q}(\alpha)$. Ainsi, $w = y \cdot v$ et donc $g_w^{-1}(\mathbb{Z}^n) = xI$. Finalement, puisque M représente $m_\alpha : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ dans la base canonique $\{e_1, \dots, e_n\}$, on a que M représente aussi $m_\alpha : I \rightarrow I$ dans la $\mathbb{Z}$ -base $\{g_v^{-1}(e_1), \dots, g_v^{-1}(e_n)\}$, ce qui conclut. $\square$

Exemple 4.0.3. • Il n'y a qu'une seule classe de conjugaison de matrices entières ayant pour polynôme caractéristique $X^2 - 3$ d'après le premier exemple de 2.3.37.

- D'après le troisième exemple de 2.3.37, on l'égalité suivante

$$\text{Pic}(\mathbb{Z}[\sqrt{-5}]) = \{[\mathbb{Z}[\sqrt{-5}]], [2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]]\}.$$

Donc d'après le théorème de Latimer–MacDuffee, il y a 2 classes de similitudes de matrices 2×2 ayant $X^2 + 5$ comme polynôme caractéristique. Pour trouver des représentants de ces classes, il faut regarder comment la multiplication par $\sqrt{-5}$ agit sur les bases des idéaux fractionnaires $\mathbb{Z}[\sqrt{-5}]$ et $2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$. Pour $\mathbb{Z}[\sqrt{-5}]$, on a $\sqrt{-5} \times 1 = 0 \times 1 + 1 \times \sqrt{-5}$ et $\sqrt{-5}\sqrt{-5} = -5 = -5 \times 1 + 0 \times \sqrt{-5}$. La matrice correspondante est alors donnée par

$$\begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}.$$

Maintenant pour $2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$, on a $\sqrt{-5} \times 2 = -1 \times 2 + 2 \times (1 + \sqrt{-5})$ et $\sqrt{-5}(1 + \sqrt{-5}) = -5 + \sqrt{-5} = -3 \times 2 + 1 \times (1 + \sqrt{-5})$. La matrice correspondante est alors donnée par

$$\begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix}.$$

Ensuite, si on a par exemple la matrice

$$\begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix}$$

qui a aussi $X^2 + 5$ comme polynôme caractéristique, on peut savoir à quelle classe de similitude elle appartient grâce à la preuve de la surjectivité dans 4.0.2. En considérant $\mathbb{Q}^2$ comme un $\mathbb{Q}(\sqrt{-5})$ -espace vectoriel comme dans la preuve, on obtient

$$(a + b\sqrt{-5}) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} := \left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + b \begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix} \right) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a + 2b \\ -3b \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

On cherche alors $g_v^{-1}(\mathbb{Z}^2)$ où $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. On a

$$\begin{aligned} g_v(a + b\sqrt{-5}) \in \mathbb{Z}^2 &\iff \begin{pmatrix} a \\ b \end{pmatrix} \in \begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix}^{-1} \mathbb{Z}^2 \\ &= \begin{pmatrix} 1 & \frac{2}{3} \\ 0 & -\frac{1}{3} \end{pmatrix} \mathbb{Z}^2 = \left\{ \begin{pmatrix} x + \frac{2}{3}y \\ -\frac{y}{3} \end{pmatrix} \mid x, y \in \mathbb{Z} \right\}. \end{aligned}$$

L'idéal fractionnaire correspondant à notre matrice a donc pour $\mathbb{Z}$ -base $(1, \frac{2-\sqrt{-5}}{3})$. On remarque en multipliant par 3, que cette idéal fractionnaire est équivalent à l'idéal entier $3\mathbb{Z}[\sqrt{-5}] + (2 - \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$. On a que $3 \notin (2 - \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ donc $3\mathbb{Z}[\sqrt{-5}] + (2 - \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ est un diviseur non trivial de $3\mathbb{Z}[\sqrt{-5}]$. D'après le théorème de Dedekind–Kummer 2.2.28, on a que 3 est totalement décomposé car $X^2 + 5 \equiv X^2 - 1 = (X - 1)(X + 1) \pmod{3}$. On a donc que $3\mathbb{Z}[\sqrt{-5}] + (2 - \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ est un idéal premier au-dessus de 3 et est donc ici de norme 3. Cet idéal n'est pas principal car l'équation diophantienne $a^2 + 5b^2 = \pm 3$ n'admet pas de solutions. On en conclut que

$$\begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix}$$

est conjugué à

$$\begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix}.$$

- D'après l'exemple fournit par 2.4.39, on a deux classes de conjugaison de matrices entières ayant pour polynôme caractéristique $X^2 - 13$. Comme précédemment, la matrice correspondant à l'idéal fractionnaire $\mathbb{Z}[\sqrt{13}]$ via le théorème de Latimer–MacDuffee 4.0.2 est la matrice compagnon de $X^2 + 13$. Pour ce qui est de l'idéal fractionnaire $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, on obtient en faisant le même processus que le point précédent (regarder où est envoyée sa $\mathbb{Z}$ -base quand on multiplie par $\sqrt{13}$) la matrice suivante

$$\begin{pmatrix} -1 & 6 \\ 2 & 1 \end{pmatrix}.$$

Bibliographie

- [1] Z. I. Borevich and I. R. Shafarevich, *Théorie des nombres*, translated from the Russian by Myriam Verley and Jean-Luc Verley Reprint of the 1967 French translation, Les Grands Classiques Gauthier-Villars, Éd. Jacques Gabay, Sceaux, 1993 ; MR1355542
- [2] J. W. Cannon, Max Dehn and the word problem, in *Max Dehn—polyphonic portrait*, 167–180, Hist. Math., 46, Amer. Math. Soc., Providence, RI, ; MR4813449
- [3] P-E Caprace, Théorie de Galois, LMAT1361
- [4] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138, Springer, Berlin, 1993 ; MR1228206
- [5] K. Conrad, Fermat’s last theorem for regular primes, Expository Papers
- [6] K. Conrad, Ideal classes and matrix conjugation over $\mathbf{Z}$, Expository Papers
- [7] K. Conrad, Kummer’s lemma, Expository Papers
- [8] K. Conrad, The conductor ideal of an order, Expository Papers
- [9] D. A. Cox, *Primes of the form $x^2 + ny^2$* , A Wiley-Interscience Publication, Wiley, New York, 1989 ; MR1028322
- [10] H. M. Edwards, *Fermat’s last theorem*, corrected reprint of the 1977 original, Graduate Texts in Mathematics, 50, Springer, New York, 1996 ; MR1416327
- [11] B. Eick, T. Hofmann and E. A. O’Brien, The conjugacy problem in $\mathrm{GL}(n, \mathbb{Z})$, J. Lond. Math. Soc. (2) **100** (2019), no. 3, 731–756 ; MR4048718
- [12] F. J. Grunewald, Solution of the conjugacy problem in certain arithmetic groups, in *Word problems, II (Conf. on Decision Problems in Algebra, Oxford, 1976)*, pp. 101–139, Stud. Logic Found. Math., 95, North-Holland, Amsterdam-New York, ; MR0579942
- [13] C. G. Latimer and C. C. MacDuffee, A correspondence between classes of ideals and classes of matrices, Ann. of Math. (2) **34** (1933), no. 2, 313–316 ; MR1503108
- [14] S. Mac Lane and G. Birkhoff, *Algèbre*, translated from the 1965 English edition and with a foreword by J. Weil Reprint of the French editions, published 1970–1973, Les Grands Classiques Gauthier-Villars, Éd. Jacques Gabay, Paris, 1996 ; MR1452598
- [15] S. Marseglia, Computing the ideal class monoid of an order, J. Lond. Math. Soc. (2) **101** (2020), no. 3, 984–1007 ; MR4111932
- [16] J. Neukirch, *Algebraic number theory*, translated from the 1992 German original and with a note by Norbert Schappacher, Grundlehren der mathematischen Wissenschaften, 322, Springer, Berlin, 1999 ; MR1697859

- [17] P. S. Novikov, Unsolvability of the conjugacy problem in the theory of groups, *Izv. Akad. Nauk SSSR Ser. Mat.* **18** (1954), 485–524 ; MR0075196
- [18] H. Olbermann, *Analyse mathématique : intégration*, LMAT1221
- [19] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 1967 ; MR0215808
- [20] P. F. Stebe, Conjugacy separability of groups of integer matrices, *Proc. Amer. Math. Soc.* **32** (1972), 1–7 ; MR0289666
- [21] I. N. Stewart and D. Tall, *Algebraic number theory and Fermat’s last theorem*, fourth edition, CRC Press, Boca Raton, FL, 2016 ; MR3443702
- [22] O. Taussky-Todd, On a theorem of Latimer and MacDuffee, *Canad. J. Math.* **1** (1949), 300–302 ; MR0030491
- [23] E. Vitale, *Algèbre commutative*, LMAT1331

UNIVERSITÉ CATHOLIQUE DE LOUVAIN

Faculté des sciences

Place des sciences, 2 bte L6.06.01, 1348 Louvain-la-Neuve, Belgique | www.uclouvain.be/sc