Rapport de stage de M1

Timothée Defourné

31 août 2022

1 Déroulé du stage

Mon stage s'est déroulé en distanciel à l'université de Lille, de février à juin 2022, sous l'encadrement de Julien Hauseux. Je travaillais la semaine en distanciel et me rendais à Lille une fois par semaine, le jeudi, afin de discuter de mon avancement avec Julien. J'ai également suivi le séminaire d'arithmétique qui se déroulait le jeudi matin au laboratoire.

Je tiens avant tout à remercier Julien pour son accueil et son encadrement, malgré les difficultés rencontrées pendant le stage et notamment l'écriture du rapport, comme expliqué ci-dessous.

2 Sujet du stage et difficultés

Le sujet du stage, tel qu'il était noté dans la convention de stage, était volontairement assez vague : « Formes quadratiques et Théorie des nombres ». L'idée était de m'introduire dans un premier temps à ces deux domaines et de démontrer le théorème de Hasse-Minkowski, puis de décider au milieu du stage de la direction à prendre en fonction de ce qui m'intéressait. Malheureusement, cette deuxième partie n'a pas vraiment eu lieu.

Mon stage a donc principalement consisté en de la lecture bibliographique, sans qu'un contenu final ne soit produit et sans qu'une ligne directrice ne soit clairement établie. J'ai notamment lu des références sur la théorie des nombres, les nombres p-adiques (que je ne connaissais précédemment que de nom), les formes quadratiques, et la démonstration du sus-cité théorème de Hasse-Minkowski dans $\mathbb{Q}$. Les principales références utilisées sont notées à la fin de ce document.

A la fin de mon stage, l'idée que Julien et moi avons eu pour l'écriture du rapport était d'essayer d'étendre la démonstration de Hasse-Minkowski de Jean-Pierre Serre [2] aux corps de nombres, si besoin en admettant certains des résultats intermédiaires. Il m'a semblé au départ que cette preuve se généraliserait facilement en admettant les cas des formes de rang 2 et 3, ce qui est la décision prise dans [5]. Cependant, après de nombreux retards pendant l'écriture du rapport, j'ai finalement réalisé que la preuve ne pouvait pas se généraliser simplement, à moins d'admettre plus de résultats intermédiaires ou d'introduire d'autres concepts (notamment les algèbres de quaternions) que je n'ai pas du tout étudiés durant mon stage.

Réalisant que mon rapport contenait déjà beaucoup de travail qui n'a dans les faits pas été réalisé pendant le stage, et étant déjà en retard dans sa rédaction, il m'a semblé impossible de présenter le théorème tel que prévu initialement sans tomber dans la malhonnêteté et sans augmenter encore plus mon retard. J'ai considéré l'idée de ne présenter le théorème que dans le

cas de $\mathbb{Q}$, mais tout le travail sur les extensions de corps effectué au cours de mon stage aurait alors été inutile, et mon rapport n'aurait été qu'un simple recopiage des 4 premiers chapitres de [2].

J'ai finalement décidé d'abandonner la production de mon rapport et d'écrire à la place ces quelques paragraphes détaillant les difficultés que j'ai rencontrées.

Je tiens à m'excuser profondément pour la gêne occasionnée par mon retard et pour l'absence d'un réel compte-rendu de stage. La suite de ce document contient le rapport que j'avais commencé à rédiger, afin de fournir une preuve du travail effectué pendant ces derniers mois. Comme expliqué précédemment, ce rapport n'est pas fini ; il n'a en particulier pas été relu, manque de mise en page, dépasse la limite de pages demandée, et s'arrête abruptement au milieu d'une preuve.

3 Contenu du stage

3.1 Valeurs absolues sur un corps

Dans cette section, nous parlons rapidement du concept de valeurs absolues sur un corps, notamment afin de présenter le théorème d'Ostrowski, et le théorème d'approximation, qui sera utile dans les parties suivantes. Les résultats présentés ici étant assez classiques, la plupart ne seront pas démontrés, à l'exception des deux précédemment cités. Cette section est principalement basée sur [1].

3.1.1 Valeurs absolues archimédiennes, non archimédiennes

Définition 1. *Étant donné un corps $\mathbb{K}$, une valeur absolue sur $\mathbb{K}$ est une fonction $|\cdot| : \mathbb{K} \to \mathbb{R}$ vérifiant les axiomes suivants :*

1. $\forall x \in \mathbb{K}$, $|x| \geq 0$
2. $\forall x \in \mathbb{K}$, $|x| = 0 \iff x = 0$
3. $\forall x, y \in \mathbb{K}$, $|xy| = |x|\,|y|$
4. $\forall x, y \in \mathbb{K}$, $|x + y| \leq |x| + |y|$

On peut sans problème montrer des résultats préliminaires sur les valeurs absolues. En voici quelques-uns :

i. $\forall x \neq 0$, $|x^{-1}| = |x|^{-1}$
ii. $|1| = 1$
iii. Si x est une racine de l'unité, $|x| = 1$
iv. $\forall x \in \mathbb{K}$, $|-x| = |x|$

De plus, un corps $\mathbb{K}$ peut être vu comme un $\mathbb{K}$-espace vectoriel de dimension 1, et une valeur absolue sera en particulier une norme sur $\mathbb{K}$. Tous les résultats sur les normes s'appliquent donc aux valeurs absolues.

L'exemple le plus connu de valeur absolue est la valeur absolue usuelle sur $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ (plus généralement, sur n'importe quel sous-corps de $\mathbb{C}$). On peut également définir, pour un corps $\mathbb{K}$ quelconque, la valeur absolue triviale, définie par $|x| = 1$ si $x \neq 0$ et $|0| = 0$. Comme son nom l'indique, cette valeur absolue n'est pas très intéressante. Si $\mathbb{K}$ est un corps fini, tout élément non nul est une racine de l'unité, et par conséquent la seule valeur absolue possible est la valeur absolue triviale.

Cependant, il existe d'autres valeurs absolues, telle que la valeur absolue p-adique sur $\mathbb{Q}$:

Définition 2. *Soit p un nombre premier. On note v_p la valuation p-adique sur $\mathbb{Z}$, que l'on étend à $\mathbb{Q}$ par la formule :*

$$\forall x \in \mathbb{Z},\ y \in \mathbb{Z}^\star,\ v_p\left(\frac{x}{y}\right) \widehat{=} v_p(x) - v_p(y)$$

On montre aisément que cette définition est indépendante du choix de x et y. On définit alors la valeur absolue p-adique sur $\mathbb{Q}$:

$$\forall x \in \mathbb{Q},\ |x|_p \widehat{=} p^{-v_p(x)}$$

Par convention, $v_p(0) = -\infty$, de sorte que $|0|_p = 0$

Cette fonction est une valeur absolue sur $\mathbb{Q}$, différente de la valeur absolue usuelle. Avec cette valeur absolue, un élément de $\mathbb{Q}$ est "petit" lorsqu'il est divisible par p. Elle vérifie de plus une inégalité plus forte que l'inégalité triangulaire usuelle, appelée l'inégalité ultramétrique :

$$\forall x, y \in \mathbb{Q},\ |x+y|_p \leq \max\left(|x|_p, |y|_p\right)$$

Définition 3. *On dit qu'une valeur absolue est non-archimédienne, ou ultramétrique, si elle vérifie l'inégalité ultramétrique :*

4.b. $\forall x, y \in \mathbb{K},\ |x+y| \leq \max\left(|x|, |y|\right)$

Sinon, on dit que la valeur absolue est archimédienne.

Les valeurs absolues non-archimédiennes ont des propriétés assez intéressantes. Par exemple, dans un corps muni d'une telle valeur absolue, *tous les triangles sont isocèles.* On a en effet :

$$\forall x, y \in \mathbb{K} \text{ tels que } |x| \neq |y|,\ |x+y| = \max\left(|x|, |y|\right)$$

Notons quelques caractérisations utiles des valeurs absolues non-archimédiennes :

Propriété 1. *Soit $\mathbb{K}$ un corps, et $|\cdot|$ une valeur absolue sur $\mathbb{K}$. Alors les assertions suivantes sont équivalentes :*

1. $|\cdot|$ *est non-archimédienne*
2. $\forall x \in \mathbb{Z},\ |x| \leq 1$
3. $\sup\limits_{x \in \mathbb{Z}} |x| < +\infty$
4. $\forall x \in \mathbb{K},\ |x+1| \leq \max\left(|x|, 1\right)$

Où la notation $\mathbb{Z}$ désigne abusivement l'image dans $\mathbb{K}$ de l'unique morphisme d'anneaux $\mathbb{Z} \to \mathbb{K}$.

Démonstration. Les implications $1 \Rightarrow 2$, $2 \Rightarrow 3$, et $4 \Rightarrow 1$ sont triviales. Montrons l'implication $3 \Rightarrow 4$.

Supposons qu'il existe une constante $C > 0$ telle que $\forall x \in \mathbb{Z},\ |x| \leq C$. On a alors, pour tout $x \in \mathbb{K}$ et pour tout $n \in \mathbb{N}$,

$$\begin{aligned}
|x+1|^n &= \left|\sum_{k=0}^{n} \binom{n}{k} x^k\right| \\
&\leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| |x|^k \\
&\leq C \sum_{k=0}^{n} |x|^k \\
&\leq C(n+1)\max\left(|x|^n, 1\right) \\
\text{D'où } |x+1| &\leq \left(C(n+1)\right)^{\frac{1}{n}} \max\left(|x|, 1\right)
\end{aligned}$$

Or $\left(C(n+1)\right)^{\frac{1}{n}} \underset{n \to +\infty}{\longrightarrow} 1$, d'où le résultat souhaité. □

Terminons avec quelques notions supplémentaires sur les valeurs absolues non-archimédiennes, qui nous seront utiles par la suite :

Définition 4. *Soit $|\cdot|$ une valeur absolue non-archimédienne sur $\mathbb{K}$. On définit :*

1. *L'anneau de valuation de $|\cdot|$: $\mathcal{O} = \{x \in \mathbb{K}, |x| \leq 1\}$*
   C'est un sous-anneau de $\mathbb{K}$, et un anneau local.
2. *L'idéal de valuation de $|\cdot|$: $\mathfrak{P} = \{x \in \mathbb{K}, |x| < 1\}$*
   l'unique idéal maximal de $\mathcal{O}$
3. *Le corps résiduel de $|\cdot|$: $\kappa = \mathcal{O}/\mathfrak{P}$*

Le fait que $\mathcal{O}$ soit un sous-anneau de $\mathbb{K}$ et que $\mathfrak{P}$ soit un idéal de $\mathcal{O}$ se vérifient sans difficulté. Pour montrer que $\mathcal{O}$ est un anneau local dont l'idéal maximal est $\mathfrak{P}$, il suffit de constater que tout élément $x \in \mathcal{O} - \mathfrak{P}$ est inversible (en effet, sa valeur absolue vaut 1, donc son inverse dans $\mathbb{K}$ appartient à $\mathcal{O}$)

3.1.2 Valeurs absolues équivalentes, théorème d'Ostrowski

Nous connaissons deux types de valeurs absolues non-triviales sur $\mathbb{Q}$: la valeur absolue usuelle, que l'on notera $|\cdot|_\infty$, et pour tout nombre premier p, la valeur absolue p-adique $|\cdot|_p$. Le théorème d'Ostrowski affirme que ces valeurs absolues sont les seules possibles, à équivalence près. Précisons ce que l'on entend par "équivalence" :

Définition 5. *Deux valeurs absolues sur un corps $\mathbb{K}$ sont dites* équivalentes *si elles définissent la même topologie sur $\mathbb{K}$. C'est une relation d'équivalence.*

On appelle place *de $\mathbb{K}$ une classe d'équivalence de valeurs absolues. On dénote souvent par Ω l'ensemble des places de $\mathbb{K}$.*

Propriété 2. *Soit $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur un corps $\mathbb{K}$. Les assertions suivantes sont équivalentes :*

1. *$|\cdot|_1$ et $|\cdot|_2$ sont équivalentes.*
2. *$\forall x \in \mathbb{K}$, $|x|_1 < 1 \iff |x|_2 < 1$*
3. *$\exists \alpha > 0$ tel que $\forall x \in \mathbb{K}$, $|x|_1 = |x|_2^\alpha$*

Une preuve de cette propriété est disponible dans [1].

D'après la deuxième caractérisation, et la propriété 1, on montre aisément qu'une valeur absolue archimédienne et une valeur absolue non-archimédienne ne peuvent pas être équivalentes. Il est également clair que si p et q sont deux nombres premiers distincts, les valeurs absolues p-adiques et q-adiques ne sont pas équivalentes.

Dans le $\mathbb{Q}$, on sait donc que les places des valeurs absolues $|\cdot|_\infty$ et $|\cdot|_p$ sont deux à deux distinctes. Le théorème d'Ostrowski assure que ce sont les seules.

Théorème 1 (Ostrowski)**.** *Toute valeur absolue non-triviale sur $\mathbb{Q}$ est équivalente à $|\cdot|_\infty$ ou à l'une des $|\cdot|_p$.*

On note donc l'ensemble des places de $\mathbb{Q}$:

$$\Omega = \{1, 2, 3, 5, 7, 11, \ldots, \infty\}$$

Une preuve de ce théorème est également disponible dans [1]. On montrera cependant plus loin une généralisation du cas non-archimédien pour un corps de nombres quelconques.

3.1.3 Complétion d'un corps valué

Définition 6. *Soit $\mathbb{K}$ un corps, et $|\cdot|$ une valeur absolue sur $\mathbb{K}$. On dit qu'une suite $(u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ est une suite de Cauchy si :*

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N},\ \forall n, m \geq N,\ |u_n - u_m| \leq \epsilon$$

Pour une place $\mathfrak{p} \in \Omega$ donnée, cette définition ne dépend pas du choix du représentant de $\mathfrak{p}$. On peut donc définir le complété de $\mathbb{K}$ pour une place donnée.

Définition 7. *Soit $\mathfrak{p}$ une place de $\mathbb{K}$. On définit la relation d'équivalence $\mathcal{R}$ sur les suites de Cauchy de $\mathbb{K}$:*

$$u\,\mathcal{R}\,v \iff (u_n - v_n) \underset{n\to+\infty}{\longrightarrow} 0$$

On définit ensuite le complété de $\mathbb{K}$ en $\mathfrak{p}$:

$$\mathbb{K}_\mathfrak{p} \widehat{=} \{\textit{suites de Cauchy de } \mathbb{K}\}_{/\mathcal{R}}$$

On a une inclusion canonique $\mathbb{K} \hookrightarrow \mathbb{K}_\mathfrak{p}$ donnée par les suites constantes.

Pour $|\cdot| \in \mathfrak{p}$, on peut étendre $|\cdot|$ aux suites de Cauchy de $\mathbb{K}$ par $|(u_n)_{n\in\mathbb{N}}| = \lim\limits_{n\to\infty} |u_n|$. On peut vérifier que cette définition passe au quotient par $\mathcal{R}$, de même que l'addition et la multiplication terme à terme. Ces opérations font de $K_\mathfrak{p}$ une extension de corps de $\mathbb{K}$, dont $|\cdot|$ est une valeur absolue.

$(\mathbb{K}_\mathfrak{p}, |\cdot|)$ est la plus petite extension de corps de $(\mathbb{K}, |\cdot|)$ complète. De plus, $\mathbb{K}$ est dense dans $\mathbb{K}_\mathfrak{p}$, par construction.

Dans le cas de $\mathbb{Q}$, pour $\mathfrak{p} = \infty$, on reconnaît la construction canonique de l'ensemble des nombres réels : $\mathbb{Q}_\infty = \mathbb{R}$. Pour $\mathfrak{p} = p$ un nombre premier, $\mathbb{Q}_p$ est le corps des nombres p-adiques. Nous en avons donné une construction analytique, mais il est possible d'en donner une description plus algébrique. En effet, tout nombre p-adique peut s'écrire d'une unique façon sous la forme

$$x = \sum_{i=k}^{\infty} a_i p^i \qquad \text{avec } k \in \mathbb{Z},\ \forall i \geq k,\ a_i \in [\![0\,;\,p-1]\!],\ \text{et } a_k \neq 0$$

Cette notation a du sens car $|p|_p < 1$. Comme $\mathbb{Q}_p$ est complet, on peut donc en déduire que la série $\sum\limits_{i=k}^{\infty} a_i p^i$ converge.

3.1.4 Lemme d'approximation

On a vu que si $\mathbb{K}$ est un corps et $\mathfrak{p}$ une place de $\mathbb{K}$, alors $\mathbb{K}$ est dense dans $\mathbb{K}_\mathfrak{p}$. En réalité, il existe un résultat plus général : pour tout ensemble fini S de places de $\mathbb{K}$, $\mathbb{K}$ est dense dans $\prod\limits_{\mathfrak{p}\in S} \mathbb{K}_\mathfrak{p}$.

Ce résultat peut être montré directement pour $\mathbb{Q}$ grâce au théorème des restes chinois (une telle démonstration est proposée dans [2]), mais nous allons ici montrer sa version générale.

Propriété 3. *Soit $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolue sur $\mathbb{K}$ non triviales, telles que pour tout $x \in \mathbb{K}$,*

$$|x|_1 < 1 \Rightarrow |x|_2 < 1$$

Alors $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes.

Démonstration. Par passage à l'inverse, on a $|x|_1 > 1 \Rightarrow |x|_2 \geq 1$. On souhaite désormais montrer que $|x|_1 = 1 \Rightarrow |x|_2 = 1$, afin d'obtenir par contraposée $|x|_2 < 1 \Rightarrow |x|_1 < 1$. Il suffira alors d'utiliser la propriété 2 pour montrer que les valeurs absolues sont équivalentes.

Soit $x \in \mathbb{K}$ tel que $|x|_1 = 1$. Comme $|\cdot|_1$ est non triviale, il existe un élément x_0 tel que $|x_0| < 1$. On a alors, pour tout $n \in \mathbb{N}$,

$$\begin{aligned} & |x^n x_0|_1 < 1 \\ \text{Donc} \quad & |x^n x_0|_2 < 1 \\ \text{Donc} \quad & |x|_2^n \, |x_0|_2 < 1 \\ \text{Donc} \quad & |x|_2 \leq 1, \text{ en faisant tendre } n \text{ vers } +\infty \end{aligned}$$

En passant à l'inverse, on a également $|x^{-1}|_2 \leq 1$, d'où finalement $|x|_2 = 1$, ce qui conclut la preuve.

□

Propriété 4. *Soit $n \geq 2$ et $|\cdot|_1, \ldots |\cdot|_n$ des valeurs absolues sur $\mathbb{K}$ non triviales et 2 à 2 non-équivalentes. Alors il existe un élément $x \in \mathbb{K}$ tel que*

$$|x|_1 > 1 \text{ et } \forall 2 \leq i \leq n, \, |x|_i < 1$$

Démonstration. On procède par récurrence sur n.

Supposons d'abord que $n = 2$. Par la propriété précédente, il existe des éléments x et y dans $\mathbb{K}$ tels que $|x|_1 < 1, |x|_2 \geq 1$, $|y|_2 < 1$ et $|y|_1 \geq 1$. $\dfrac{y}{x}$ répond alors a la propriété.

Supposons maintenant le résultat prouvé jusqu'au rang n, et montrons-le au rang $n+1$.

On sait par hypothèse de récurrence qu'il existe $x \in \mathbb{K}$ tels que $|x|_1 > 1$, $|x|_i < 1$ pour tout $2 \leq i \leq n$. Si $|x|_{n+1} < 1$, il n'y a rien à faire. Sinon, on considère un élément y tel que $|y|_1 > 1$ et $|y|_{n+1} < 1$.

Si $|x|_{n+1} = 1$, alors pour tout $1 \leq i \leq n$, $|x^k \, y|_i \to 0$, et $|x^k \, y|_{n+1} > 1$. Donc pour une valeur de k suffisamment grande, $x^k \, y$ convient.

Enfin, si $|x|_{n+1} > 1$, on considère cette fois les éléments du type

$$a_k = \frac{x^k \, y}{1 + x^k}$$

On remarque que $|a_k|_i \to 0$ si $|x|_i < 1$ (c'est-à-dire $2 \leq i \leq n$) et $|a_k|_i \to |y|_i$ si $|x|_i > 1$ (c'est-à-dire $i = 1$ ou $n+1$). Par conséquent, a_k convient pour une valeur de k suffisamment grande □

Cette propriété nous permet de « séparer »les valeurs absolues en trouvant des éléments dont la valeur absolue est inférieure strictement à 1 pour une et une seule valeur absolue. Cela nous permet d'avoir un résultat plus fort, parfois appelé le théorème d'approximation faible :

Théorème 2. *Théorème d'approximation faible*

Soit $n \in \mathbb{N}$ et $n \geq 2$ et $|\cdot|_1, \ldots |\cdot|_n$ des valeurs absolues sur $\mathbb{K}$ non triviales et 2 à 2 non équivalentes. Soit $(x_i)_{1 \leq i \leq n}$ une famille d'éléments de $\mathbb{K}$.

Alors pour tout $\varepsilon > 0$, il existe un élément $y \in \mathbb{K}$ tel que

$$\forall 1 \leq i \leq n,\ |y - x_i|_i < \varepsilon$$

Démonstration. On réutilise la même astuce que dans la démonstration précédente, en remarquant que si $|x| \neq 1$, la suite $\dfrac{x^n}{1+x^n}$ tend vers 0 si $|x| < 1$ et vers 1 si $|x| > 1$

Pour tout $1 \leq i \leq n$, on fixe un élément a_i tel que $|a_i|_i > 1$ et $|a_i|_j < 1$ pour tout $j \neq i$. On considère alors la suite

$$y_k = \sum_{i=1}^{n} \frac{x_i a_i^k}{1 + a_i^k}$$

On vérifie immédiatement que y_k tend vers x_i pour la normale $|\cdot|_i$. Donc pour une valeur de k suffisamment grande, y_k convient. □

Le lemme d'approximation dont nous avons parlé en début de section n'est qu'une reformulation de ce théorème.

Propriété 5. *Lemme d'approximation*

Soit $\mathbb{K}$ un corps et S un ensemble fini de places non triviales de $\mathbb{K}$. On considère le produit $\prod_{\mathfrak{p} \in S} \mathbb{K}_\mathfrak{p}$, que l'on munit de la topologie produit. Alors l'inclusion canonique $\mathbb{K} \hookrightarrow \prod_{\mathfrak{p} \in S} \mathbb{K}_\mathfrak{p}$ est dense.

Démonstration. Fixons pour tout $\mathfrak{p} \in S$ une valeur absolue $|\cdot|_\mathfrak{p}$ représentant $\mathfrak{p}$.

$\prod_{\mathfrak{p} \in S} \mathbb{K}_\mathfrak{p}$ est un $\mathbb{K}$-espace vectoriel, et sa topologie est équivalente à celle induite par la norme $\|(x_\mathfrak{p})\| = \max\left(|x_\mathfrak{p}|_\mathfrak{p}\right)$

Soit $x = (x_\mathfrak{p}) \in \prod_{\mathfrak{p} \in S} \mathbb{K}_\mathfrak{p}$, et soit $\varepsilon > 0$. On pose $\varepsilon' = \varepsilon/2$.

Comme $\mathbb{K}$ est dense dans chacun des $\mathbb{K}_\mathfrak{p}$, il existe pour tout $\mathfrak{p} \in S$ un élément $y_\mathfrak{p} \in \mathbb{K}$ tel que $|y_\mathfrak{p} - x_\mathfrak{p}|_\mathfrak{p} < \varepsilon'$. Par le théorème d'approximation faible, il existe un $y \in \mathbb{K}$ tel que $\forall \mathfrak{p} \in S,\ |y - y_\mathfrak{p}| < \varepsilon'$.

On a alors $\|y - x\| < \varepsilon$, ce qui achève la preuve. □

3.2 Corps de nombres

Dans cette partie, nous allons rappeler des propriétés générales sur les éléments entiers d'un anneau, puis plus particulièrement sur les *corps de nombres*, c'est-à-dire les extensions de corps de $\mathbb{Q}$ de degré fini. Cela nous permettra ensuite d'énoncer une version plus générale du théorème d'Ostrowski sur les corps de nombres.

3.2.1 Éléments entiers sur un anneau

Définition 8. *Soit B un anneau, A un sous-anneau de B, et $x \in B$. Les assertions suivantes sont équivalentes :*

1. *x admet une équation de dépendance intégrale, c'est-à-dire qu'il existe un entier $n \in \mathbb{N}$ et des éléments $a_0, a_1, \ldots, a_{n-1} \in A$ tels que :*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

2. *$A[x]$ est un A-module de type fini*

3. *Il existe un sous-anneau $A' \subset B$ contenant A et x, qui soit un A-module de type fini.*

Dans ce cas, on dit que x est entier sur A.

Définition 9. *Soit B un anneau, et A un sous-anneau de B. On appelle* fermeture intégrale de A dans B *l'ensemble des éléments de B entiers sur A. Cet ensemble est un sous-anneau de B, contenant A.*

Si $B = \mathbb{K}$ est le corps des fractions de A, on appelle clotûre intégrale de A *sa fermeture intégrale dans $\mathbb{K}$. On dit que A est* intégralement clos *s'il est intègre et si sa fermeture intégrale est A lui-même.*

Propriété 6. *Si A est un anneau principal, il est intégralement clos. En particulier, $\mathbb{Z}$ est intégralement clos.*

Démonstration. Soit A un anneau principal, et $\mathbb{K}$ son corps de fractions. A est en particulier intègre. Soit x un élément de $\mathbb{K}$ entier sur A. On peut écrire x sous la forme $x = \frac{a}{b}$ avec $a, b \in A$ premiers entre eux.

On a une équation de dépendance intégrale :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$
$$\text{D'où} \quad a^n + b\left(a_{n-1}a^{n-1} + \cdots + a_1 b^{n-2}a + a_0 b^{n-1}\right) = 0$$

On en déduit que $b \mid a^n$. Comme a et b sont premiers entre eux, on a alors $b \mid a$, et donc $x \in A$, ce qui conclut la preuve. □

Propriété 7. *(Transitivité) Soit C un anneau, B un sous-anneau de C et A un sous-anneau de B. On suppose que tous les éléments de B sont entiers sur A. Alors si $x \in C$ est entier sur B, il est entier sur A.*

Démonstration. On considère une équation de dépendance intégrale :

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0$$

On considère également $B' = A[b_0, b_1, \ldots, b_{n-1}] \subseteq B$. x est entier sur B', donc $B'[x]$ est un B'-module de type fini. Or les b_i étant chacun entiers sur A et étant en nombre fini, B' est lui-même un A-module de type fini. Donc $B'[x]$ est un A-module de type fini, et donc x est entier sur A. □

Lemme 1. *Soit B un anneau intègre, et A un sous-anneau de B tel que tous les éléments de B soient entiers sur A. On suppose que A est un corps. Alors B est un corps.*

Démonstration. Soit $x \in B$. On considère une équation de dépendance intégrale de x de degré minimal :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Si $a_0 = 0$, alors, comme B est intègre et $x \neq 0$, on a $x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1 = 0$, ce qui contredit la minimalité de n. Donc $a_0 \neq 0$. Quitte à multiplier les coefficients par $-a_0^{-1}$, on peut alors réécrire la relation :

$$\begin{aligned} a'_n x^n + a'_{n-1}x^{n-1} + \cdots + a'_1 x - 1 = 0 \\ \text{D'où } \; x\left(a_n x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1\right) = 1 \end{aligned}$$

Donc x est inversible dans B. □

3.2.2 Extensions algébriques d'un corps

Si $\mathbb{K}$ est un corps, et A un anneau contenant $\mathbb{K}$, un élément x de A est dit algébrique s'il existe un polynôme $P \in \mathbb{K}[X]$ non nul tel que $P(x) = 0$. Comme $\mathbb{K}$ est un corps, cette notion est équivalente à celle d'élément entier sur $\mathbb{K}$.

Définition 10. *Soit $\mathbb{K}'$ une extension de corps de $\mathbb{K}$. On dit que $\mathbb{K}'$ est une extension algébrique de $\mathbb{K}$ si tous les éléments de $\mathbb{K}'$ sont algébriques.*

Si x est algébrique, alors il existe un unique polynôme non nul unitaire de degré minimal tel que $P(x) = 0$. En effet, on considère le morphisme $\varphi : \mathbb{K}[X] \to A$ tel que $\varphi(X) = x$. Le noyau de ce morphisme est non nul par hypothèse. Comme $\mathbb{K}[X]$ est un anneau principal, ce noyau est donc engendré par un polynôme $P(X)$ de degré minimal, et on peut supposer P unitaire quitte à le multiplier par une constante. On a alors $\forall Q(X) \in \mathbb{K}[X],\ Q(x) = 0 \iff P(X) \,|\, Q(X)$

Le morphisme φ passe donc au quotient pour créer un isomorphisme

$$\mathbb{K}[X]/(P(X)) \xrightarrow{\sim} \mathbb{K}[x]$$

On a alors la propriété suivante, garantissant l'existence d'extensions algébriques de $\mathbb{K}$ contenant des racines de polynômes quelconques :

Propriété 8. *Soit $\mathbb{K}$ un corps, et $P(X) \in \mathbb{K}[X]$ un polynôme non constant. Alors il existe une extension algébrique de $\mathbb{K}$ dans laquelle $P(X)$ est scindé.*

Démonstration. On raisonne par récurrence sur le degré d de $P(X)$.

Si $d = 1$, il n'y a rien à faire ($\mathbb{K}$ convient).

Supposons maintenant la propriété est vraie jusqu'au rang $d \geq 1$, et supposons que $\deg P = d+1$. Soit $P1(X)$ un facteur irréductible de $P(X)$. On considère l'anneau $\mathbb{K}'\widehat{=}\mathbb{K}[X]/(P1(X))$. En tant que $\mathbb{K}$-module, il est de degré fini, ses éléments sont donc tous algébriques. L'irréductibilité de $P1(X)$ assure que $\mathbb{K}'$ est intègre, et le lemme 1 implique donc que $\mathbb{K}'$ est un corps.

$\mathbb{K}'$ donc une extension algébrique de $\mathbb{K}$ de degré finie, et la classe de X dans $\mathbb{K}'$ est une racine de $P1(X)$. En notant x cette classe, on a donc $P(X) = (X - x)P2(X)$ sur $\mathbb{K}'$. Par hypothèse de récurrence, il existe une extension algébrique $\mathbb{K}''$ de $\mathbb{K}'$, de degré finie, sur laquelle $P2(X)$ est scindé. $\mathbb{K}''$ est alors une extension algébrique de $\mathbb{K}$ de degré finie (par la propriété 7), et $P(X)$ est scindé sur $\mathbb{K}''$. □

On cherche maintenant à plonger une extension algébrique $\mathbb{K}'$ de $\mathbb{K}$ dans une extension algébriquement close de $\mathbb{K}$. Il semble naturel de penser que si $\mathbb{K}'$ est de degré n, alors ces plongements sont au nombre de n, car les n racines de $P(X)$ seront 2 à 2 distinctes et seront « interchangeables ». Nous allons montrer ce résultat.

Définition 11. *Soit L, L' deux extensions d'un corps $\mathbb{K}$. On dit que $\varphi : L \to L'$ est un $\mathbb{K}$-isomorphisme si c'est un isomorphisme de corps et si $\forall a \in \mathbb{K}$, $\varphi(a) = a$.*

On dit que deux éléments $a \in L$ et $b \in L'$ sont conjugués s'il existe un $\mathbb{K}$-isomorphisme φ tel que $\varphi(a) = b$.

Lemme 2. *Soit $\mathbb{K}$ un corps de caractéristique 0, et $P(X) \in \mathbb{K}[X]$ un polynôme unitaire irréductible. On considère une extension algébrique finie $\mathbb{K}'$ dans laquelle $P(X)$ est scindée, et $P = \prod_{i-1}^{n} (X - x_i)$ la décomposition de $P(X)$ dans ce corps. Alors les x_i sont deux à deux distincts et deux à deux conjugués.*

Démonstration. Le fait que les x_i soient conjugués découle directement des isomorphismes explicites $\mathbb{K}[X]/(P(X)) \simeq \mathbb{K}[x_i]$ envoyant X sur x_i.

Pour montrer que les x_i sont 2 à 2 distincts, on raisonne par l'absurde : supposons à la place que $P(X)$ possède une racine multiple x. On a alors $P'(x) = 0$, ce qui signifie par minimalité du degré de $P(X)$ que $P'(X) = 0$, ce qui est absurde car $\mathbb{K}$ est de caractéristique 0. □

Ce lemme permet de montrer le théorème suivant, qui sera utile par la suite :

Théorème 3. *Soit $\mathbb{K}$ un corps de caractéristique 0, $\mathbb{K}'$ une extension de $\mathbb{K}$ de degré fini n, et C une extension algébriquement close de $\mathbb{K}$. Alors il existe exactement n $\mathbb{K}$-morphismes de $\mathbb{K}'$ dans C.*

Démonstration. Le lemme précédent montre presque entièrement le cas où $\mathbb{K}'$ est monogène, c'est-à-dire $\mathbb{K}' = \mathbb{K}[x]$.

Dans ce cas, on considère $P(X)$ le polynôme irréductible de x, de degré n. On a vu que ce polynôme admet n racines distinctes dans C, que l'on note $x_1, x_2, \ldots, x_n$. Il est clair qu'on a pour tout $1 \leq i \leq n$ un unique $\mathbb{K}$-morphisme envoyant x sur x_i. Ces $\mathbb{K}$-morphismes sont les seuls possibles, car un $\mathbb{K}$-morphisme conserve les relations polynomiales, l'image de x est donc nécessairement un des x_i.

Pour montrer le cas général, on raisonne par récurrence forte sur n. Le cas $n = 1$ est trivial.

Si $n > 1$, et supposons que $\mathbb{K}'$ ne soit pas monogène. On fixe un élément $x' \in \mathbb{K}'$
K. On a alors $\mathbb{K} \subsetneq \mathbb{K}[x] \subsetneq K'$. En notant $q = [\mathbb{K}[x] : \mathbb{K}]$, on a par hypothèse $q < n$ et $\frac{n}{q} < n$. D'après le cas monogène, il existe q morphismes $\varphi_1, \ldots, \varphi_n : \mathbb{K}[x] \to C$. Pour tout i, $\mathbb{K}[\varphi_i(x)]$ est isomorphe à $\mathbb{K}[x]$, on peut donc construire une extension $\mathbb{K}'_i$ de $\mathbb{K}[\varphi_i(x)]$ et un isomorphisme $\psi_i : \mathbb{K}' \to \mathbb{K}'_i$ qui prolonge φ_i.

Comme $[\mathbb{K}'_i : \mathbb{K}[\varphi_i(x)]] = \frac{n}{q}$, on sait par hypothèse de récurrence qu'il existe $\frac{n}{q}$ $\mathbb{K}[\varphi_i(x)]$-morphismes de $\mathbb{K}'i$ dans C. La composée de ces morphismes par ψ_i fournit n $\mathbb{K}$-morphismes de $\mathbb{K}'$ dans C, deux à deux distincts.

Il n'en existe pas d'autre car tout $\mathbb{K}$-morphisme de $\mathbb{K}'$ dans C prolongerait l'un des φ_i, et l'hypothèse de récurrence assure que pour chaque i, il n'existe que $\frac{n}{q}$ tels prolongements. □

Corollaire 1 (Théorème de l'élément primitif)**.** *Avec les mêmes hypothèses, $\mathbb{K}$ est nécessairement monogène, autrement dit il existe $x \in \mathbb{K}'$ tel que $\mathbb{K}'[x]$*

Démonstration. Soit $\sigma_1, \ldots, \sigma_n$ les n isomorphismes de $\mathbb{K}$ dans $\mathbb{K}'$. Pour tout $i \neq j$, on considère l'ensemble $E_{ij} = \{x \in \mathbb{K}' \,|\, \sigma_i(x) \neq \sigma_j(x)\}$. C'est un sous-espace vectoriel de $\mathbb{K}'$, différent de $\mathbb{K}'$ car $\sigma_i \neq \sigma_j$. Comme $\mathbb{K}$ est de caractéristique 0, il est infini, et on sait donc que la réunion des E_{ij} ne peut alors pas être égale à $\mathbb{K}'$.

On fixe alors un élément $x \in \mathbb{K}'$ n'appartenant pas à cette union : par définition, les $\sigma_i(x)$ sont deux à deux distincts. Soit $P(X)$ le polynôme minimal de x. Les $\sigma_i(x)$ sont des racines distinctes de $P(X)$ dans C. On a donc $\deg x \geq n$, et donc $[\mathbb{K}[x] : \mathbb{K}] \geq n$. Or $[\mathbb{K}[x] : \mathbb{K}] \leq [\mathbb{K}' : \mathbb{K}] \leq n$. On en déduit que $[\mathbb{K}[x] : \mathbb{K}] = n$ et que $\mathbb{K}[x] = \mathbb{K}'$. □

3.2.3 Trace, norme et discriminant dans une extension

Définition 12. *Soit B un anneau, et A un sous-anneau de B tel que B soit un A-module libre de rang fini n (en particulier, tous les éléments de B sont entiers sur A). Soit $x \in B$.*

1. *On note m_x l'application de multiplication par x dans B. C'est une application A-linéaire*
2. *On appelle* trace de x *et on note* $\mathrm{Tr}_{A/B}(x)$ *la trace de l'application m_x*
3. *On appelle* norme de x *et on note* $\mathrm{N}_{A/B}(x)$ *le déterminant de l'application m_x*

On notera simplement $\mathrm{Tr}(x)$ et $\mathrm{N}(x)$ lorsqu'aucune confusion n'est possible. Ce sont des éléments de A. Le lemme 2 permet d'expliciter leur valeur sous certaines conditions :

Propriété 9. *Soit $\mathbb{K}$ un corps de caractéristique 0, et $\mathbb{K}'$ une extension de $\mathbb{K}$ de degré n. Soit $x \in \mathbb{K}'$, et $x_1, \ldots, x_n$ les racines du polynôme minimal de x, chacune répétée $[\mathbb{K}' : \mathbb{K}[x]]$ fois. Alors $\mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(x) = x_1 + x_2 + \cdots + x_n$ et $\mathrm{N}_{\mathbb{K}'/\mathbb{K}}(x) = x_1 x_2 \ldots x_n$.*

Démonstration. Soit $P(X)$ le polynôme minimal de x. La proposition est équivalente au fait que le polynôme caractéristique de m_x est $P(X)^k$ avec $k = [\mathbb{K}' : \mathbb{K}[x]]$. On se contente de montrer le cas $k = 1$ (c'est-à-dire $\mathbb{K}' = \mathbb{K}[x]$), le cas général étant simplement un peu plus technique.

Comme $\mathbb{K}' = \mathbb{K}[x]$, on sait que $P(X)$ est de degré n. On note $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$.

La famille $(x^i)_{0 \leq i \leq n-1}$ est une base de $\mathbb{K}'$. Dans cette base, la matrice de m_x s'écrit :

$$M_x = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

On reconnaît la matrice compagnon de $P(X)$. Il en découle que le polynôme caractéristique de m_x est $P(X)$, d'où le résultat. □

Une conséquence de cette propriété est que, si $\mathbb{K}$ est le corps des fractions de A et que x est entier sur A, alors la trace et la norme de x seront entiers sur A. En particulier, pour $\mathbb{K} = \mathbb{Q}$ et $A = \mathbb{Z}$, la trace et la norme de x sont entiers.

Les notions de trace et de norme d'un élément sont absolument fondamentales en théorie algébrique des nombres, et nous les réutiliseront par la suite. On a par exemple d'obtenir le résultat suivant :

Propriété 10. *Avec les mêmes hypothèses, on a $\forall x \in B$, $\mathrm{N}(x) \in xB \cap A$.*

Démonstration. On considère le polynôme caractéristique de m_x :

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

Alors $a_0 = (-1)^n \,\mathrm{N}(x)$. Or on a vu que $P(X)$ est une puissance du polynôme minimal de x. En particulier, $P(x) = 0$. On en déduit alors :

$$\mathrm{N}(x) = (-1)^{n+1} x \left(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1\right)$$

D'où $\mathrm{N}(x) \in xB$ □

Corollaire 2. *Avec les mêmes hypothèses, soit $\mathfrak{p}'$ est un idéal premier de B non réduit à (0). Alors $\mathfrak{p} = \mathfrak{p}' \cap A$ est également un idéal premier de A non réduit à (0). On dit que $\mathfrak{p}'$ est un relèvement de $\mathfrak{p}$.*

Démonstration. Le fait que $\mathfrak{p}$ soit un idéal premier de A est un résultat classique. Le fait qu'il soit non réduit à (0) découle de la propriété précédente : on fixe un élément x de $\mathfrak{p}'$ non nul. On a alors $\mathrm{N}(x) \in \mathfrak{p}$, et $\mathrm{N}(x) \neq 0$ car l'application m_x est inversible. □

Les notions de trace et de norme permettent également de définir le discriminant d'une famille d'éléments, et le discriminant d'un anneau, et de montrer le résultat suivant :

Théorème 4. *Soit A un anneau, et $\mathbb{K}$ son corps de fractions, que l'on suppose de caractéristique 0. Soit $\mathbb{K}'$ une extension de corps de $\mathbb{K}$ de degré fini n, et A' la fermeture intégrale de A dans $\mathbb{K}'$. Alors A' est un sous-module d'un A-module libre de rang n.*

De plus, si A est principal, alors A' est un A-module libre de rang n.

Le deuxième résultat est assez intuitif : dans le cas des corps de nombres, il signifiera que si $\mathbb{K}$ est une extension finie de $\mathbb{Q}$, alors l'anneau des entiers de $\mathbb{K}$ sera un $\mathbb{Z}$-module libre de même dimension que $\mathbb{K}$. Ce théorème est admis dans ce document, car il nécessite des résultats plus avancés sur les normes et les traces. Ce travail est effectué dans [3].

3.2.4 Anneaux de Dedekind et décomposition en produit d'idéaux premiers

Afin d'étendre le théorème d'Ostrowski aux corps de nombres, nous avons besoin d'un type d'anneau plus faible que les anneaux principaux (l'anneau des entiers sur un corps de nombre n'étant en général pas principal), mais permettant tout de même de faire de l'arithmétique. C'est le cas des anneaux de Dedekind.

Définition 13. *Soit A un anneau. On dit que A est un anneau de Dedekind s'il est noethérien (c'est-à-dire que tous ses idéaux sont de type finis), intégralement clos, et si tous ses idéaux premiers non nuls sont maximaux.*

On vérifie aisément que tout anneau principal est un anneau de Dedekind. En revanche, nous avons le résultat fondamental suivant, qui n'est pas vrai pour les anneaux principaux :

Théorème 5. *Soit A un anneau de Dedekind, et $\mathbb{K}$ son corps de fractions. Soit $\mathbb{K}'$ une extension de degré fini de $\mathbb{K}$, et A' la fermeture intégrale de A dans $\mathbb{K}'$. Alors A' est un anneau de Dedekind, et un A-module de type fini.*

Une conséquence immédiate de ce théorème est que si $\mathbb{K}$ est un corps de nombre, l'anneau des entiers sur $\mathbb{K}$ sera un anneau de Dedekind.

Démonstration. Le fait que A' soit un anneau noethérien découle du théorème 4 que nous avons admis précédemment. A' est un sous-module d'un A-module libre de rang fini. Le fait qu'un tel module soit noethérien est un résultat classique.

Soit x un élément de $\mathrm{Frac}(A')$ entier sur A'. En particulier, $x \in \mathbb{K}'$ et x est entier sur A' grâce à la propriété de transitivité, donc $x \in A'$ par définition de A'. Montrons maintenant que tout idéal premier $\mathfrak{p}' \neq (0)$ de A' est maximal.

On considère l'idéal $\mathfrak{p} = \mathfrak{p}' \cap A$. C'est un idéal premier de A. Il est non réduit à 0, car si l'on fixe un élément $x \in \mathfrak{p}'$ non nul, x vérifie une équation de dépendance intégrale de degré minimal :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Cette équation vérifie alors $a_0 \neq 0$ (par minimalité du degré), et $a_0 \in \mathfrak{p}$.

$\mathfrak{p}$ est donc par hypothèse un idéal maximal de A, donc $A/\mathfrak{p}$ est un corps. Or, le morphisme canonique $A \to A'/\mathfrak{p}'$ a pour noyau $\mathfrak{p}$. $A/\mathfrak{p}$ est donc un sous-anneau de $A'/\mathfrak{p}'$, et tout élément de $A'/\mathfrak{p}'$ est alors entier sur $A/\mathfrak{p}$. On peut donc appliquer le Lemme 1 pour montrer que $A'/\mathfrak{p}'$ est un corps. $\mathfrak{p}'$ est donc un idéal maximal de A'. □

L'intérêt des anneaux de Dedekind est qu'ils possèdent une forme légèrement plus faible du théorème de décomposition de facteurs premiers dans les anneaux principaux. Au lieu de considérer des *éléments premiers* de A, on considérera les *idéaux premiers* de A. Pour cela, nous devons d'abord définir les idéaux fractionnaires de A :

Définition 14. *Soit A un anneau intègre, et $\mathbb{K}$ son corps de fractions. On dit qu'un ensemble $I \subset \mathbb{K}$ est un* idéal fractionnaire *de A si c'est un sous-A-module de $\mathbb{K}$ et si*

$$\exists d \in A \text{ tel que } I \subset d^{-1}A$$

On dira que d est un dénominateur commun *de I.*

En particulier, les idéaux de A sont également des idéaux fractionnaires. On les appelle également des idéaux entiers.

On définit le produit et la somme d'idéaux fractionnaires de la même manière que pour les idéaux entiers :

$$I + I' = \{a + a' \,|\, a \in I,\, a' \in I'\}$$
$$II' = \left\{\sum a_i + a'_i \,|\, (a_i) \in I,\, (a'_i) \in I'\right\}$$

Ce sont également des idéaux fractionnaires.

Dans le cas des anneaux de Dedekind (plus généralement, des anneaux noethériens), un sous-module de I de $\mathbb{K}$ est un idéal fractionnaire si et seulement si il est de type fini. En effet, il est clair que tout sous-module de type fini a un dénominateur commun. Réciproquement, si I est un idéal fractionnaire, c'est un sous-module de $d^{-1}A$ pour un certain $d \in A$. Or $d^{-1}A$ est un A-module isomorphe à A, il est donc noethérien, et donc I est de type fini.

Comme dit précédemment, les anneaux de Dedekind vérifient un théorème équivalent à la décomposition en facteurs premiers dans les anneaux principaux :

Théorème 6. *Soit A un anneau de Dedekind. On note P l'ensemble des idéaux premiers de A. Alors tout idéal fractionnaire non nul I s'écrit de manière unique sous la forme*

$$I = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_\mathfrak{p}(I)}$$

Où les $n_\mathfrak{p}$ sont des éléments de $\mathbb{Z}$, presque tous nuls.

La démonstration de ce théorème est admise.

On a de plus les formules suivantes :

$$\begin{aligned} n_\mathfrak{p}(II') &= n_\mathfrak{p}(I) + n_\mathfrak{p}(I') \\ n_\mathfrak{p}(I + I') &= \min\left(n_\mathfrak{p}(I),\, n_\mathfrak{p}(I')\right) \\ n_\mathfrak{p}(I \cap I') &= \max\left(n_\mathfrak{p}(I),\, n_\mathfrak{p}(I')\right) \\ I \subset I' &\iff \forall \mathfrak{p} \in P,\, n_\mathfrak{p}(I) \geq n_\mathfrak{p}(I') \end{aligned}$$

Ce théorème implique également que l'ensemble des idéaux fractionnaires de A est un groupe lorsqu'on le muni du produit d'idéaux, dont l'élément neutre est A lui-même. (avec $n_\mathfrak{p}\left(I^{-1}\right) = -n_\mathfrak{p}\left(I\right)$)

3.2.5 Valeurs absolues dans un corps de nombres

Nous avons maintenant tous les outils en main pour caractériser les différentes places des extensions finies de $\mathbb{Q}$.

Définition 15. *On dit qu'un corps $\mathbb{K}$ est un* corps de nombres *si c'est une extension finie de $\mathbb{Q}$.*

Lorsqu'on parlera d'élément entier de $\mathbb{K}$, ce sera toujours désigner les éléments de $\mathbb{K}$ entiers sur $\mathbb{Z}$.

Les résultats des paragraphes précédents s'appliquent dans le cas particulier des corps de nombres : L'anneau des entiers sur un corps de nombres est un anneau de Dedekind. C'est aussi un $\mathbb{Z}$-module libre, dont le rang est égal au degré $[\mathbb{K} : \mathbb{Q}]$. En particulier, $\mathbb{K}$ est le corps de fractions sur cet anneau. De plus, si $\mathbb{K}$ est un corps de nombre de degré n, il possède exactement n isomorphismes à image dans $\mathbb{C}$.

Considérons un tel isomorphisme $\sigma : \mathbb{K} \to \mathbb{C}$. On observe deux cas possibles : Soit l'image de σ est incluse dans $\mathbb{R}$, soit elle ne l'est pas. Dans ce deuxième cas, en notant ι l'involution $z \in \mathbb{C} \to \bar{z}$, $\iota \circ \sigma$ est également un isomorphisme de $\mathbb{K}$ dans $\mathbb{C}$, distinct de σ.

Par conséquent, il existe des entiers r_1 et r_2 tels que $r_1 + 2r_2 = n$ et tels que les isomorphismes de $\mathbb{K}$ dans $\mathbb{C}$ puissent être numérotées σ_1, σ_2, $\ldots \sigma_n$ en vérifiant :

$$\forall 1 \leq i \leq r_1,\ \ \sigma_i\left(\mathbb{K}\right) \subset \mathbb{R}$$

$$\forall 1 \leq j \leq r_2,\ \ \sigma_{r_1+j} = \iota \circ \sigma_{r_1+r_2+j}$$

Autrement dit, connaître les $r_1 + r_2$ premiers isomorphismes suffit à déterminer les r_2 derniers.

Chacun de ces isomorphismes permet de définir une valeur absolue archimédienne sur $\mathbb{K}$, induite de celle sur $\mathbb{C}$:

$$|x|_\sigma \widehat{=} |\sigma(x)|$$

Propriété 11. *En réutilisant les mêmes notations que dans le paragraphe précédent, les valeurs absolues $|\cdot|_{\sigma_i}$ définissent exactement $r_1 + r_2$ places archimédiennes différentes.*

Plus précisément, si $i \neq j$, $|\cdot|_{\sigma_i}$ et $|\cdot|_{\sigma_j}$ sont équivalentes si et seulement si $\sigma_i = \iota \circ \sigma_j$.

Démonstration. Il est clair que si $\sigma_i = \iota \circ \sigma_j$, alors les valeurs absolues $|\cdot|_{\sigma_i}$ et $|\cdot|_{\sigma_j}$ sont équivalentes (elles sont même égales).

Supposons maintenant que σ et σ' induisent des valeurs absolues équivalentes. Autrement dit, leurs valeurs absolues appartiennent à la même place v. On note $\mathbb{K}_1$ (resp. $\mathbb{K}_2$) l'image de $\mathbb{K}$ par σ (resp. σ'). Ces deux ensembles sont par définition des sous-corps de $\mathbb{C}$ isomorphes à $\mathbb{K}$. On considère maintenant $\mathbb{K}_v$, le complété de $\mathbb{K}$ en v. Le morphisme σ (resp. σ') se relève en un isomorphisme $\tilde{\sigma}$ (resp. $\tilde{\sigma}'$) de $\mathbb{K}_v$ dans $\mathbb{K}_{1,\infty}$ (resp. $\mathbb{K}_{2,\infty}$), où $\mathbb{K}_{i,\infty}$ désigne le complété de $\mathbb{K}_i$ pour la valeur absolue usuelle de $\mathbb{C}$. Si $\mathbb{K}_i \subset \mathbb{R}$, il est dense dans $\mathbb{R}$ et donc $\mathbb{K}_{i,\infty} = \mathbb{R}$. Sinon, $\mathbb{K}_i$ est dense dans $\mathbb{C}$ et donc $\mathbb{K}_{i,\infty} = \mathbb{C}$.

$\tilde{\sigma_j} \circ {\tilde{\sigma_i}}^{-1}$ est donc un isomorphisme de corps et une isométrie de $\mathbb{K}_{1,\infty}$ dans $\mathbb{K}_{2,\infty}$. Cela n'est possible que si $\mathbb{K}_{1,\infty} = \mathbb{K}_{2,\infty}$, et dans ce cas :

1. Soit $\mathbb{K}_{1,\infty} = \mathbb{R}$, auquel cas $\tilde{\sigma_j} \circ {\tilde{\sigma_i}}^{-1} = \mathrm{Id}_{\mathbb{R}}$.
2. Soit $\mathbb{K}_{1,\infty} = \mathbb{C}$, auquel cas $\tilde{\sigma_j} \circ {\tilde{\sigma_i}}^{-1} = \mathrm{Id}_{\mathbb{C}}$ ou ι.

On a donc bien $\sigma = \sigma'$ ou $\sigma = \iota \circ \sigma'$, ce qui conclut la preuve. □

Cherchons à présent les valeurs absolues non-archimédiennes de $\mathbb{K}$. Dans le cas de $\mathbb{Q}$, il s'agissait des valeurs absolues p-adiques. Ici, les idéaux premiers prennent la place des nombres premiers dans le cas de $\mathbb{Q}$, il semble donc naturel de construire des valeurs absolues à partir de ces idéaux premiers.

Définition 16. *Soit A l'ensemble des entiers de $\mathbb{K}$, et $\mathfrak{p}$ un idéal premier non nul de A. Pour tout $x \in \mathbb{K}$, on note $n_{\mathfrak{p}}(x)$ l'exposant de $\mathfrak{p}$ dans la décomposition de l'idéal fractionnaire xA en produit d'idéaux premiers. Par convention, $n_{\mathfrak{p}}(0) = +\infty$.*

On définit la valeur absolue $\mathfrak{p}$-adique sur $\mathbb{K}$:

$$\forall x \in \mathbb{K},\ |x|_{\mathfrak{p}} \widehat{=} e^{-n_{\mathfrak{p}}(x)}$$

Propriété 12. *L'application $|\cdot|_{\mathfrak{p}}$ est une valeur absolue non-archimédienne sur $\mathbb{K}$. Si $\mathfrak{p}$ et $\mathfrak{q}$ sont deux idéaux premiers non nuls distincts, $|\cdot|_{\mathfrak{p}}$ et $|\cdot|_{\mathfrak{q}}$ appartiennent à deux places différentes.*

Démonstration. Il est clair que $|x|_{\mathfrak{p}} \geq 0$ et que $|x|_{\mathfrak{p}} = 0 \iff x = 0$. Les autres axiomes des valeurs absolues non-archimédiennes découlent des propriétés de $n_{\mathfrak{p}}$, plus précisément du fait que $n_{\mathfrak{p}}(II') = n_{\mathfrak{p}}(I) + n_{\mathfrak{p}}(I')$ et $n_{\mathfrak{p}}(I + I') = \min\left(n_{\mathfrak{p}}(I),\, n_{\mathfrak{p}}(I')\right)$.

Le fait que les places des valeurs absolues $|\cdot|_{\mathfrak{p}}$ et $|\cdot|_{\mathfrak{q}}$ soient distinctes découle directement de la propriété 2 et du fait que l'idéal de valuation de $|\cdot|_{\mathfrak{p}}$ est $\mathfrak{p}$ lui-même. □

Les places que nous avons définies sont en vérité toutes les places possibles de $\mathbb{K}$. Pour le montrer, nous allons admettre un théorème supplémentaire, dû à Ostrowski :

Théorème 7. *Les seuls corps archimédiens complets, à isomorphisme prêt, sont $\mathbb{R}$ et $\mathbb{C}$ dotés de la valeur absolue usuelle $|\cdot|_\infty$.*

Une démonstration de ce théorème est disponible dans [4]

On peut maintenant montrer qu'un corps de nombres n'a pas d'autre place que celles que nous avons déjà définies :

Théorème 8. *Soit $\mathbb{K}$ un corps de nombres de degré n. Soit r_1 et r_2 les deux entiers définis précédemment. Alors les seules places de $\mathbb{K}$ sont :*

1. *La place triviale*
2. *Les $r_1 + r_2$ places archimédiennes induites par les morphismes de $\mathbb{K}$ dans $\mathbb{C}$*
3. *Les places induites par les valeurs absolues $\mathfrak{p}$-adiques, pour $\mathfrak{p}$ un idéal premier de $\mathbb{K}$*

Démonstration. Montrons d'abord que $\mathbb{K}$ n'a pas d'autre place archimédienne que celles induites par les morphismes de $\mathbb{K}$ dans $\mathbb{C}$. Pour cela, on considère une place archimédienne v, et on fixe une valeur absolue $|\cdot|$ représentant v. On note $\mathbb{K}_v$ le complété de $\mathbb{K}$ en v. $|\cdot|$ s'étend naturellement à $\mathbb{K}_v$ et en fait un corps archimédien complet.

D'après le théorème précédent, il existe donc un isomorphisme φ de $\mathbb{K}_v$ dans $\mathbb{C}$ ou $\mathbb{R}$ tel que $\varphi \circ |\cdot|$ est équivalente à $|\cdot|_\infty$. Ainsi, la composée de φ par l'inclusion de $\mathbb{K}$ dans $\mathbb{K}_v$ induit un $\mathbb{Q}$-isomorphisme σ de $\mathbb{K}$ dans un sous-corps de $\mathbb{C}$, tel que $|\cdot|$ est équivalente à $|\cdot|_\sigma$. Donc v est la place induite par $|\cdot|_\sigma$.

On suppose maintenant que v est une place non-archimédienne, que l'on suppose non triviale, et on fixe $|\cdot|$ un de ses représentants. On note A l'ensemble des entiers de $\mathbb{K}$, et $\mathfrak{p}$ l'ensemble des éléments de A de valeur absolue < 1. Montrons que tout élément de A est de valeur absolue ≤ 1. Pour cela, supposons par l'absurde qu'il existe un $x \in A$ tel que $|x| > 1$. x vérifie une équation de dépendance intégrale :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Avec $a_0, \ldots, a_{n-1} \in \mathbb{Z}$. On sait qu'on a, pour tout i, $|a_i| \leq 1$. Or, d'après l'inégalité ultramétrique (« tous les triangles sont isocèles »), comme $|a_{n-1}x^{n-1} + \cdots + a_1 x| \leq |x|^{n-1} < |x|^n$, on a $a_0 = \max\left(|x^n|, |a_{n-1}x^{n-1} + \cdots + a_1 x|\right) = |x|^n$, donc $|a_0| > 1$, ce qui est absurde.

Par conséquent, on a $\forall a \in A$, $\forall x \in \mathfrak{p}, ax \in \mathfrak{p}$. On en déduit que $\mathfrak{p}$ est un idéal de A, et il est bien évidemment premier. Reste à montrer que $|\cdot|$ est équivalente à $|\cdot|_\mathfrak{p}$. Pour cela, on montre d'abord que $|\cdot|$ est constante sur $\mathfrak{p} - \mathfrak{p}^2$. Si ce n'était pas le cas, il existerait des éléments $x, y \in \mathfrak{p} - \mathfrak{p}^2$ tels que $|x| < |y|$. Mais alors $\left|\dfrac{x}{y}\right| < 1$, donc $\dfrac{x}{y} \in \mathfrak{p}$, et donc $x \in y\mathfrak{p} \subset \mathfrak{p}^2$, ce qui est absurde.

On note alors α la valeur prise par $|\cdot|$ sur $\mathfrak{p} - \mathfrak{p}^2$. Comme v est non triviale, $\alpha > 0$. Pour tout $x \in \mathbb{K}$, on décompose l'idéal fractionnaire engendré par x :

$$xA = \prod_{\mathfrak{q} \in P} \mathfrak{q}^{n_\mathfrak{q}}$$

et on souhaite montrer que $|x| = \alpha^{n_\mathfrak{p}}$, ce qui prouverait que $|\cdot|$ est équivalente à $|\cdot|_\mathfrak{p}$. Comme $\mathbb{K}$ est le corps de fractions sur A, il suffit de le montrer pour $x \in A$, autrement dit $n_\mathfrak{q} \geq 0$ pour tout $\mathfrak{q}$.

On peut écrire $x = \prod\limits_{\mathfrak{q} \in P} x_\mathfrak{q}$, avec $x_\mathfrak{q} \in \mathfrak{q}^{n_\mathfrak{q}}$. Si $\mathfrak{q}$ et $\mathfrak{q}'$ sont deux idéaux premiers de A (éventuellement égaux) $x_\mathfrak{q}$ ne peut pas appartenir à $\mathfrak{q}^{n_\mathfrak{q}}\mathfrak{q}'$. Sinon, on aurait

$$x \in \left(\prod_{\mathfrak{q} \in P} \mathfrak{q}^{n_\mathfrak{q}}\right) \mathfrak{q}'$$

$$\text{Donc } xA \subset \left(\prod_{\mathfrak{q} \in P} \mathfrak{q}^{n_\mathfrak{q}}\right) \mathfrak{q}'$$

Ce qui contredirait l'unicité de la décomposition en idéaux premiers. En particulier, $\forall \mathfrak{q} \neq \mathfrak{p}$, $x_\mathfrak{q} \notin \mathfrak{q}^{n_\mathfrak{q}}\mathfrak{p} = \mathfrak{q}^{n_\mathfrak{q}} \cap \mathfrak{p}$. Donc $x_\mathfrak{q} \notin \mathfrak{p}$, et donc $|x_q| = 1$.

On a alors $|x| = |x_\mathfrak{p}|$, et d'après ce qu'on vient de montrer, $x_\mathfrak{p} \in \mathfrak{p}^{n_\mathfrak{p}} - \mathfrak{p}^{n_\mathfrak{p}+1}$. On peut donc décomposer $x_\mathfrak{p}$ en un produit $x_\mathfrak{p} = y_1 y_2 \dots y_{n_\mathfrak{p}}$, où $\forall i$, $y_i \in \mathfrak{p} - \mathfrak{p}^2$. On en déduit que $|y_i| = \alpha$, et donc $|x| = \alpha^{n_\mathfrak{p}}$, ce qui termine la preuve. □

Terminons par un dernier résultat sur les corps de nombres :

Définition 17. *Soit $\mathbb{K}$ un corps de nombre, A l'anneau des entiers de $\mathbb{K}$, et I un idéal entier. On appelle* norme de I *l'entier* $\mathrm{N}(I) = \mathrm{Card}(A/I)$

Bien qu'innocente en apparence, il n'est pas évident que la norme de I soit finie. Nous l'admettons ici, et une preuve est présentée dans [2].

Corollaire 3. *Soit $\mathbb{K}$ un corps de nombre, et $\mathfrak{p}$ une place non-archimédienne de $\mathbb{K}$. Alors le corps résiduel de $\mathfrak{p}$ est un corps fini. On dira que le complété $\mathbb{K}_\mathfrak{p}$ de $\mathbb{K}$ en $\mathfrak{p}$ est un corps local.*

3.3 Formes quadratiques

Cette partie est principalement basée sur [2]. On y présentera des généralités sur les formes quadratiques ainsi que le théorème de Hasse-Minkowski, qui sera entièrement démontré sur $\mathbb{Q}$ et partiellement démontré sur un corps de nombres quelconque.

3.3.1 Généralités sur les formes quadratiques

Dans cette section, $\mathbb{K}$ désigne un corps de caractéristique différente de 2.

Définition 18. *Soit V un $\mathbb{K}$-espace vectoriel. On dit que $Q : V \to \mathbb{K}$ est une forme quadratique si elle vérifie les propriétés suivantes :*

1. $\forall a \in \mathbb{K}$, $\forall x \in V$, $Q(ax) = a^2 Q(x)$
2. *L'application $(x, y) \in V^2 \to Q(x + y) - Q(x) - Q(y)$ est bilinéaire.*

On dit alors que (V, Q) est un espace quadratique.

Étant donné un espace quadratique (V, Q), on définit le produit scalaire associé à Q :

$$\forall x, y \in V,\ x.y = \frac{1}{2}\left(Q(x + y) - Q(x) - Q(y)\right)$$

Le produit scalaire associé à Q est une forme bilinéaire symétrique. De plus, si f est une forme bilinéaire symétrique sur V, l'application $x \to f(x, x)$ est une forme quadratique, dont le produit scalaire associé est f. Il y a donc une bijection entre les formes quadratiques et les formes bilinéaires symétriques.

Définition 19 (Représentation matricielle d'une forme quadratique)**.** *Soit (V, Q) une forme quadratique, avec V de dimension finie n. Soit $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base de V. On appelle matrice de Q par rapport à $\mathcal{B}$ la matrice $A = (e_i.e_j)_{1 \leq i,j \leq n}$.*

C'est une matrice symétrique. De plus, si x et y sont des vecteurs de V, représentés dans la base $\mathcal{B}$ par les matrices colonnes X et Y respectivement, alors $x.y = X^T A Y$.

Le déterminant de A ne dépend de la base $\mathcal{B}$ choisie qu'à un facteur carré près. On définit donc le discriminant de Q comme étant la classe du déterminant de A dans $\mathbb{K}/\left(\mathbb{K}*^2\right)$

Définissons quelques autres notions classiques sur les espaces quadratiques :

Définition 20. *Soit (V, Q) un espace quadratique.*

1. *Soit $x, y \in V$. On dit que x et y sont orthogonaux si $x.y = 0$*
2. *Soit H une partie de V. On note H^0 l'orthogonal de H :*

$$H^0 = \{x \in V \,|\, \forall y \in H,\, x.y = 0\}$$

   C'est un sous-espace vectoriel de V.

3. *Si H_1 et H_2 sont des sous-espaces vectoriels de V, on dit qu'ils sont orthogonaux si $H_1 \subset H_2^0$*
4. *On appelle radical de V l'ensemble $\operatorname{rad} V = V^0$. Si $\operatorname{rad} V = 0$, on dit que Q est non dégénérée. Si V est de dimension finie, c'est équivalent à dire que le discriminant de Q est non nul.*
5. *Lorsque V est de dimension finie, on appelle rang de Q l'entier $\operatorname{rg} Q = \dim V - \dim(\operatorname{rad} V)$.*
6. *Soit $x \in V$. On dit que x est isotrope si $Q(x) = 0$*
7. *Un morphisme d'espaces quadratiques (ou morphisme métrique) de (V, Q) dans (V', Q') est une application $\varphi : V \to V'$ telle que φ soit linéaire et $\forall x \in V$, $Q(x) = Q'(\varphi(x))$. Si φ est un isomorphisme en tant qu'application linéaire, on dira que c'est un isomorphisme d'espaces qudratiques.*
8. *On dit qu'un élément $a \in \mathbb{K}$ est représenté par Q si il existe un vecteur $x \in V$ non nul tel que $Q(x) = a$. L'ensemble des éléments représentés par Q est stable par multiplication par un élément de $\mathbb{K}*^2$.*

Un exemple fondamental d'espace quadratique est le plan hyperbolique :

Définition 21 (Plan hyperbolique)**.** *On dit que (H, Q) est un plan hyperbolique s'il admet une base (x, y), où x et y sont deux éléments isotropes, et $x.y = 1$.*

C'est équivalent à dire que (H, Q) est isomorphe à $\mathbb{K}^2$ muni de la forme quadratique :

$$(x, y) \in \mathbb{K}^2 \to x^2 - y^2$$

Le plan hyperbolique représente tous les éléments de $\mathbb{K}$. En effet, si (x, y) est une base de H comme dans la définition de H, alors $Q\left(x + \frac{a}{2}y\right) = a$.
Le discriminant du plan hyperbolique est -1.

Cet exemple est particulièrement important car il est omniprésent dans les espaces quadratiques. On peut en effet montrer le résultat suivant :

Propriété 13. *Soit (V, Q) un espace quadratique non dégénéré, et $x \neq 0$ un vecteur isotrope de V. Alors il existe un sous-espace U de V contenant x et tel que U soit un plan hyperbolique.*

Démonstration. Comme V est non dégénéré, la forme linéaire $y \to x.y$ est non nulle, et donc il existe un vecteur y tel que $x.y = 1$. On pose alors $z = y - \frac{1}{2}(y.y)x$ et on vérifie aisément que z est isotrope et que $x.z = 1$. L'espace engendré par x et z est donc un plan hyperbolique. □

On a enfin le résultat suivant :

Propriété 14. *Tout espace quadratique de dimension finie admet une base orthogonale, c'est-à-dire une base* $(e_i)_{1\leq i\leq n}$ *telle que* $\forall i \neq j,\ e_i.e_j = 0$
Étant donné une telle base, le discriminant de Q *est alors* $\prod_{i=1}^{n} Q(e_i)$

Démonstration. La deuxième partie découle directement de la définition de discriminant. Pour la première, on procède par récurrence. Si $\dim V = 1$ ou si tous les vecteurs de V sont isotropes, il n'y a rien à faire.

Sinon, il existe un élément $x \in V$ tel que $x.x \neq 0$. On considère alors $H = (x)^0$. C'est un hyperplan ne contenant pas x. Par hypothèse de récurrence, il admet donc une base orthogonale $(e_1, \ldots, e_{n-1})$, et $(x, e_1, \ldots e_{n-1})$ est alors une base orthogonale de V □

3.3.2 Représentation d'une forme quadratique par un polynôme

Étant donné un espace quadratique (V, Q) de dimension n, donc la matrice dans une base $\mathcal{B}$ fixée est $A = (a_{ij})$, on associe à Q le polynôme à n variables :

$$\begin{aligned} f(X_1, \ldots, X_n) &= \sum_{1\leq i,j\leq n} a_{ij} X_i X_j \\ &= \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum i < j a_{ij} X_i X_j \end{aligned}$$

C'est un polynôme homogène de degré 2. Réciproquement, tout polynôme homogène à n variables de degré 2 définit une forme quadratique sur $\mathbb{K}^n$.

Les résultats précédents peuvent alors se traduire dans le langage des polynômes :

1. Deux formes f et f' sont dites équivalentes si les espaces quadratiques associés sont isomorphes. On notera $f \sim f'$
2. Une forme f est hyperbolique si $f \sim X^2 - Y^2 \sim XY$
3. On dit que f représente a s'il existe des éléments $x_1, \ldots, x_n$ de $\mathbb{K}$, non tous nuls, tels que $f(x_1, \ldots, x_n) = a$
4. Si f représente 0, alors $f \sim g + h$, où g est hyperbolique et g et h utilisent des variables deux à deux distinctes.
5. Si f représente 0, elle représente tous les éléments de $\mathbb{K}$.
6. Soit f une forme quadratique à n variables. Alors il existe des scalaires $a_1, \ldots, a_n \in \mathbb{K}$ tels que
$$f \sim a_1 X_1^2 + \cdots + a_n X_n^2$$
Le discriminant de f est alors le produit des a_i. f est non dégénérée si et seulement si les a_i sont tous non nuls.
On notera par la suite $\langle a_1, \ldots, a_n \rangle$ la forme $a_1 X_1^2 + \cdots + a_n X_n^2$.

Les deux propriétés suivantes font le lien entre le fait de représenter 0 et représenter un scalaire $a \in \mathbb{K}*$ quelconque :

Propriété 15. *Soit* $f(X_1, \ldots, X_n)$ *une forme quadratique non dégénérée, et* $a \in \mathbb{K}*$. *Alors les assertions suivantes sont équivalentes :*

1. *f représente a*

2. $f \sim g + aZ^2$, *où* $g(Y_1, \ldots, Y_{n-1})$ *est une forme quadratique à* $n-1$ *variables*
3. $f - aZ^2$ *représente* 0

Propriété 16. *Soit* $g(X_1, \ldots, X_n)$ *et* $h(Y_1, \ldots, Y_m)$ *deux formes non dégénérées, de rang* ≥ 1*, et soit* $f = g - h$*. Les assertions suivantes sont équivalentes :*

1. f *représente* 0
2. *Il existe un* $a \in \mathbb{K}*$ *représenté par* g *et par* h
3. *Il existe un* $a \in \mathbb{K}^*$ *tel que* $g - aZ^2$ *et* $h - aZ^2$ *représentent* 0.

Terminons par le résultat suivant dans le cas des corps finis, qui sera utile par la suite :

Propriété 17. *Soit* $\mathbb{K}$ *un corps fini. Toute forme quadratique de degré au moins égal à* 3 *représente* 0*. En particulier, elle représente donc tout élément* $a \in \mathbb{K}$

Ce résultat découle directement du théorème de Chevalley-Warning :

Théorème 9 (Chevalley-Warning)**.** *Soit* $\mathbb{K}$ *un corps fini de caractéristique* p*, et* $P_1, \ldots, P_r$ *une famille de polynôme à* n *variables à coefficients dans* $\mathbb{K}$*, tels que* $\sum \deg P_i < n$*. On note* V *l'ensemble des zéros communs des* P_i*. Alors*

$$\mathrm{Card}(V) \equiv 0 (\mathrm{mod}\, p)$$

3.3.3 Symbole de Hilbert

Dans cette section, $\mathbb{K}$ désigne soit $\mathbb{R}$, soit $\mathbb{C}$, soit un corps local, c'est-à-dire un corps complet non-archimédien dont le corps résiduel est fini.

Définition 22. *Soit* $a, b \in \mathbb{K}^*$*. On définit le symbole de Hilbert de* a *et* b *dans* $\mathbb{K}$ *:*

$$(a,b)_{\mathbb{K}} = 1 \text{ si la forme } \langle 1, -a, -b\rangle = Z^2 - aX^2 - bY^2 \text{ représente } 0 \text{ dans } \mathbb{K}$$
$$(a,b)_{\mathbb{K}} = -1 \text{ sinon}$$

On notera simplement (a, b) *lorsqu'il n'y a pas d'ambiguïté sur* $\mathbb{K}$*.*

Le symbole de Hilbert est facile à calculer si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$: pour $\mathbb{C}$, il vaut toujours 1. Pour $\mathbb{R}$, on a $(a, b) = 1 \iff a > 0$ ou $b > 0$. On supposera par la suite que $\mathbb{K}$ est un corps local.

La valeur de (a, b) ne change pas lorsqu'on multiplie un des termes par un carré. C'est donc une application $\mathbb{K}* / \left(\mathbb{K}*^2\right) \times \mathbb{K}* / \left(\mathbb{K}*^2\right) \to \{\pm 1\}$.

Propriété 18. *Soit* $a, b \in \mathbb{K}*$*. On note* $\mathbb{K}_b$ *le corps* $\mathbb{K}\left(\sqrt{b}\right)$ *(c'est donc une extension de* $\mathbb{K}$ *de degré* 1 *ou* 2*), et* N_b* *le groupe des normes des éléments de* $\mathbb{K}_b*$*. Alors* $(a, b) = 1$ *si et seulement si* $a \in N_b*$*.*

Démonstration. Si b est un carré, mettons $c^2 = b$, alors $\mathbb{K}_b = \mathbb{K}$ et donc $N_b* = \mathbb{K}*$. On cherche donc à montrer que pour tout $a \in \mathbb{K}*$, $(a, b) = 1$, ce qui est vrai car $(c, 0, 1)$ est une racine de $\langle 1, -a, -b\rangle$

Supposons que b ne soit pas un carré. Tout élément de $\mathbb{K}_b$ s'écrit sous la forme $x + y\sqrt{b}$ avec $x, y \in \mathbb{K}$, et sa norme vaut alors $x^2 - by^2$.
Si a appartient à $\mathbb{K}_b*$, on considère deux tels éléments x et y. $(x, 1, y)$ est alors une racine de $\langle 1, -a, -b\rangle$ d'où $(a, b) = 1$.

Réciproquement, supposons que $(a,b)=1$. La forme a donc un zéro (z,x,y) non nul. Comme b n'est pas un carré, $x \neq 0$, et donc

$$\begin{aligned} ax^2 &= z^2 - by^2 \\ a &= \left(\frac{z}{x}\right)^2 - b\left(\frac{y}{x}\right)^2 \\ &= \mathrm{N}\left(\frac{z}{x} + \frac{y}{x}\sqrt{b}\right) \end{aligned}$$

□

Propriété 19. *Soit $a,b \in \mathbb{K}^*$. On a les formules suivantes :*

1. *Si a est un carré dans $\mathbb{K}$, $(a,b)=1$*
2. *$(a,b)=(b,a)$*
3. *$(a,-a)=1$ et $(a,1-a)=1$*
4. *Si $(a,b)=1$ alors $\forall a' \in \mathbb{K}*, (aa',b)=(a',b)$*
5. *$(a,b)=(a,-ab)=(a,(1-a)b)$*

Ces propriétés se montrent toutes facilement. La quatrième peut d'ailleurs se généraliser :

Propriété 20. *Le symbole de Hilbert est bilinéaire. Autrement dit, on a pour tout $a,a',b \in \mathbb{K}*$:*

$$(aa',b)=(a,b)(a',b)$$

La démonstration de cette propriété est assez complexe et nécessite d'étudier le symbole de Hilbert sous un autre angle, celui des anneaux de quaternions. Le résultat est prouvé dans [4].

Cependant, la bilinéarité du symbole de Hilbert peut être montrée plus simplement dans le corps des nombres p-adique $\mathbb{Q}_p$. En effet, il est alors possible de donner une formule explicite de (a,b)

Théorème 10. *Soit p un nombre premier. On note $\mathbb{Q}_p$ le corps des nombres p-adiques, et $\mathbb{Z}_p = \{x \in \mathbb{Q}_p,\ |x|_p \leq 1\}$ l'anneau des entiers p-adiques.*
Soit $a,b \in \mathbb{Q}_p$. a et b peuvent être écrits d'une unique façon sous la forme $a=p^\alpha u$ et $b=p^\beta v$, où α et β sont des entiers et u et v sont des éléments inversibles de $\mathbb{Z}_p$.
On introduit les notations :

$$\left(\frac{u}{p}\right) = 1 \text{ si l'image de } u \text{ dans } F_p* \text{ est un carré}, -1 \text{ sinon.}$$

$$\text{Si } n \equiv 1 \pmod 2 \text{ : } \varepsilon(n) = \begin{cases} 0 & si \quad n \equiv 1 \pmod 4 \\ 1 & si \quad n \equiv -1 \pmod 4 \end{cases}$$

$$\omega(n) = \begin{cases} 0 & si \quad n \equiv \pm 1 \pmod 8 \\ 1 & si \quad n \equiv \pm 3 \pmod 8 \end{cases}$$

Le symbole de Hilbert de a et b vaut alors :

$$(a,b) = (-1)^{\alpha\beta\,\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \qquad si\ p \neq 2$$

$$(a,b) = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)} \qquad si\ p = 2$$

3.3.4 Théorème de Hasse-Minkowski

Nous avons maintenant les outils nécessaires pour démontrer le théorème de Hasse-Minkowski :

Théorème 11 (Hasse-Minkowski)**.** *Soit $\mathbb{K}$ un corps de nombres, et Ω l'ensemble des places non-triviales de $\mathbb{K}$.*

Soit $f(X_1, \ldots, X_n)$ une forme quadratique sur $\mathbb{K}$. Alors f représente 0 dans $\mathbb{K}$ si et seulement si elle représente 0 dans tous les $\mathbb{K}_\mathfrak{p}$, pour $\mathfrak{p} \in \Omega$

Corollaire 4. *Avec les mêmes notations, pour tout $a \in \mathbb{K}$, f représente a dans $\mathbb{K}$ si et seulement si elle représente a dans tous les $\mathbb{K}_\mathfrak{p}$.*

Le sens direct du théorème est évident : comme $\mathbb{K}$ se plonge naturellement dans les $\mathbb{K}_\mathfrak{p}$, tout zéro de f dans $\mathbb{K}$ sera en particulier un zéro de f dans chacun des $\mathbb{K}_\mathfrak{p}$.

Ce théorème est un exemple d'un principe général de la théorie algébrique des nombres qu'on appelle le *principe local-global* : Pour connaître une propriété globale sur un élément, il suffit parfois d'étudier cette propriété *localement* (c'est-à-dire sur chaque place).

Nous allons démontrer le théorème de Hasse-Minkowski partiellement dans le cas d'un corps de nombres, en admettant quelques résultats, puis montrer ces résultats dans le cas de $\mathbb{Q}$ afin d'obtenir une preuve complète du théorème dans $\mathbb{Q}$. La démonstration est principalement basée sur [2] (qui ne traite que du cas de $\mathbb{Q}$) Le théorème est vrai dans un cadre plus global que celui des corps de nombres (on parle de *corps global*), mais nous ne traitons pas ce cas dans ce document.

Avant de passer à la démonstration, nous avons besoin d'un lemme préliminaire :

Lemme 3 (Lemme d'Hensel)**.** *Soit $\mathbb{K}$ un corps local sur un corps de nombres, A l'anneau des entiers de $\mathbb{K}$ et $\mathfrak{p}$ son idéal de valuation. Soit $P(X)$ un polynôme à coefficients dans A. On suppose qu'il existe un élément $\alpha_1 \in A$ tel que*

$$P(\alpha_1) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p})$$
$$P'(\alpha_1) \not\equiv 0 \,(\mathrm{mod}\, \mathfrak{p})$$

Alors il existe $\alpha \in A$ tel que $\alpha \equiv \alpha_1 (\mathrm{mod}\, \mathfrak{p})$ et $P(\alpha) = 0$

Démonstration. On construit récursivement une suite $(\alpha_n)_{n\in\mathbb{N}}$ vérifiant les propriétés suivantes :

$$P(\alpha_n) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}^n)$$
$$\alpha_{n+1} \equiv \alpha_n \,(\mathrm{mod}\, \mathfrak{p}^n)$$

Pour cela, on suppose α_n défini. On cherche un terme sous la forme

$$\alpha_{n+1} = \alpha_n + b_n$$

avec $b_n \in \mathfrak{p}^n$ tel que $P(\alpha_{n+1}) \in \mathfrak{p}^{n+1}$. D'après la décomposition de Taylor de P, on a

$$P(\alpha_n + b_n) = P(\alpha_n) + P'(\alpha_n) b_n + c_n$$

avec $c_n \in \mathfrak{p}^{n+1}$

Remarquons que par hypothèse, $\alpha_n \equiv \alpha_1 (\mathrm{mod}\, \mathfrak{p})$, et donc $P'(\alpha_n) \equiv P'(\alpha_1) \not\equiv 0 (\mathrm{mod}\, \mathfrak{p})$. $P'(\alpha_n)$ est donc un élément de valeur absolue 1, et est donc inversible dans A. On pose alors :

$$b_n = -\left(P'(\alpha_n)\right)^{-1} P(\alpha_n)$$

On a bien $b_n \in \mathfrak{p}^n$ et $P(\alpha_n + b_n) \in \mathfrak{p}^{n+1}$, donc $\alpha_{n+1} = \alpha_n + b_n$ convient.

La suite (α_n) ainsi construite est alors une suite de Cauchy (car si $m < n$ alors $|\alpha_m - \alpha_n| \leq e^{-m}$). Comme $\mathbb{K}$ est complet, elle a donc une limite $\alpha \in A$, qui, par continuité de P, vérifie $P(\alpha) = 0$, ce qui achève la preuve. □

Corollaire 5. *Soit $\mathbb{K}$ un corps de nombres et $f = \langle a_1, \ldots, a_n \rangle$ une forme quadratique de degré $n \geq 3$. Soit $\mathfrak{p}$ une place non-archimédienne de $\mathbb{K}$ relevant un nombre premier $p \neq 2$, telle que $|a_i|_\mathfrak{p} = 1$ pour tout i. Alors f représente 0 dans $\mathbb{K}_\mathfrak{p}$.*

Démonstration. Si la forme est dégénérée (c'est-à-dire que l'un des a_i est nul), le résultat est trivial. On suppose donc f non dégénérée, et on note A l'anneau des entiers de $\mathbb{K}_\mathfrak{p}$. Par hypothèse, les a_i appartiennent à A et sont inversibles dans A. Autrement dit, leur projection sur le corps résiduel $A/\mathfrak{p}$ est non nulle. D'après la propriété 17, f représente 0 sur ce corps. Autrement dit, il existe $x = (x_1, \ldots, x_n) \in A^n$ non nul tel que

$$f(x) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p})$$

Pour relever x en un zéro de $\mathbb{K}_p$, on souhaite utiliser le lemme d'Hensel. Pour cela il suffit de montrer que l'une des dérivées partielles de f en x n'est pas nulle. Or on a

$$\frac{\partial f}{\partial X_i}(x) = 2 a_i x_i$$

et on sait que $\mathfrak{p} \cap \mathbb{Q} = p\mathbb{Z}$ avec $p \neq 2$, donc $A/\mathfrak{p}$ n'est pas de caractéristique 2. Comme $x \neq 0$, il existe donc un i tel que $\dfrac{\partial f}{\partial X_i}(x) \neq 0$, et on peut alors appliquer le lemme d'Hensel pour relever x_i en un y_i tel que $f(x_1, \ldots, y_i, \ldots, x_n) = 0$ □

Pour montrer le théorème de Hasse-Minkowski, nous allons admettre deux résultats correspondant aux cas $n = 2$ et $n = 3$. On montrera ensuite ces deux résultats dans $\mathbb{Q}$ afin d'avoir une preuve complète du théorème dans ce corps, et une démonstration incomplète dans un corps de nombres quelconque.

Théorème 12. *Soit $\mathbb{K}$ un corps de nombres et Ω l'ensemble de ses places non triviales.*

Alors pour tout $a \in \mathbb{K}$:

$$a \in \mathbb{K}^2 \iff \forall \mathfrak{p} \in \Omega,\ a \in \mathbb{K}_\mathfrak{p}^2$$

Théorème 13. *Avec les mêmes notations, on a pour tout $a, b \in \mathbb{K}$:*

$$(a,b)_\mathbb{K} = 1 \iff \forall \mathfrak{p} \in \Omega,\ (a,b)_{\mathbb{K}_\mathfrak{p}} = 1$$

Preuve du théorème de Hasse-Minkowski

Si la forme quadratique f est dégénérée, le théorème est trivial. On supposera donc f non dégénérée.

Le cas $n = 1$ est trivial, car $f = \langle a \rangle$ ne représente jamais 0 sauf si elle est dégénérée.

Si f est de rang 2, on peut, quitte à la multiplier par un scalaire, supposer $f = \langle 1, a \rangle$. f représente alors 0 si et seulement si il existe un couple $(x, y) \in \mathbb{K}^2$ non nul tel que

$$x^2 + ay^2 = 0$$

Si $y = 0$ alors $x = 0$, ce qui est impossible. Donc $y \neq 0$, et l'équation se réécrit alors

$$\begin{aligned} -a &= \frac{x^2}{y^2} \\ \iff -a &\in \mathbb{K}^2 \end{aligned}$$

Le résultat découle alors directement du Théorème 12

De la même manière, le cas $n = 3$ est une conséquence directe du Théorème 13

Cas n=4

Références

[1] Fernando Q. Gouvêa, *p-adic numbers, an introduction*, Springer, 1997

[2] Jean-Pierre Serre, *Cours d'arithmétique*, PUF, 1994

[3] Pierre Samuel, *Théorie algébrique des nombres*, Hermann, 1997

[4] O. Timothy O'Meara, *Introduction to Quadratic Forms*, Springer, 2000

[5] T.Y Lam, *Introduction to Quadratic Forms over Fields*, AMS, 2004