

Exposé de maîtrise 1999-2000

\mathbb{Z} est simplement connexe

(Sujet proposé par Yves LASZLO)

par

Erwan BILAND

et

Xavier CARUSO

La théorie de la ramification présente deux aspects, l'un algébrique et l'autre topologique. Dans la théorie topologique, on montre qu'une surface S est simplement connexe si et seulement si tout revêtement non trivial de S se ramifie en au moins un point. Dans la théorie algébrique, on montre que tout corps de nombres distinct de \mathbb{Q} se ramifie en au moins un idéal premier. On relie les deux théories en étudiant les surfaces de Riemann et leurs corps de fonctions méromorphes. L'énoncé " \mathbb{Z} est simplement connexe" provient de cette analogie.

Table des matières

I	La ramification	3
1	Ramification et revêtement des surfaces	3
1.1	Surfaces topologiques	3
1.2	Surfaces de Riemann	4
2	Ramification et extensions de corps	4
2.1	Les anneaux de Dedekind	4
2.2	Ramification pour les anneaux principaux	6
II	Surfaces de Riemann et corps de fonctions méromorphes	9
3	Revêtements ramifiés et extensions étales	9
3.1	Le foncteur \mathcal{M}	9
3.2	Une équivalence de catégories	10
4	Lien avec la ramification	11
III	\mathbb{Z} est simplement connexe	13
5	Préliminaires	13
5.1	Réseaux sur un espace euclidien	13
5.2	Discriminant	15
5.3	Norme d'un idéal	16
6	Démonstration	17
6.1	Discriminant et ramification	17
6.2	L'espace de Minkowski	18
7	Compléments	20
7.1	Un résultat de finitude	20
7.2	Le théorème des unités	21
8	L'exemple de $\mathbb{Q}[\sqrt{d}]$	23
8.1	Cas où d n'est pas congru à 1 modulo 4	23
8.2	Cas où d est congru à 1 modulo 4	24
8.3	Extension au cas général	24

Première partie

La ramification

1 Ramification et revêtement des surfaces

Dans cette partie, on va définir deux théories de la ramification ; l'une est topologique et porte sur les revêtements de surfaces, l'autre est algébrique et concerne les extensions de corps.

1.1 Surfaces topologiques

Définition 1.1.1 On appelle surface topologique une variété topologique complexe de dimension 1.

Définition 1.1.2 Soient B et X des surfaces topologiques ; on appelle revêtement étale fini de B par X une application $\pi : X \rightarrow B$ telle que, pour tout $b \in B$, il existe un voisinage ouvert V de b et des ouverts $(U_i)_{1 \leq i \leq n}$ en nombre fini, disjoints deux à deux, tels que :

$$- \pi^{-1}(V) = \bigsqcup_{i=1}^n U_i$$

- pour tout i , $1 \leq i \leq n$, π induit un homéomorphisme de U_i sur V .

Définition 1.1.3 Avec les notations précédentes, l'application $b \mapsto n$ est localement constante. Donc si B est connexe, n ne dépend pas du point b choisi. On l'appelle le degré du revêtement.

On appelle D le disque unité ouvert de \mathbb{C} et $D^* = D - \{0\}$. On appelle carte centrée de X en x , une carte définie sur un voisinage de x à valeur dans D qui envoie x en 0.

Définition 1.1.4 Soient B et X des surfaces topologiques ; on appelle revêtement ramifié fini de B par X une application $\pi : X \rightarrow B$ telle que, pour tout $b \in B$, il existe un voisinage ouvert V de b et des ouverts $(U_i)_{1 \leq i \leq n}$ en nombre fini, disjoints deux à deux, tels que :

$$- \pi^{-1}(V) = \bigsqcup_{i=1}^n U_i$$

- pour tout i , $1 \leq i \leq n$, il existe $x_i \in U_i$ tel que $\pi(x_i) = b$ et des cartes complexes, $U_i \rightarrow D$ et $V \rightarrow D$, centrées respectivement en x_i et en b telles que l'application π s'écrive dans ces cartes $z \mapsto z^{d_i}$ avec $d_i \in \mathbb{N}^*$.

Définition 1.1.5 L'entier d_i défini précédemment ne dépend que de x_i . On l'appelle l'indice de ramification de π en x_i .

Définition 1.1.6 On dit que π se ramifie en $b \in B$ s'il existe un point x au dessus de b d'indice de ramification strictement supérieur à 1. L'ensemble des points où π se ramifie est appelé l'ensemble de ramification de π . C'est une partie fermée discrète de B .

Définition 1.1.7 L'application $b \mapsto \sum d_i$ est localement constante. Donc si on suppose que B est connexe, on définit de même que précédemment le degré d'un revêtement ramifié fini.

La notion de revêtement ramifié fini découle naturellement de la notion de revêtement étale fini comme le montre le théorème suivant :

Théorème 1.1.1 Soit B une surface topologique, Δ une partie fermée discrète dans B et $\pi : X \rightarrow B - \Delta$ un revêtement étale fini. Alors il existe une surface topologique $\tilde{X} \supset X$ et un revêtement ramifié fini $\tilde{\pi} : \tilde{X} \rightarrow B$ prolongeant π . De plus $\tilde{X} - X$ est une partie fermée discrète de \tilde{X} .

Démonstration. Faisons-le tout d'abord dans le cas où $B = D$ et $\Delta = \{0\}$. Quitte à raisonner séparément sur chaque composante connexe, on peut supposer que X est connexe. On prend $\pi : X \rightarrow D - \{0\}$ un revêtement fini de degré d et f l'application de D^* dans lui-même qui à z associe z^d . Soient $b_0 \in D^*$, x_0 un point au-dessus de b_0 et $\bar{x}_0 \in D^*$, tel que $f(\bar{x}_0) = b_0$. L'application $\pi_* : \pi_1(X, x_0) \rightarrow \pi_1(D^*, b_0)$ est injective. En identifiant $\pi_1(D^*, b_0)$ à \mathbb{Z} , l'image de π_* est $d\mathbb{Z}$. En effet, si $[\alpha]$ désigne un générateur de $\pi_1(D^*, b_0)$, $[\alpha]$ agit sur la fibre au-dessus de b_0 par un cycle d'ordre d . De même $f_* : \pi_1(D^*, \bar{x}_0) \rightarrow \pi_1(D^*, b_0)$ a pour image $d\mathbb{Z}$. Prenons alors u un lacet de X d'origine x_0 . On considère $v = \pi \circ u$ qui est un lacet dans D^* d'origine b_0 . On peut le relever en un chemin \bar{u} d'origine \bar{x}_0 dans D^* . Les propriétés de π_* et de f_* prouvent alors que \bar{u} est un lacet.

On peut ainsi définir une application ψ de la façon suivante. Soit $x \in X$. Considérons u un chemin reliant x_0 à x . On considère $v = \pi \circ u$ et \bar{u} le relèvement de v d'origine \bar{x}_0 . En posant $\psi(x) = \bar{u}(1)$, on vient de voir que $\psi(x)$ ne dépend pas du choix du chemin u . L'application ψ ainsi définie est continue grâce à la continuité du relèvement. Comme on peut faire la même opération dans l'autre sens, on en déduit que ψ est un homéomorphisme. On a ainsi le diagramme commutatif suivant :

$$\begin{array}{ccc} X & \xrightarrow{\psi} & D^* \\ \pi \searrow & & \swarrow z \mapsto z^d \\ & D^* & \end{array}$$

On pose alors $\tilde{X} = X \sqcup \{\tilde{x}\}$ et on prolonge la topologie de sorte que $\tilde{\psi}$ prolongée en \tilde{x} par 0 reste un homéomorphisme. On prolonge également π en $\tilde{\pi}$ en posant $\tilde{\pi}(\tilde{x}) = 0$. $\tilde{\pi}$ est alors un revêtement ramifié fini de degré d de D .

Pour le cas général, on considère $(V_b)_{b \in \Delta}$ des ouverts disjoints de B tels que $b \in V_b$. On choisit des cartes centrées en b , $\psi_b : V_b \rightarrow D$ et on se ramène ainsi au cas précédent. \square

1.2 Surfaces de Riemann

Définition 1.2.1 On appelle surface de Riemann une variété analytique complexe de dimension 1.

On dispose du théorème très important :

Théorème 1.2.1 Soient B une surface de Riemann, X une surface topologique et $\pi : X \rightarrow B$ un revêtement ramifié fini. Alors il existe une unique structure de surface de Riemann sur X telle que π soit holomorphe.

Démonstration. Soit Δ l'ensemble de ramification de π . On se place tout d'abord dans le cas $B = D$, $\Delta = \{0\}$ et X connexe. On note d le degré de $\pi : X \rightarrow D$. On retrouve la situation du théorème 1.1.1 pour $\pi : X - \pi^{-1}(0) \rightarrow D^*$. On construit alors une carte $\psi : X \rightarrow D$ comme précédemment. ψ définit une structure analytique sur X . On remarque que ψ ainsi définie est unique modulo les rotations d'angle $\frac{2k\pi}{d}$.

On se ramène au cas général comme précédemment en découpant B en domaines de cartes centrées sur lesquels π ne se ramifie qu'au centre. On dispose alors d'un atlas sur X et la remarque que l'on vient de faire montre que les changements de cartes sont analytiques.

Si on choisit deux structures holomorphes σ et σ' sur X , alors on vérifie que l'application identité de (X, σ) dans (X, σ') est holomorphe et donc les deux structures sont équivalentes. \square

2 Ramification et extensions de corps

2.1 Les anneaux de Dedekind

Définition 2.1.1 (Anneau noëthérien) On dit qu'un anneau A est noëthérien s'il satisfait à l'une des trois conditions équivalentes suivantes :

- i) Tout idéal de A est engendré par un nombre fini d'éléments (ie tout idéal de A est un A -module de type fini).
- ii) Toute suite croissante d'idéaux de A est stationnaire.
- iii) Toute famille non vide d'idéaux de A admet un élément maximal.

Lemme 2.1.1 Soit A un anneau noëthérien intègre. Alors tout idéal non nul de A contient un produit d'idéaux premiers non nuls.

Démonstration. Notons Φ l'ensemble des idéaux non nuls de A ne vérifiant pas la propriété énoncée et supposons que $\Phi \neq \emptyset$.

Comme A est noëthérien, Φ possède un élément maximal. Notons-le \mathfrak{a} . Alors \mathfrak{a} n'est pas un idéal premier donc il existe x et y n'appartenant pas à \mathfrak{a} tels que $xy \in \mathfrak{a}$. On en déduit, par maximalité, que $\mathfrak{a} + Ax \notin \Phi$ et donc on peut écrire $\mathfrak{a} + Ax \supset \mathfrak{p}_1 \dots \mathfrak{p}_m$. De même on a $\mathfrak{a} + Ay \supset \mathfrak{q}_1 \dots \mathfrak{q}_n$.

On en déduit que $\mathfrak{a} \supset (\mathfrak{a} + Ax)(\mathfrak{a} + Ay) \supset \mathfrak{p}_1 \dots \mathfrak{p}_m \mathfrak{q}_1 \dots \mathfrak{q}_n$, ce qui contredit le fait que $\mathfrak{a} \in \Phi$. □

Lemme 2.1.2 Soit A un anneau noëthérien. Alors tout idéal de A contient un produit d'idéaux premiers.

Démonstration. Comme précédemment. □

Définition 2.1.2 Soit A un anneau intègre. Soit K son corps des fractions. On dit que A est intégralement clos si les seuls éléments de K qui sont entiers sur A (ie qui sont racines d'un polynôme unitaire à coefficients dans A) sont les éléments de A .

Définition 2.1.3 (Anneau de Dedekind) Un anneau A est dit de Dedekind s'il est noëthérien, intégralement clos et si tout idéal premier non nul de A est maximal.

Par exemple, tout anneau principal est un anneau de Dedekind.

Définition 2.1.4 (Idéal fractionnaire) Soit A un anneau intègre. On note K son corps des fractions. On appelle idéal fractionnaire \mathfrak{a} de A tout A -module inclus dans K tel qu'il existe $d \in A$ vérifiant $\mathfrak{a} \subset d^{-1}A$. Les idéaux de A sont des idéaux fractionnaires de A (en effet, on peut choisir $d = 1$). On les appelle parfois des idéaux entiers.

Lemme 2.1.3 Soit A un anneau de Dedekind. Soit \mathfrak{p} un idéal premier non nul de A , alors il existe un unique idéal fractionnaire de A , \mathfrak{p}' tel que $\mathfrak{p}\mathfrak{p}' = A$.

Remarque 2.1.1 \mathfrak{p}' est noté \mathfrak{p}^{-1}

Démonstration. Posons $\mathfrak{p}' = \{x \in K/x\mathfrak{p} \subset A\}$. C'est un idéal fractionnaire de A (en effet, tout élément x non nul de \mathfrak{p} vérifie $x\mathfrak{p}' \subset A$).

Montrons tout d'abord que $\mathfrak{p}' \neq A$. En effet, soit $x \neq 0$ appartenant à \mathfrak{p} . D'après le lemme 2.1.1, on peut écrire $Ax \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$. On peut choisir n minimal. On a alors $\mathfrak{p} \supset Ax \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$ et donc il existe j tel que $\mathfrak{p} \supset \mathfrak{p}_j$. Par maximalité, on obtient $\mathfrak{p} = \mathfrak{p}_j$. On peut supposer $j = 1$. Posons maintenant $\mathfrak{b} = \mathfrak{p}_2 \dots \mathfrak{p}_n$ de sorte que l'on a $Ax \supset \mathfrak{p}\mathfrak{b}$ et $Ax \not\supset \mathfrak{b}$ (par minimalité de n). Considérons donc $y \in \mathfrak{b} - Ax$. On a alors $yx^{-1} \notin A$ et $\mathfrak{p}y \subset \mathfrak{p}\mathfrak{b} \subset Ax$ et donc, par définition de \mathfrak{p}' , $yx^{-1} \in \mathfrak{p}'$. On en déduit finalement que $\mathfrak{p}' \neq A$.

On vérifie que $\mathfrak{p}\mathfrak{p}' \subset A$. D'autre part, $A \subset \mathfrak{p}'$ et donc $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}'$ puis par maximalité $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$ ou $\mathfrak{p}\mathfrak{p}' = A$.

Supposons que $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$. Soit $x \in \mathfrak{p}'$, alors pour tout n , on a $x^n\mathfrak{p} \subset \mathfrak{p}$. On en déduit que $A[x]$ est un idéal fractionnaire. En effet, tout élément d non nul de \mathfrak{p} vérifie alors $A[x] \subset d^{-1}A$. Mais $d^{-1}A$ est un A -module de type fini donc $A[x]$ est un A -module de type fini (car A est noëthérien), ce qui prouve que x est entier sur A puis est un élément de A (car A est intégralement clos). On en déduit que $\mathfrak{p}' = A$, ce qui est faux.

Finalement, on a bien $\mathfrak{p}\mathfrak{p}' = A$. □

Théorème 2.1.4 Soit A un anneau de Dedekind, alors tout idéal fractionnaire non nul \mathfrak{a} de A s'écrit, de façon unique, comme produit d'idéaux premiers de A . C'est-à-dire :

$$\mathfrak{a} = \prod_{\mathfrak{p} \text{ premier}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})} \quad (\text{où les } n_{\mathfrak{p}}(\mathfrak{a}) \text{ sont des entiers relatifs presque tous nuls})$$

Démonstration. Remarquons tout d'abord que, via l'égalité $\mathfrak{a} = (d\mathfrak{a})(Ad)^{-1}$, on peut supposer que \mathfrak{a} est un idéal entier (ie un idéal de A).

Notons Φ l'ensemble des idéaux entiers de A qui ne s'écrivent pas comme produit d'idéaux premiers et supposons que $\Phi \neq \emptyset$. Alors, comme A est noëthérien, Φ admet un élément maximal \mathfrak{a} . On a bien entendu $\mathfrak{a} \neq A$ donc d'après le théorème de Krull, il existe \mathfrak{p} un idéal premier de A tel que $\mathfrak{a} \subset \mathfrak{p}$. On a alors $\mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = A$ et $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$ (car $A \subset \mathfrak{p}^{-1}$ car $\mathfrak{p} \subset A$). On montre comme dans la preuve précédente que l'on ne peut pas avoir $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$ et donc on obtient $\mathfrak{a}\mathfrak{p}^{-1} \notin \Phi$ de sorte que l'on peut écrire $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_n$ puis $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_n$, ce qui est absurde. On en déduit que $\Phi = \emptyset$, ce qui prouve l'existence de la décomposition.

Pour montrer l'unicité, il suffit de voir que $\left(\prod_{\mathfrak{p} \text{ premier}} \mathfrak{p}^{n_{\mathfrak{p}}} = A \right)$ implique $n_{\mathfrak{p}} = 0$ pour tout \mathfrak{p} . Supposons que ce n'est pas le cas. Alors regroupant les puissances positives et les puissances négatives, on obtient l'égalité $\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_m^{\alpha_m} = \mathfrak{q}_1^{\beta_1} \dots \mathfrak{q}_n^{\beta_n}$ où tous les exposants ainsi que m et n sont strictement positifs et tous les idéaux premiers qui apparaissent sont distincts. Mais alors on a $\mathfrak{p}_1 \supset \mathfrak{q}_1^{\beta_1} \dots \mathfrak{q}_n^{\beta_n}$ et donc il existe un entier j tel que $\mathfrak{p}_1 \supset \mathfrak{q}_j$ et puis par maximalité $\mathfrak{p}_1 = \mathfrak{q}_j$, ce qui est supposé faux. \square

Ceci peut s'interpréter en disant que, de même que tout nombre d'un anneau principal peut se décomposer en produit de nombres premiers, tout idéal d'un anneau de Dedekind peut se décomposer en produit d'idéaux premiers.

Corollaire 2.1.5 L'ensemble des idéaux fractionnaires non nuls d'un anneau de Dedekind forme un groupe.

Proposition 2.1.6 (Formulaire) Soit \mathfrak{p} un idéal premier de A , un anneau de Dedekind. Soient \mathfrak{a} et \mathfrak{b} deux idéaux fractionnaires de A . On a alors les formules suivantes :

- i) $n_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = n_{\mathfrak{p}}(\mathfrak{a}) + n_{\mathfrak{p}}(\mathfrak{b})$
- ii) $\mathfrak{a} \subset A \Rightarrow n_{\mathfrak{p}}(\mathfrak{a}) \geq 0$
- iii) $\mathfrak{a} \subset \mathfrak{b} \Rightarrow n_{\mathfrak{p}}(\mathfrak{a}) \geq n_{\mathfrak{p}}(\mathfrak{b})$
- iv) $n_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \inf(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b}))$
- v) $n_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \sup(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b}))$

Démonstration.

- i) est essentiellement trivial.
- ii) a été démontré dans le théorème précédent.
- iii) vient du fait que $\mathfrak{a} \subset \mathfrak{b}$ équivaut à $\mathfrak{a}\mathfrak{b}^{-1} \subset A$.
- iv) vient du fait que $\mathfrak{a} + \mathfrak{b}$ est la borne supérieure pour l'inclusion de $\{\mathfrak{a}, \mathfrak{b}\}$
- v) vient du fait que $\mathfrak{a} \cap \mathfrak{b}$ est la borne inférieure pour l'inclusion de $\{\mathfrak{a}, \mathfrak{b}\}$

\square

2.2 Ramification pour les anneaux principaux

On considère ici un anneau principal \mathfrak{o} . On note k son corps des fractions. On considère alors K une extension finie séparable de degré n de k et \mathcal{O} l'anneau des entiers de K sur \mathfrak{o} . On a alors le diagramme commutatif suivant :

$$\begin{array}{ccc}
\mathcal{O} & \longrightarrow & K \\
\uparrow & \circlearrowleft & \uparrow n \\
\mathfrak{o} & \longrightarrow & k
\end{array}$$

Définition 2.2.1 On définit le spectre d'un anneau A comme l'ensemble des ses idéaux premiers non nuls. On le note $\text{Spec}(A)$.

Lemme 2.2.1 Soit $\mathfrak{p} \in \text{Spec}(\mathcal{O})$, alors $\mathfrak{p} \cap \mathfrak{o} \in \text{Spec}(\mathfrak{o})$ et \mathcal{O}/\mathfrak{p} est une extension du corps $\mathfrak{o}/(\mathfrak{p} \cap \mathfrak{o})$.

Démonstration. L'homomorphisme $\mathfrak{o} \longrightarrow \mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}$ a pour noyau $\mathfrak{p} \cap \mathfrak{o}$ et donc se factorise de la façon suivante (où φ est injectif) :

$$\begin{array}{ccccc}
\mathfrak{o} & \longrightarrow & \mathcal{O} & \longrightarrow & \mathcal{O}/\mathfrak{p} \\
& \searrow & & \nearrow \varphi & \\
& & \mathfrak{o}/(\mathfrak{p} \cap \mathfrak{o}) & &
\end{array}$$

On en déduit que $\mathfrak{o}/(\mathfrak{p} \cap \mathfrak{o})$ peut se voir comme un sous-anneau de l'anneau intègre \mathcal{O}/\mathfrak{p} . Il est donc intègre, ce qui prouve que $\mathfrak{p} \cap \mathfrak{o}$ est un idéal premier de \mathfrak{o} .

Soit $x \in \mathfrak{p}$, $x \neq 0$. On a alors une équation de dépendance intégrale $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ où les $a_i \in \mathfrak{o}$. Quitte à diviser par x , on peut supposer $a_0 \neq 0$. Mais on a alors $a_0 \in \mathcal{O}x \cap \mathfrak{o} \subset \mathfrak{p} \cap \mathfrak{o}$ donc $\mathfrak{p} \cap \mathfrak{o}$ est un idéal premier non nul de \mathfrak{o} .

Il ne reste plus qu'à montrer que \mathcal{O}/\mathfrak{p} est un corps. Soit donc $\bar{x} \in \mathcal{O}/\mathfrak{p}$, $\bar{x} \neq 0$. x est entier sur \mathfrak{o} donc \bar{x} est entier sur $\mathfrak{o}/(\mathfrak{p} \cap \mathfrak{o})$, on a ainsi une équation de dépendance intégrale (où on peut supposer $\bar{a}_0 \neq 0$) :

$$\begin{aligned}
\bar{x}^n + \bar{a}_{n-1} \bar{x}^{n-1} + \dots + \bar{a}_0 &= 0 \quad \text{avec} \quad \bar{a}_i \in \mathfrak{o}/(\mathfrak{p} \cap \mathfrak{o}) \\
\bar{x} \left(-\frac{\bar{a}_{n-1}}{\bar{a}_0} \bar{x}^{n-1} - \dots - \frac{\bar{a}_1}{\bar{a}_0} \right) &= 1
\end{aligned}$$

ce qui prouve que \bar{x} est inversible. □

Théorème 2.2.2 \mathcal{O} est un \mathfrak{o} -module libre de dimension n .

Démonstration. Soit $x \in K$, alors il existe un polynôme à coefficients dans \mathfrak{o} qui annule x ie $a_m x^m + \dots + a_0 = 0$ puis $(a_m x)^m + a_{m-1} (a_m x)^{m-1} + \dots + a_0 a_m^{m-1} = 0$, ce qui prouve que $a_m x \in \mathcal{O}$.

On peut donc trouver (x_1, \dots, x_n) une base de K sur k telle que tous les x_i appartiennent à \mathcal{O} . Comme l'extension est séparable, la trace est non dégénérée et on peut donc considérer la base duale (y_1, \dots, y_n) .

Soit $z \in \mathcal{O}$. On peut alors écrire $z = \sum_{j=1}^n \alpha_j y_j$ avec $\alpha_j \in k$. Par dualité, on a $\text{Tr}(x_i z) = \alpha_i$. D'autre part,

$x_i z \in \mathcal{O}$ donc $\text{Tr}(x_i z) \in k \cap \mathcal{O} = \mathfrak{o}$, ce qui prouve que $\alpha_i \in \mathfrak{o}$ et donc $\mathcal{O} \subset \bigoplus_{j=1}^n y_j \mathfrak{o}$. On en déduit que \mathcal{O} est

un \mathfrak{o} -module libre de dimension inférieure ou égale à n .

Mais on a vu que (x_1, \dots, x_n) est une famille libre sur k et donc sur \mathfrak{o} d'éléments de \mathcal{O} . Donc finalement, \mathcal{O} est de dimension n . □

Théorème 2.2.3 \mathcal{O} est un anneau de Dedekind.

Démonstration. Soit \mathfrak{a} un idéal de \mathcal{O} . \mathfrak{a} est alors un \mathfrak{o} -module inclus dans \mathcal{O} . \mathfrak{a} est donc de type fini sur \mathfrak{o} et donc sur \mathcal{O} . Ceci prouve que \mathcal{O} est noëthérien.

D'autre part \mathcal{O} est intégralement clos.

Considérons \mathfrak{p} un idéal premier non nul de \mathcal{O} . Alors comme nous l'avons vu dans la démonstration du lemme 2.2.1, \mathcal{O}/\mathfrak{p} est un corps, ce qui prouve que \mathfrak{p} est maximal. □

On a introduit tous les outils indispensables à la théorie algébrique de la ramification. Passons maintenant à l'exposé de cette théorie.

Soit p un nombre premier de \mathfrak{o} (ie l'idéal $p\mathfrak{o}$ est premier). Alors $p\mathcal{O}$ est un idéal non nul de \mathcal{O} (car il contient $p\mathfrak{o}$) et donc on a la décomposition (unique) :

$$p\mathcal{O} = \prod_{i=1}^q \mathfrak{p}_i^{e_i}$$

où les \mathfrak{p}_i sont des idéaux premiers de \mathcal{O} deux à deux distincts et les e_i sont des entiers strictement positifs.

Définition 2.2.2 e_i s'appelle l'indice de ramification de \mathfrak{p}_i sur \mathfrak{o} .

Définition 2.2.3 On dit que K se ramifie en p , s'il existe un i tel que $e_i > 1$.

Proposition 2.2.4 Les \mathfrak{p}_i sont exactement les idéaux premiers \mathfrak{p} de \mathcal{O} tels que $\mathfrak{p} \cap \mathfrak{o} = p\mathfrak{o}$.

Démonstration. Soit \mathfrak{p} un idéal premier non nul de \mathcal{O} .

Supposons que $\mathfrak{p} \supset p\mathcal{O}$, alors $\mathfrak{p} \cap \mathfrak{o}$ est un idéal premier de \mathfrak{o} contenant p , donc $\mathfrak{p} \cap \mathfrak{o} = p\mathfrak{o}$. Réciproquement, si $\mathfrak{p} \cap \mathfrak{o} = p\mathfrak{o}$, alors $p \in \mathfrak{p}$ et donc $\mathfrak{p} \supset p\mathcal{O}$.

D'autre part, d'après les formules sur les anneaux de Dedekind, on a $\mathfrak{p} \supset p\mathcal{O}$, si et seulement si $n_{\mathfrak{p}}(p\mathcal{O}) \geq 1$.

On en déduit la proposition énoncée. \square

Définition 2.2.4 On en déduit que l'on a l'extension de corps $\mathfrak{o}/p\mathfrak{o} \rightarrow \mathcal{O}/\mathfrak{p}_i$. Son degré s'appelle le degré résiduel de \mathfrak{p}_i sur \mathfrak{o} et est noté f_i .

Nous allons voir que la notion introduite correspond bien à la notion de revêtements ramifiés finis. Cette affirmation découle immédiatement du théorème suivant :

Théorème 2.2.5 Avec les notations précédentes, on a $\sum_{i=1}^q e_i f_i = n$

Démonstration. Montrons tout d'abord que si \mathfrak{p} est un idéal premier non nul de \mathcal{O} (en fait de n'importe quel anneau de Dedekind) et si \mathfrak{a} est un idéal de \mathcal{O} , alors $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ est un espace vectoriel de dimension 1 sur \mathcal{O}/\mathfrak{p} . En effet, soit E un sous-espace vectoriel de $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$, alors E est de la forme $\mathfrak{b}/\mathfrak{a}\mathfrak{p}$ où $\mathfrak{a}\mathfrak{p} \subset \mathfrak{b} \subset \mathfrak{a}$. D'après les formules sur les anneaux de Dedekind, on obtient $\mathfrak{b} = \mathfrak{a}$ (soit $E = \mathfrak{a}/\mathfrak{a}\mathfrak{p}$) ou $\mathfrak{b} = \mathfrak{a}\mathfrak{p}$ (soit $E = 0$). On en déduit la propriété voulue.

Montrons alors que $\sum_{i=1}^q e_i f_i = \dim_{\mathfrak{o}/p\mathfrak{o}} \mathcal{O}/p\mathcal{O}$. Pour cela, on écrit la suite d'inclusion suivante :

$$\mathcal{O} \supset \mathfrak{p}_1 \supset \dots \supset \mathfrak{p}_1^{e_1} \supset \mathfrak{p}_1^{e_1} \mathfrak{p}_2 \supset \dots \supset \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \supset \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_q^{e_q} = p\mathcal{O}$$

Par la propriété précédente, on en déduit que le quotient de deux idéaux consécutifs qui apparaît dans cette décomposition est de dimension 1 sur $\mathcal{O}/\mathfrak{p}_i$ et donc de dimension f_i sur $\mathfrak{o}/p\mathfrak{o}$, d'où le résultat annoncé.

Considérons pour finir (x_1, \dots, x_n) une base de \mathcal{O} en tant que \mathfrak{o} -module. On obtient alors, en réduisant modulo $p\mathcal{O}$, une base de $\mathcal{O}/p\mathcal{O}$ comme $\mathfrak{o}/p\mathfrak{o}$ -espace vectoriel ce qui prouve que $\dim_{\mathfrak{o}/p\mathfrak{o}} \mathcal{O}/p\mathcal{O} = n$ et achève la démonstration. \square

Remarque 2.2.1 Dans tout ce paragraphe, nous avons supposé que \mathfrak{o} était un anneau principal pour simplifier les démonstrations. Cependant, tous les résultats énoncés précédemment restent vrais si on suppose seulement que \mathfrak{o} est un anneau de Dedekind. Pour plus de détails, se reporter à [1].

Deuxième partie

Surfaces de Riemann et corps de fonctions méromorphes

3 Revêtements ramifiés et extensions étales

On s'intéresse désormais aux surfaces de Riemann connexes compactes. Etant donné X une telle surface de Riemann, on note $\mathcal{M}(X)$ son corps des fonctions méromorphes. Si $\pi : X \rightarrow B$, avec X et B deux surfaces de Riemann connexes compactes, est un revêtement ramifié fini analytique, on a un plongement $\pi^* : \mathcal{M}(B) \rightarrow \mathcal{M}(X)$ qui fait de $\mathcal{M}(X)$ une extension du corps $\mathcal{M}(B)$. On montre que \mathcal{M} constitue un foncteur de la catégorie des revêtements ramifiés finis de B dans la catégorie des extensions finies de $\mathcal{M}(B)$ et que ce foncteur est une équivalence de catégories. Nous nous contenterons de prouver partiellement ces propriétés.

3.1 Le foncteur \mathcal{M}

On admet le théorème suivant, dont la démonstration fait appel à l'analyse :

Théorème 3.1.1 (Théorème de séparation) *Soit X une surface de Riemann compacte, soient a et b des points distincts de X ; alors il existe une fonction méromorphe f sur X définie en a et b et telle que $f(a) \neq f(b)$.*

Corollaire 3.1.2 *Soit X une surface de Riemann compacte, soient $a_1 \dots a_d$ des points distincts de X ; alors il existe une fonction méromorphe f sur X définie en tous les a_i et telle que les valeurs $f(a_i)$ soient deux à deux distinctes.*

Démonstration. Pour tout couple $1 \leq i < j \leq d$, il existe une fonction f méromorphe sur X , définie en $a_1 \dots a_d$ et telle que $f(a_i) \neq f(a_j)$. En effet, le théorème de séparation nous fournit une fonction g méromorphe sur X définie en a_i et a_j avec $g(a_i) \neq g(a_j)$; quitte à ajouter une constante, on peut supposer que g ne s'annule pas sur $a_1 \dots a_d$, auquel cas $f = 1/g$ convient. Si maintenant on note A le sous-espace vectoriel (non nul) de $\mathcal{M}(X)$ constitué des fonctions méromorphes définies aux points $a_1 \dots a_d$, et A_{ij} le sous-espace des $f \in A$ tels que $f(a_i) = f(a_j)$, on vient de montrer $A_{ij} \neq A$, donc $\bigcup A_{ij} \neq A$. Toute fonction $f \in A - \bigcup A_{ij}$ répond à la question. \square

Théorème 3.1.3 *Soient B et X deux surfaces de Riemann connexes compactes et $\pi : X \rightarrow B$ un revêtement analytique de degré d de B par X . Alors $\mathcal{M}(X)$ est une extension finie de degré d de $\mathcal{M}(B)$.*

Démonstration. Soit $f \in \mathcal{M}(X)$. Montrons que f est algébrique sur $\mathcal{M}(B)$ de degré au plus d , en exhibant un polynôme annulateur de f de degré d . On note $\Delta \subset B$ l'image par π de l'ensemble des pôles de f . Pour $b \in B - \Delta$, on note $x_1 \dots x_d$ les antécédents de b par π (comptés avec leur indice de ramification); soient $a_i(b)$ les valeurs en $f(x_1) \dots f(x_d)$ des fonctions symétriques élémentaires :

$$a_0(b) = 1, \quad a_1(b) = \sum f(x_j), \quad \dots, \quad a_n(b) = \prod f(x_j)$$

On a clairement, pour tout i , $a_i \in \mathcal{M}(B)$. Posons $P(Z) = \sum_i (-1)^i a_i Z^{d-i} \in \mathcal{M}(B)[Z]$ et montrons $P(f) = 0$. C'est clair car les $f(x_j)$ sont justement les racines de $P_b(Z) = \sum_i (-1)^i a_i(b) Z^{d-i}$.

Montrons que $\mathcal{M}(X)$ est étale de degré au plus d . $\mathcal{M}(X)$ est réunion filtrante des sous-extensions E de type fini de $\mathcal{M}(B)$. Comme les E sont de type fini et que leurs générateurs sont algébriques, ce sont des extensions finies donc étales (car $\mathcal{M}(B)$ est de caractéristique nulle), donc monogènes d'après le théorème de l'élément primitif, donc de degré au plus d . Par conséquent $\mathcal{M}(X)$ est de degré au plus d .

Montrons que le degré de $\mathcal{M}(X)$ est supérieur à d . Soit $b_0 \in B$ un point où le revêtement est non ramifié, et soient $x_1 \dots x_d$ les points de X au dessus de B (tous distincts donc). D'après le théorème de séparation, il existe $f \in \mathcal{M}(X)$ définie en les $x_1 \dots x_d$ et prenant en ces points des valeurs distinctes. Soit $P = \sum_{i=0}^k c_i Z^i$ un polynôme annulateur non nul de f , $c_i \in \mathcal{M}(B)$ pour tout i . L'ensemble des pôles des c_i est discret dans B , ainsi que l'ensemble de ramification du revêtement, donc il existe un voisinage V de b_0 tel que $V - \{b_0\}$ ne rencontre pas ces ensembles et tel que pour tout $b \in V - \{b_0\}$, la fonction f prend des valeurs distinctes en les points de $\pi^{-1}(b)$. Ces valeurs sont alors toutes racines de $P_b(Z)$, qui par conséquent est nul ou de degré supérieur à d . Mais si les c_i s'annulent en tout point de $V - \{b_0\}$, c'est qu'ils sont nuls partout, ce qui contredit $P \neq 0$, donc on a montré que le degré de P est au moins d . \square

3.2 Une équivalence de catégories

Lemme 3.2.1 Soient B un espace topologique et $b \mapsto P_b$ une application continue de B dans $\mathbb{C}_d[Z]$, l'espace des polynômes à coefficients dans \mathbb{C} de degré inférieur ou égal à d . On suppose que pour tout $b \in B$, P_b admet d racines distinctes dans \mathbb{C} . On pose $X = \{(b, z) \in B \times \mathbb{C} \mid P_b(z) = 0\}$.

Alors $\pi : \begin{pmatrix} X & \longrightarrow & B \\ (b, z) & \longmapsto & b \end{pmatrix}$ est un revêtement de degré d de B .

Démonstration. C'est une application directe du théorème des fonctions implicites. \square

Lemme 3.2.2 Soit $P(Z) = Z^d + a_1 Z^{d-1} + \dots + a_d \in \mathbb{C}[Z]$ et z une racine de P , alors $|z| \leq \sup(1, |a_1| + \dots + |a_d|)$

Démonstration. Si $|z| > 1$, on écrit $z = -a_1 - \frac{a_2}{z} \dots - \frac{a_d}{z^{d-1}}$ et on obtient $|z| \leq |a_1| + \dots + |a_d|$. \square

Théorème 3.2.3 Soit B une surface de Riemann connexe. Soit E une extension finie de $\mathcal{M}(B)$. Alors il existe une surface de Riemann X et un revêtement ramifié $\pi : X \rightarrow B$ tels que le diagramme suivant commute :

$$\begin{array}{ccc} \mathcal{M}(X) & \xleftarrow[\phi]{\sim} & E \\ & \searrow & \nearrow \\ & \mathcal{M}(B) & \end{array}$$

π^*

Démonstration. D'après le théorème de l'élément primitif, il existe $\zeta \in E$ tel que $E = \mathcal{M}(B)[\zeta]$. Soit $P(Z) = Z^d + a_1 Z^{d-1} + \dots + a_d$ le polynôme minimal de ζ où les $a_i \in \mathcal{M}(B)$. On définit $P_b(Z) = Z^d + a_1(b)Z^{d-1} + \dots + a_d(b)$. Considérons Δ l'ensemble des points $b \in B$ pour lesquels $a_i(b)$ n'est pas défini ou P_b n'est pas séparable.

Comme E est une extension étale, P est séparable et donc P et P' sont premiers entre eux ainsi leur résultant est non nul : On en déduit que l'ensemble des points d'annulation du résultant de P_b et P'_b est un fermé discret, ainsi l'ensemble des $b \in B$ pour lesquels P_b n'est pas séparable est également un fermé discret et donc Δ aussi.

Considérons donc $X = \{(b, z) \in (B - \Delta) \times \mathbb{C} \mid P_b(z) = 0\}$ et $\pi : \begin{pmatrix} X & \longrightarrow & B - \Delta \\ (b, z) & \longmapsto & b \end{pmatrix}$. D'après le lemme

3.2.1, π est un revêtement. En appliquant alors le théorème 1.1.1, on voit que l'on peut le prolonger en $\tilde{\pi} : \tilde{X} \rightarrow B$ un revêtement ramifié topologique. Finalement le théorème 1.2.1 prouve qu'il existe une unique structure holomorphe sur \tilde{X} rendant $\tilde{\pi}$ holomorphe.

Considérons Z l'application qui à $(b, z) \in X$ associe z . Comme π est localement un homéomorphisme biholomorphe, Z est holomorphe sur X . Soient $b \in \Delta$ et $x \in \pi^{-1}(b)$. Soient φ une carte de B centrée en b et ψ une carte de X centrée en x telles que π s'écrive dans ces cartes $z \mapsto z^r$. Si P désigne toujours le polynôme minimal de ζ , pour x' voisin de x et $b' = \pi(x')$, on a $P_{b'}(Z(x')) = 0$ d'où, d'après le lemme 3.2.1, $|Z(x')| \leq \sup(1, |a_1(b)|, \dots, |a_d(b)|)$. En passant dans les cartes, on obtient $a_i(b') = \bar{a}_i(\varphi(b')) = \bar{a}_i(\psi(x')^r)$, et comme les a_i sont méromorphes, il existe $C_i > 0$ et $n_i \in \mathbb{Z}$ tels que $|a_i(b')| \leq C_i |\psi(x') - \psi(x)|^{n_i}$. Il existe donc $C > 0$ et $n \in \mathbb{Z}$ tels que $|Z(x')| \leq C |\psi(x') - \psi(x)|^n$ au voisinage de x et alors Z est méromorphe en x si bien que $Z \in \mathcal{M}(X)$.

Considérons alors le morphisme d'anneaux $\phi : E \rightarrow \mathcal{M}(X)$ défini par $\phi(\zeta) = Z$, qui est bien défini car $P(Z) = 0$. Il fait bien commuter le diagramme précédent, reste à montrer qu'il est bijectif. Pour l'injectivité, il suffit de montrer que P est le polynôme minimal de Z , et c'est clair car si $b \in B - \Delta$ et si $\pi^{-1}(b) = \{x_1, \dots, x_d\}$, Z prend des valeurs toutes différentes en les x_i (voir démonstration du théorème 3.1.3. La surjectivité provient de l'égalité des degrés. □

4 Lien avec la ramification

Soit $\mathbb{S}^2 = \mathbb{C} \cup \{\infty\}$.

On prend ici $\mathfrak{o} = \mathbb{C}[\mathbb{S}^2]$, l'anneau des fonctions méromorphes sur la sphère de Riemann et holomorphes sur \mathbb{C} . Il s'agit en fait de l'ensemble des polynômes à coefficients dans \mathbb{C} . C'est donc un anneau principal. Son corps des fractions est $k = \mathcal{M}(\mathbb{S}^2)$ qu'on note ici $\mathbb{C}(\mathbb{S}^2)$.

On a vu que se donner un revêtement ramifié fini de degré n de \mathbb{S}^2 par une surface de Riemann connexe compacte X équivaut à se donner une extension finie K de degré n de $\mathcal{M}(\mathbb{S}^2)$. On a alors :

$$\begin{array}{ccc} \mathcal{O}_X & \longrightarrow & \mathbb{C}(X) \\ \uparrow & & \uparrow n \\ \mathbb{C}[\mathbb{S}^2] & \longrightarrow & \mathbb{C}(\mathbb{S}^2) \end{array} \qquad \begin{array}{c} X \\ \downarrow \pi \\ \mathbb{S}^2 \end{array}$$

Proposition 4.0.1 *L'anneau des entiers \mathcal{O}_X est l'anneau des fonctions méromorphes sur X et holomorphes sur $X - \pi^{-1}(\infty)$. On le notera $\mathbb{C}[X]$.*

Démonstration. La démonstration effectuée dans le théorème 3.1.3 prouve que $\mathbb{C}[X]$ est entier sur $\mathbb{C}[\mathbb{S}^2]$. Réciproquement si $f \in \mathcal{M}(X)$ est entier sur $\mathbb{C}[\mathbb{S}^2]$, alors on peut écrire l'équation de dépendance intégrale $f^n + a_{n-1}(b)f^{n-1} + \dots + a_0(b) = 0$ où les a_i sont holomorphes sur \mathbb{C} . Supposons que f admette un pôle d'ordre $\alpha > 0$ en $x \in X - \pi^{-1}(\infty)$, f^n admet alors en ce point un pôle d'ordre $n\alpha$ mais $a_{n-1}(b)f^{n-1} + \dots + a_0(b)$ admet en ce point un pôle d'ordre inférieur à $(n-1)\alpha$, ce qui est absurde. □

Nous admettrons les résultats suivants :

Proposition 4.0.2 *Les idéaux premiers de $\mathbb{C}[X]$ sont exactement les idéaux de la forme $\mathfrak{p}_x = \{f \in \mathbb{C}[X] \mid f(x) = 0\}$ pour $x \in X - \pi^{-1}(\infty)$. En particulier les idéaux premiers de $\mathbb{C}[\mathbb{S}^2]$ sont exactement les idéaux de la forme \mathfrak{p}_b , $b \in \mathbb{C}$.*

Théorème 4.0.3 *Soit $x \in X - \pi^{-1}(\infty)$. Alors l'indice de ramification de $\mathcal{M}(X)$ en \mathfrak{p}_x est égal à l'indice de ramification de π en x . En particulier pour $b \in \mathbb{C}$, $\mathcal{M}(X)$ se ramifie en \mathfrak{p}_b si et seulement si π se ramifie en b .*

Le fait que \mathbb{C} est simplement connexe assure que tout revêtement de degré supérieur ou égal à 2 se ramifie en au moins un point. Or d'après le théorème 1.1.1 se donner un revêtement de \mathbb{C} c'est se donner un revêtement de \mathbb{S}^2 . On peut donc dire que tout revêtement non trivial se ramifie en au moins un point autre que l'infini. Grâce au dictionnaire précédent, on peut énoncer ce résultat sous une forme plus algébrique : toute extension finie de $\mathcal{M}(\mathbb{S}^2)$ se ramifie sur $\mathbb{C}[\mathbb{S}^2]$ en au moins un idéal premier.

Mais ne pourrait-on pas trouver d'autres corps pour lesquels ce résultat reste vrai ?

Troisième partie

\mathbb{Z} est simplement connexe

A partir de maintenant et jusqu'à la fin, on se place dans la situation suivante : K est un corps de nombres (c'est-à-dire une extension finie de \mathbb{Q}) de degré $n \geq 2$. On note \mathcal{O}_K l'anneau des entiers de K sur \mathbb{Z} . On a alors le diagramme suivant :

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & K \\ \uparrow & \circlearrowleft & \uparrow n \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

Comme \mathbb{Z} est un anneau principal, les résultats vus dans la première partie s'appliquent. En particulier, \mathcal{O}_K est un anneau de Dedekind et un \mathbb{Z} -module libre de dimension n et l'on sait donner un sens au fait que K se ramifie en un nombre premier $p \in \mathbb{Z}$. On va prouver pour \mathbb{Z} ce qu'on vient de prouver pour $\mathbb{C}[\mathbb{S}^2]$, à savoir que toute extension finie non triviale de $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$ se ramifie en au moins un idéal premier non nul. Par analogie avec le précédent résultat qui signifiait que $\mathbb{C} = \text{Spec}(\mathbb{C}[\mathbb{S}^2])$ était simplement connexe, on énoncera alors que $\text{Spec}(\mathbb{Z})$ est simplement connexe ou, pour employer une formule choc, que \mathbb{Z} est simplement connexe.

5 Préliminaires

5.1 Réseaux sur un espace euclidien

Dans toute la suite, E désignera un espace vectoriel euclidien. E est alors en bijection isométrique avec \mathbb{R}^n . On notera μ la mesure image de la mesure de Lebesgue sur \mathbb{R}^n par cette application (qui ne dépend pas du choix de la bijection).

Théorème 5.1.1 (Caractérisation des sous-groupes discrets de E) *Soit E un espace euclidien de dimension d . Soit H un sous-groupe discret de E (pour la topologie induite par la norme de E). Alors H est de la forme $\mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_m$ où (v_1, \dots, v_m) est une famille libre de E sur \mathbb{R} .*

Démonstration. Soit (e_1, \dots, e_m) une famille libre sur \mathbb{R} d'éléments de H avec m maximal pour cette propriété. On définit alors :

$$K = \left\{ \sum_{i=1}^m \alpha_i e_i, \quad 0 \leq \alpha_i \leq 1 \right\}$$

K est alors un compact de E et donc $K \cap H$ est un ensemble compact et discret. Il est donc fini. Notons c son cardinal. Soit $x \in H$, alors grâce à la maximalité de m , on peut écrire $x = \sum_{i=1}^m \lambda_i e_i$ où les $\lambda_i \in \mathbb{R}$.

Pour $j \in \mathbb{N}^*$, posons $x_j = \sum_{i=0}^n (j\lambda_i - [j\lambda_i]) e_i \in K \cap H$. Ainsi il existe k et $l \leq c+1$ tels que $x_k = x_l$

et donc pour tout i , $\lambda_i = \frac{[k\lambda_i] - [l\lambda_i]}{k-l}$ si bien que $\lambda_i \in \frac{1}{k-l}\mathbb{Z} \subset \frac{1}{(c+1)!\mathbb{Z}}$. On en déduit que $H \subset \frac{e_1}{(c+1)!\mathbb{Z}} \oplus \dots \oplus \frac{e_m}{(c+1)!\mathbb{Z}}$. Ainsi H est un \mathbb{Z} -module libre de dimension inférieur ou égale à m .

Or (e_1, \dots, e_m) est une famille libre d'éléments de H donc H est de dimension m .

Si (v_1, \dots, v_m) est une base de H sur \mathbb{Z} , alors l'espace qu'elle engendre sur \mathbb{R} contient e_1, \dots, e_m et donc est de dimension m . Ceci prouve que (v_1, \dots, v_m) est une famille libre sur \mathbb{R} . \square

Définition 5.1.1 *Un réseau de E est un sous-groupe discret de E de rang n .*

Définition 5.1.2 Soit H un réseau de E et $\mathfrak{B} = (v_1, \dots, v_n)$ une base de H (en tant que \mathbb{Z} -module). On appelle maille élémentaire relativement à la base \mathfrak{B} , l'ensemble suivant :

$$P_{\mathfrak{B}} = \left\{ \sum_{i=1}^n \alpha_i v_i, \quad 0 \leq \alpha_i < 1 \right\}$$

Théorème 5.1.2 (Caractérisation des réseaux) Soit H un sous-groupe discret de E , alors H est un réseau si et seulement s'il existe un sous-ensemble borné M de E tel que $M + H = E$.

Démonstration. Soit H un réseau de E , soit \mathfrak{B} une base de H , alors $M = P_{\mathfrak{B}}$ convient. Réciproquement, supposons qu'il existe M borné tel que $M + H = E$. Notons E_0 l'espace vectoriel engendré par H . Soit $x \in E$, alors pour tout $a \in \mathbb{N}$, on a une décomposition $ax = m_x + h_x$ où $m_x \in M$ et $h_x \in H$ et donc $x = \frac{1}{a}m_x + \frac{1}{a}h_x$. En faisant tendre a vers l'infini, on trouve $x \in E_0$. Finalement, on obtient $E = E_0$ et donc H est un réseau de E . \square

Proposition 5.1.3 $\mu(P_{\mathfrak{B}})$ ne dépend pas de la base \mathfrak{B} choisie.

Démonstration. Soient $\mathfrak{B} = (v_1, \dots, v_n)$ et $\mathfrak{B}' = (v'_1, \dots, v'_n)$ deux bases de H . Notons P la matrice de passage de \mathfrak{B} à \mathfrak{B}' . On a alors $P \in GL_n(\mathbb{Z})$ et donc $|\det P| = 1$. D'autre part le théorème du changement de variable donne $\mu(P_{\mathfrak{B}'}) = |\det P| \mu(P_{\mathfrak{B}})$ d'où le résultat. \square

Définition 5.1.3 Le volume de l'un quelconque des $P_{\mathfrak{B}}$ est appelé le volume du réseau H et est noté $v(H)$.

Proposition 5.1.4 Si (v_1, \dots, v_n) est une base sur \mathbb{Z} du réseau H , alors :

$$v(H) = |\det(\langle v_i, v_j \rangle)|^{1/2}$$

Démonstration. Soit (e_1, \dots, e_n) une base orthonormale de E , et A la matrice de passage de (e_i) à (v_i) . Alors

$$\langle v_i, v_j \rangle = \left(\sum_{k,l} a_{ik} a_{jl} \langle e_k, e_l \rangle \right) = \left(\sum_k a_{ik} a_{jk} \right) = A^t A$$

d'où

$$v(H) = |\det A| = |\det(\langle v_i, v_j \rangle)|^{1/2}$$

\square

Théorème 5.1.5 (Minkowski) Soit H un réseau. Soit S une partie mesurable de E telle que $\mu(S) > v(H)$. Alors il existe deux éléments distincts de S , x et y tels que $x - y \in H$.

Démonstration. Soit \mathfrak{B} une base de H . On peut alors écrire :

$$E = \bigsqcup_{h \in H} (h + P_{\mathfrak{B}}) \quad \text{et donc} \quad S = \bigsqcup_{h \in H} S \cap (h + P_{\mathfrak{B}})$$

On en déduit que :

$$\mu(S) = \sum_{h \in H} \mu(S \cap (h + P_{\mathfrak{B}})) = \sum_{h \in H} \mu((-h + S) \cap P_{\mathfrak{B}})$$

Supposons que l'on ait $(-h + S) \cap (-h' + S) = \emptyset$ dès que $h \neq h'$, on aurait alors :

$$\mu(S) = \sum_{h \in H} \mu((-h + S) \cap P_{\mathfrak{B}}) = \mu \left(\bigsqcup_{h \in H} (-h + S) \cap P_{\mathfrak{B}} \right) \leq \mu(P_{\mathfrak{B}}) = v(H)$$

ce qui est supposé faux. On en déduit qu'il existe h et h' distincts dans H tel que $(-h + S) \cap (-h' + S) \neq \emptyset$. Et donc il existe x et y dans S vérifiant $-h + x = -h' + y$. Ainsi $x - y = h - h' \in H - \{0\}$, ce qu'il fallait démontrer. \square

Corollaire 5.1.6 Soient H un réseau et S une partie de E mesurable, convexe, symétrique par rapport à 0 et telle que $\mu(S) > 2^n v(H)$. Alors $S \cap H^* \neq \emptyset$ (où $H^* = H - \{0\}$)

Démonstration. On pose $S' = \frac{1}{2}S$, alors $\mu(S') = \frac{1}{2^n}\mu(S) > v(H)$. On en déduit, par le théorème précédent qu'il existe x et y appartenant à S' tels que $x - y \in H^*$. Mais on a $x - y = \frac{1}{2}((2x) + (-2y)) \in S$, d'où le résultat. \square

Corollaire 5.1.7 Soient H un réseau et S une partie de E mesurable, convexe, compacte, symétrique par rapport à 0 et telle que $\mu(S) \geq 2^n v(H)$. Alors $S \cap H^* \neq \emptyset$.

Démonstration. Notons, pour $\varepsilon > 0$, $S_\varepsilon = (1 + \varepsilon)S$. On a alors $\mu(S_\varepsilon) > 2^n v(H)$ et donc, d'après le corollaire précédent, $H^* \cap S_\varepsilon \neq \emptyset$. D'autre part, comme S_ε est compact, $H^* \cap S_\varepsilon$ est compact. Comme S est convexe et symétrique par rapport à 0 , on a pour $\varepsilon' < \varepsilon$, $S \subset S_{\varepsilon'} \subset S_\varepsilon$. Comme une intersection décroissante de compacts non vides est non vide, on obtient :

$$\bigcap_{\varepsilon > 0} H^* \cap S_\varepsilon = H^* \cap \left(\bigcap_{\varepsilon > 0} S_\varepsilon \right) \neq \emptyset$$

Finalement, on a $\bigcap_{\varepsilon > 0} S_\varepsilon \supset S$, d'après la remarque précédente. Réciproquement si $x \in S_\varepsilon$ pour tout $\varepsilon > 0$, on peut construire une suite (s_n) d'éléments de S telle que $x = (1 + \frac{1}{n})s_n$ pour tout n . Par compacité, (s_n) admet une valeur d'adhérence $s \in S$. Par passage à la limite, on trouve que $x = s$ et donc $x \in S$. \square

5.2 Discriminant

Définition 5.2.1 Soient B un anneau et A un sous-anneau de B tel que B soit un A -module libre de dimension n . Soit $\mathfrak{B} = (x_1, \dots, x_n)$ une base de B sur A . On appelle discriminant relativement à la base \mathfrak{B} la quantité $D(\mathfrak{B}) = \det(Tr_{B/A}(x_i x_j))$.

Proposition 5.2.1 Si \mathfrak{B} et \mathfrak{B}' sont deux bases de B sur A , alors $D(\mathfrak{B})$ et $D(\mathfrak{B}')$ diffèrent multiplicativement d'un carré d'une unité.

Démonstration. On vérifie que si P désigne la matrice de passage de \mathfrak{B} à \mathfrak{B}' , on a :

$$(Tr_{B/A}(x_i x_j)) = {}^t P (Tr_{B/A}(x'_i x'_j)) P$$

et donc $D(\mathfrak{B}) = \det(P)^2 D(\mathfrak{B}')$. Comme la matrice P est inversible, son déterminant l'est également. \square

Corollaire 5.2.2 L'idéal engendré par $D(\mathfrak{B})$ ne dépend pas de la base \mathfrak{B} choisie.

Définition 5.2.2 Cet idéal s'appelle le discriminant de B sur A et est noté $\mathfrak{D}_{B/A}$.

Lemme 5.2.3 (Stabilité par passage au quotient) Soient B un anneau et A un sous-anneau de B tel que B soit un A -module libre de dimension n . Soit \mathfrak{a} un idéal de A de sorte que l'on a le diagramme commutatif suivant :

$$\begin{array}{ccc} A & \twoheadrightarrow & A/\mathfrak{a} \\ \downarrow & \circlearrowleft & \downarrow \\ B & \twoheadrightarrow & B/\mathfrak{a}B \\ x \mapsto & & \bar{x} \end{array}$$

Si (x_1, \dots, x_n) est une base de B , alors $(\bar{x}_1, \dots, \bar{x}_n)$ est une base de $B/\mathfrak{a}B$ et $D(\bar{x}_1, \dots, \bar{x}_n) = \overline{D(x_1, \dots, x_n)}$.

Démonstration. Il suffit de vérifier $Tr(\bar{x}) = \overline{Tr(x)}$. \square

Proposition 5.2.4 Soit K une extension séparable de degré n de k . On note τ_1, \dots, τ_n les morphismes de k -algèbres de K dans \bar{k} . On considère (x_1, \dots, x_n) une base de K sur k . Alors $D(x_1, \dots, x_n) = \det(\tau_i(x_j))^2 \neq 0$.

Démonstration. On calcule :

$$D(x_1, \dots, x_n) = |Tr(x_i x_j)| = \left| \sum_{k=1}^n \tau_k(x_i x_j) \right| = \left| \sum_{k=1}^n \tau_k(x_i) \tau_k(x_j) \right| = \det(\tau_i(x_j))^2$$

La non nullité est une conséquence immédiate du lemme de Dedekind qui dit que les τ_k forme une famille libre sur \mathbb{C} . \square

Le cas qui nous intéresse et que l'on va développer dans la fin de ce paragraphe est celui où $A = \mathbb{Z}$.

Proposition 5.2.5 Soit \mathfrak{a} un idéal fractionnaire non nul de \mathcal{O}_K , c'est un \mathbb{Z} -module libre de dimension n .

Démonstration. Il existe $d \in \mathcal{O}_K$ tel que $\mathfrak{a} \subset d^{-1}\mathcal{O}_K$. \mathcal{O}_K et donc $d^{-1}\mathcal{O}_K$ est un \mathbb{Z} -module libre de dimension n , ce qui prouve que \mathfrak{a} est un \mathbb{Z} -module libre de dimension inférieure ou égale à n .

D'autre part soit (e_1, \dots, e_n) une base de \mathcal{O}_K sur \mathbb{Z} et soit x un élément non nul de \mathfrak{a} . Alors (xe_1, \dots, xe_n) est une famille libre sur \mathbb{Z} d'éléments de \mathfrak{a} . On en déduit le résultat annoncé. \square

Soit \mathfrak{B} une base de \mathfrak{a} sur \mathbb{Z} . Le calcul effectué dans la démonstration de la proposition 5.2.1 prouve que $D(\mathfrak{B})$ ne dépend pas de la base \mathfrak{B} choisie. On peut donc poser la définition suivante :

Définition 5.2.3 Soit \mathfrak{a} un idéal fractionnaire non nul de \mathcal{O}_K . On appelle discriminant de \mathfrak{a} et on note $D(\mathfrak{a})$ le discriminant d'une base quelconque de \mathfrak{a} sur \mathbb{Z} .

Définition 5.2.4 On appelle discriminant absolu du corps de nombre K le discriminant de \mathcal{O}_K , noté d_K .

Proposition 5.2.6 Soient $\mathfrak{a} \subset \mathfrak{a}'$ deux idéaux fractionnaires non nuls de K , alors l'indice $(\mathfrak{a}' : \mathfrak{a})$ est fini et vérifie

$$D(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 D(\mathfrak{a}')$$

Démonstration. \mathfrak{a} est un sous- \mathbb{Z} -module de \mathfrak{a}' libre de même dimension n . On sait donc qu'il existe une base (e_i) de \mathfrak{a}' et des entiers (a_i) tels que la famille $(a_i e_i)$ soit une base de \mathfrak{a} . Avec ces bases, on a clairement

$$\mathfrak{a}'/\mathfrak{a} = \prod_{i=1}^n \mathbb{Z}/a_i \mathbb{Z}$$

et, si A est la matrice de changement de base,

$$\det A = \prod_{i=1}^n a_i$$

d'où la proposition. \square

5.3 Norme d'un idéal

On allons étendre la notion de norme à un idéal de \mathcal{O}_K . Pour cela, on va avoir besoin de la proposition suivante :

Proposition 5.3.1 Si $x \in \mathcal{O}_K$ et $x \neq 0$, alors $|N(x)| = (\mathcal{O}_K : \mathcal{O}_K x)$.

Démonstration. \mathcal{O}_K et $\mathcal{O}_K x$ sont des \mathbb{Z} -modules libres de dimension n . On peut donc trouver une base (e_1, \dots, e_n) de \mathcal{O}_K et des entiers c_1, \dots, c_n tels que $(c_1 e_1, \dots, c_n e_n)$ soit une base de $\mathcal{O}_K x$. On a alors $(\mathcal{O}_K : \mathcal{O}_K x) = |c_1 \dots c_n|$.

D'autre part $(x e_1, \dots, x e_n)$ est également une base de $\mathcal{O}_K x$ donc le déterminant de l'application qui à $x e_i$ associe $c_i e_i$ est inversible dans \mathbb{Z} donc il vaut 1 en valeur absolue. Ceci prouve que $N(x) = |c_1 \dots c_n|$. \square

Ceci nous incite à poser la définition suivante :

Définition 5.3.1 Soit \mathfrak{a} un idéal non nul de \mathcal{O}_K . On définit la norme de \mathfrak{a} par $N(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$.

Proposition 5.3.2 Si \mathfrak{a} est un idéal non nul de \mathcal{O}_K , on a $N(\mathfrak{a}) < \infty$

Démonstration. C'est un corollaire immédiat de la proposition 5.2.6. \square

Proposition 5.3.3 Si \mathfrak{a} et \mathfrak{b} sont deux idéaux non nuls de \mathcal{O}_K alors $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) N(\mathfrak{b})$.

Démonstration. Grâce à la décomposition en idéaux maximaux dans un anneau de Dedekind, on peut supposer que \mathfrak{b} est un idéal maximal. Comme on l'a vu dans la démonstration du théorème 2.2.5, $\mathfrak{a}/\mathfrak{a}\mathfrak{b}$ est un espace vectoriel de dimension 1 sur $\mathcal{O}_K/\mathfrak{b}$ et donc $\text{Card}(\mathfrak{a}/\mathfrak{a}\mathfrak{b}) = \text{Card}(\mathcal{O}_K/\mathfrak{b})$. L'égalité $\text{Card}(\mathcal{O}_K/\mathfrak{a}\mathfrak{b}) = \text{Card}(\mathcal{O}_K/\mathfrak{a}) \text{Card}(\mathfrak{a}/\mathfrak{a}\mathfrak{b})$ permet finalement de conclure. \square

6 Démonstration

6.1 Discriminant et ramification

Nous allons montrer dans cette partie que K se ramifie en p si et seulement si p divise le discriminant absolu de K .

Lemme 6.1.1 Soit \mathcal{O} un anneau de Dedekind et \mathfrak{a} un idéal entier non nul de \mathcal{O} . On a vu qu'alors on peut écrire $\mathfrak{a} = \prod_{i=1}^q \mathfrak{m}_i^{\alpha_i}$ où les \mathfrak{m}_i sont des idéaux premiers de \mathcal{O} et les α_i des entiers strictement positifs.

Dans ces conditions on a l'isomorphisme suivant :

$$\mathcal{O}/\mathfrak{a} \xrightarrow{\sim} \prod_{i=1}^q \mathcal{O}/\mathfrak{m}_i^{\alpha_i}$$

Démonstration. D'après le théorème des restes chinois, il suffit de prouver que les $\mathfrak{m}_i^{\alpha_i}$ sont deux à deux étrangers. Or ceci se déduit du formulaire 2.1.6 sur les anneaux de Dedekind. \square

Dans notre situation, on obtient $\mathcal{O}_K/p\mathcal{O}_K \xrightarrow{\sim} \prod_{i=1}^q \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ (\star)

Lemme 6.1.2 Soit k un corps parfait et K une k -algèbre finie. Alors K est réduite (ie 0 est le seul élément nilpotent) si et seulement si $\mathfrak{D}_{K/k} \neq 0$.

Démonstration. Supposons tout d'abord que K ne soit pas réduite. Considérons donc $x_1 \in K$ un élément nilpotent non nul. On peut alors former (x_1, x_2, \dots, x_n) une base de K sur k . Mais alors pour tout j entre 1 et n , $x_1 x_j$ est un élément nilpotent et donc l'endomorphisme de multiplication par $x_1 x_j$ l'est aussi. On en déduit que $\text{Tr}(x_1 x_j) = 0$ puis que $\mathfrak{D}_{K/k} = 0$.

Réciproquement supposons que K soit réduite. K est en particulier un anneau noethérien donc, d'après le lemme 2.1.2 il existe des idéaux premiers \mathfrak{q}_i et des entiers strictement positifs α_i tels que $\mathfrak{q}_1^{\alpha_1} \dots \mathfrak{q}_l^{\alpha_l} = 0$. Soit $x \in \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_l$, alors $x^{\alpha_1 + \dots + \alpha_l} = 0$ puis $x = 0$. On en déduit que $\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_l = 0$.

D'autre part, K/\mathfrak{q}_i est une k -algèbre intègre de dimension finie, c'est donc un corps. Ainsi \mathfrak{q}_i est un idéal maximal de K . En appliquant le théorème des restes chinois, on obtient $K \sim \prod_{i=1}^l K/\mathfrak{q}_i$.

Considérons alors $\mathfrak{B} = (\mathfrak{B}_1, \dots, \mathfrak{B}_l)$ une base de K sur k adaptée à cette décomposition. En remarquant que si $x \in K/\mathfrak{q}_i$ et $y \in K/\mathfrak{q}_j$ (où $i \neq j$), alors $xy = 0$, on obtient $D(\mathfrak{B}) = D(\mathfrak{B}_1) \dots D(\mathfrak{B}_l)$, d'où il vient

$\mathfrak{D}_{K/k} = \prod_{i=1}^l \mathfrak{D}_{(K/\mathfrak{q}_i)k}$. Or K/\mathfrak{q}_i est un corps et même une extension séparable de k (car k est parfait) et donc la trace n'y est pas dégénérée, ce qui veut dire que $\mathfrak{D}_{(K/\mathfrak{q}_i)k} \neq 0$ ou encore $\mathfrak{D}_{(K/\mathfrak{q}_i)k} = k$, et puis $\mathfrak{D}_{K/k} = k \neq 0$. \square

Théorème 6.1.3 *K se ramifie en p si et seulement si p divise le discriminant absolu de K .*

Démonstration. D'après (\star) , K se ramifie en p si et seulement si $\mathcal{O}_K/p\mathcal{O}_K$ n'est pas réduit. Le lemme précédent prouve que ceci équivaut à $\mathfrak{D}_{(\mathcal{O}_K/p\mathcal{O}_K)(\mathbb{Z}/p\mathbb{Z})} = 0$, c'est-à-dire, grâce à la stabilité par passage au quotient, $\mathfrak{D}_{\mathcal{O}_K/\mathbb{Z}} \subset p\mathbb{Z}$, ce qui veut bien dire que p divise le discriminant absolu de K . \square

Corollaire 6.1.4 *Pour prouver que K se ramifie en au moins un idéal premier, il suffit de montrer que son discriminant absolu n'est jamais 1, ni (-1) .*

6.2 L'espace de Minkowski

Pour obtenir ce résultat, on va plonger K dans un espace vectoriel euclidien et utiliser les propriétés des réseaux énoncées précédemment.

K est une extension séparable de \mathbb{Q} donc il existe exactement n homomorphismes de corps de K dans \mathbb{C} . On pose $K_{\mathbb{C}} = \mathbb{C}^{\text{hom}(K, \mathbb{C})}$ et on munit $K_{\mathbb{C}}$ du produit scalaire canonique.

On a l'application naturelle $j : \begin{pmatrix} K & \longrightarrow & K_{\mathbb{C}} \\ x & \longmapsto & (\tau x)_{\tau} \end{pmatrix}$.

Le groupe de Galois $\text{gal}(\mathbb{C}|\mathbb{R}) = \{1, F\}$ agit sur $K_{\mathbb{C}}$ de la façon suivante : si $z = (z_{\tau})$, $(Fz)_{\tau} = \overline{z_{\bar{\tau}}}$. L'action de F est une isométrie de $K_{\mathbb{C}}$.

On appelle $K_{\mathbb{R}}$ le sous-espace stable par F ; le produit scalaire (hermitien) sur $K_{\mathbb{C}}$ induit sur $K_{\mathbb{R}}$ un produit scalaire réel qui en fait un espace vectoriel euclidien. Comme $F \circ j = j$, on a par restriction $j : K \longrightarrow K_{\mathbb{R}}$. Nous allons maintenant étudier l'espace de Minkowski $K_{\mathbb{R}}$.

Soit $\tau \in \text{hom}(K, \mathbb{C})$. On dit que τ est réel si $\bar{\tau} = \tau$, complexe dans le cas contraire ; $\text{hom}(K, \mathbb{C})$ contient r morphismes réels $\rho_1, \dots, \rho_r : K \longrightarrow \mathbb{R}$ et s paires de morphismes complexes conjugués $\sigma_1, \bar{\sigma}_1, \dots, \sigma_s, \bar{\sigma}_s : K \longrightarrow \mathbb{C}$, d'où $n = r + 2s$. Dans la suite, ρ décrira l'ensemble des ρ_i et σ l'ensemble des σ_j . Alors :

$$K_{\mathbb{R}} = \{(z_{\tau}) \in K_{\mathbb{C}} \mid z_{\rho} \in \mathbb{R}, z_{\sigma} = \overline{z_{\bar{\sigma}}}\}$$

Proposition 6.2.1 *On a un isomorphisme $f : \begin{pmatrix} K_{\mathbb{R}} & \longrightarrow & \mathbb{R}^{\text{hom}(K, \mathbb{C})} = \mathbb{R}^{r+2s} \\ (z_{\tau}) & \longmapsto & (x_{\tau}) \end{pmatrix}$ défini par $x_{\rho} = z_{\rho}$,*

$x_{\sigma} = \text{Re}(z_{\sigma})$, $x_{\bar{\sigma}} = \text{Im}(z_{\sigma})$.

Si on munit $\mathbb{R}^{\text{hom}(K, \mathbb{C})}$ du produit scalaire $(x, y) \longmapsto \sum_{\tau} \alpha_{\tau} x_{\tau} y_{\tau}$, où $\alpha_{\tau} = 1$ si τ est réel, $\alpha_{\tau} = 2$ si τ est complexe, alors f est de plus une isométrie.

L'application $j : K \longrightarrow K_{\mathbb{R}}$ nous fournit les réseaux suivants dans $K_{\mathbb{R}}$:

Proposition 6.2.2 *Soit \mathfrak{a} un idéal non nul de \mathcal{O}_K , alors $\Gamma = j\mathfrak{a}$ est un réseau de $K_{\mathbb{R}}$, de volume*

$$\text{vol}(\Gamma) = \sqrt{|d_K|}N(\mathfrak{a})$$

Démonstration. \mathfrak{a} est libre de rang n sur \mathbb{Z} ; soit donc $(\alpha_1, \dots, \alpha_n)$ une base de \mathfrak{a} . Alors $\Gamma = \mathbb{Z}j\alpha_1 + \dots + \mathbb{Z}j\alpha_n$. En posant $\text{hom}(K, \mathbb{C}) = \{\tau_1, \dots, \tau_n\}$, et $A = (\tau_l\alpha_i)$, on a :

$$(\langle j\alpha_i, j\alpha_k \rangle) = \left(\sum_{l=1}^n \tau_l\alpha_i\bar{\tau}_l\alpha_k \right) = A^t A$$

et

$$(\det A)^2 = D(\mathfrak{a}) = N(\mathfrak{a})^2 d_K$$

d'où

$$v(\Gamma) = |\det(\langle j\alpha_i, j\alpha_k \rangle)|^{1/2} = |\det A| = \sqrt{|d_K|}N(\mathfrak{a})$$

□

Théorème 6.2.3 *Le discriminant d'un corps de nombres K de degré n vérifie $|d_K|^{1/2} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}$.*

Démonstration. Le théorème de Minkowski sur les réseaux s'applique de la façon suivante : soit X une partie mesurable, convexe, compacte, symétrique par rapport à l'origine de $K_{\mathbb{R}}$, et telle que $\mu(X) \geq 2^n v(\Gamma)$, où $\Gamma = j\mathcal{O}_K$, alors il existe $a \in \mathcal{O}_K$ tel que $a \neq 0$ et $ja \in X$.

Pour $t > 0$, posons

$$X_t = \left\{ (z_\tau) \in K_{\mathbb{R}} \mid \sum_{\tau} |z_\tau| \leq t \right\}$$

X_t est clairement mesurable, convexe, compacte et symétrique par rapport à l'origine, et on montre (voir lemme suivant) que $\mu(X_t) = 2^r \pi^s \frac{t^n}{n!}$. Pour appliquer le résultat, on choisit donc $\mu(X_t) = 2^n v(\Gamma)$, ce qui correspond à $t^n = n! \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$. On dispose donc du a désiré.

L'inégalité entre les moyennes arithmétique et géométrique nous donne :

$$\left(\prod_{\tau} |\tau a| \right)^{1/n} \leq \frac{1}{n} \sum_{\tau} |\tau a|$$

d'où

$$|N_{K/\mathbb{Q}}(a)| = \prod_{\tau} |\tau a| \leq \frac{1}{n^n} \left(\sum_{\tau} |\tau a| \right)^n \leq \frac{t^n}{n^n}$$

Comme $n = r + 2s$, on a $s \leq n/2$ et $\frac{t^n}{n^n} \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{n/2} \sqrt{|d_K|}$. Enfin, $a \in \mathcal{O}_K$ donc $N_{K/\mathbb{Q}}(a) \in \mathbb{Z}$ et en particulier $|N_{K/\mathbb{Q}}(a)| \geq 1$. On en déduit le résultat demandé. □

Lemme 6.2.4 *Dans l'espace de Minkowski $K_{\mathbb{R}}$, la partie mesurable*

$$X_t = \left\{ (z_\tau) \in K_{\mathbb{R}} \mid \sum_{\tau} |z_\tau| \leq t \right\}$$

a pour volume $\mu(X_t) = 2^r \pi^s \frac{t^n}{n!}$.

Démonstration. Si λ est la mesure de Lebesgue sur $\mathbb{R}^{\text{hom}(K, \mathbb{C})}$, et $f : K_{\mathbb{R}} \rightarrow \mathbb{R}^{\text{hom}(K, \mathbb{C})}$ l'application précédemment définie, alors $\mu(X_t) = 2^s \lambda(f(X_t))$. On a :

$$f(X_t) = \left\{ (x_\rho, x_\sigma, x_{\bar{\sigma}}) \mid \sum_\rho |x_\rho| + 2 \sum_\sigma \sqrt{x_\sigma^2 + x_{\bar{\sigma}}^2} \leq t \right\}$$

Le facteur 2 est dû au fait que $|z_{\bar{\sigma}}| = |z_\sigma|$.
On passe en coordonnées polaires

$$(u_\sigma, \theta_\sigma) \mapsto \left(x_\sigma = \frac{u_\sigma}{2} \cos \theta_\sigma, x_{\bar{\sigma}} = \frac{u_\sigma}{2} \sin \theta_\sigma \right)$$

et on utilise la symétrie de X_t pour se restreindre au domaine où $x_\rho \geq 0$, ce qui divise le volume par 2^r . Ce travail nous permet d'obtenir l'expression

$$\lambda(f(X_t)) = \int_{Y_{r,s}(t) \times [0, 2\pi]^s} 2^r 4^{-s} u_1 \dots u_s dx_1 \dots dx_r du_1 \dots du_s d\theta_1 \dots d\theta_s$$

où $Y_{r,s}(t) = \left\{ (x_1, \dots, x_r, u_1, \dots, u_s) \in \mathbb{R}^{r+s} \mid x_1 + \dots + x_r + u_1 + \dots + u_s \leq t \right\}$,
d'où finalement $\mu(X_t) = 2^r \pi^s I_{r,s}(t)$ avec

$$I_{r,s}(t) = \int_{Y_{r,s}(t)} u_1 \dots u_s dx_1 \dots dx_r du_1 \dots du_s$$

On a clairement $I_{r,s}(t) = t^{r+2s} I_{r,s}(1)$. Si, en appliquant le théorème de Fubini, on intègre d'abord par rapport aux variables $x_1, \dots, x_{r-1}, u_1, \dots, u_s$, puis par rapport à x_r , on obtient :

$$I_{r,s}(1) = \int_0^1 I_{r-1,s}(1-x_r) dx_r = \int_0^1 (1-x_r)^{n-1} dx_r \cdot I_{r-1,s}(1) = \frac{1}{n} I_{r-1,s}(1)$$

d'où, par récurrence, $I_{r,s}(1) = \frac{(n-r)!}{n!} I_{0,s}(1)$. De la même manière, on obtient

$$I_{0,s}(1) = \int_0^1 u_s (1-u_s)^{2s-2} du_s \cdot I_{0,s-1}(1)$$

et $I_{0,s}(1) = \frac{1}{(2s)!} I_{0,0}(1) = \frac{1}{(2s)!} = \frac{1}{(n-r)!}$. Finalement, $I_{r,s}(1) = \frac{1}{n!}$, d'où le résultat annoncé. \square

Corollaire 6.2.5 (Théorème de Minkowski) *Tout corps de nombres différent de \mathbb{Q} se ramifie en au moins un idéal premier.*

Démonstration. On a vu dans le paragraphe précédent qu'il suffisait de prouver que $|d_K| > 1$. Posons alors $u_n = \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}$. On a alors $u_2 = \frac{\pi}{2} > 1$ et $\frac{u_{n+1}}{u_n} = \sqrt{\frac{\pi}{4}} \left(1 + \frac{1}{n}\right)^n > 1$, ce qui prouve le théorème. \square

On a montré que \mathbb{Z} est simplement connexe !

7 Compléments

7.1 Un résultat de finitude

Théorème 7.1.1 *Il n'y a qu'un nombre fini de corps de nombres de discriminant donné.*

Démonstration. La formule de Stirling permet de montrer que le discriminant d'un corps de nombre tend vers l'infini avec le degré du corps de nombres. Ainsi, on peut supposer que le degré n ainsi donc que les nombres r et s définis précédemment sont donnés.

Soit K un corps de nombres. Montrons qu'il existe un élément primitif de K n pas trop grand.

Si $r = 0$, alors les résultats sur les réseaux prouvent qu'il existe une constante C_0 et un élément $x \in \mathcal{O}_K$ vérifiant $\text{Im}(\sigma_1(x)) \leq C_0$, $\text{Re}(\sigma_1(x)) \leq \frac{1}{2}$ et pour tout i supérieur ou égal à 2, $|\sigma_i(x)| \leq \frac{1}{2}$. Comme $x \in \mathcal{O}_K$, on a $|N(x)| \geq 1$ et donc $|\sigma_1(x)| \geq 1$. On en déduit que pour i supérieur ou égal à 2, $\sigma_1(x) \neq \sigma_i(x)$ et $\sigma_1(x) \neq \bar{\sigma}_i(x)$. D'autre part on a $\sigma_1(x) \neq \bar{\sigma}_1(x)$. Ceci prouve que x est un élément primitif.

Si $r > 0$, alors comme précédemment il existe une constante C_1 et $x \in \mathcal{O}_K$ tel que $|\rho_1(x)| \leq C_1$ et pour tout $\tau \in \text{hom}(K, \mathbb{C})$ différent de ρ_1 , $|\tau(x)| \leq \frac{1}{2}$. On en déduit, grâce à la norme, que $|\rho_1(x)| \geq 1$ et donc que x est un élément primitif.

Les majorations ci-dessus prouvent que les fonctions symétriques élémentaires des τx appartiennent à un ensemble borné et donc ne peuvent prendre qu'un nombre fini de valeurs. On en déduit qu'il n'y a qu'un nombre fini de possibilités pour le polynôme caractéristique de x et donc également pour x . Comme $K = \mathbb{Q}[x]$, on obtient le théorème annoncé. \square

7.2 Le théorème des unités

Soit K un corps de nombres, les entiers r et s sont définis comme précédemment. On notera \mathcal{O}_K^* le groupe des unités de l'anneau \mathcal{O}_K et μ_K l'ensemble des racines de l'unité contenues dans K .

Le but de ce paragraphe est de démontrer le théorème suivant :

Théorème 7.2.1 *Avec les notations précédentes, \mathcal{O}_K^* est isomorphe au produit direct de μ_K par \mathbb{Z}^{r+s-1} .*

Proposition 7.2.2 *Les éléments de \mathcal{O}_K^* sont exactement les éléments de \mathcal{O}_K de norme 1 ou (-1) .*

Démonstration. Si x est inversible dans \mathcal{O}_K alors on a $N(x)N(x^{-1}) = N(1) = 1$ et $N(x) \in \mathbb{Z}$ d'où la première implication.

Réciproquement si $N(x) \in \{1, -1\}$, on peut écrire l'équation de dépendance intégrale $x^n + a_{n-1}x^{n-1} + \dots + N(x) = 0$, ce qui prouve bien que x est inversible dans \mathcal{O}_K . \square

Définition 7.2.1 (Plongement logarithmique) *Avec les notations précédentes, on appelle plongement logarithmique le morphisme suivant :*

$$L : \begin{pmatrix} K^* & \rightarrow & \mathbb{R}^{r+s} \\ x & \mapsto & (\ln |\rho_1(x)|, \dots, \ln |\rho_r(x)|, \ln |\sigma_1(x)|, \dots, \ln |\sigma_s(x)|) \end{pmatrix}$$

On notera λ la restriction de ce morphisme à \mathcal{O}_K^* et Γ l'image de λ .

Proposition 7.2.3 *Le noyau de λ est exactement μ_K .*

Démonstration. Si $x \in \ker \lambda$, alors les coefficients de son polynôme caractéristique (qui s'expriment comme les fonctions symétriques élémentaires de $\tau(x)$, $\tau \in \text{hom}(K, \mathbb{C})$) sont bornées. Ceci prouve que $\ker \lambda$ est un sous-groupe fini de K^* , il est donc formé de racines de l'unité.

D'autre part, si $x \in \mu_K$, alors il est clair que $|\tau(x)| = 1$ pour tout $\tau \in \text{hom}(K, \mathbb{C})$ et donc $x \in \ker \lambda$. \square

Remarque 7.2.1 *La proposition dit exactement que la suite suivante est exacte :*

$$1 \longrightarrow \mu_K \longrightarrow \mathcal{O}_K^* \longrightarrow \Gamma \longrightarrow 1$$

Proposition 7.2.4 *Γ est un sous-groupe discret de \mathbb{R}^{r+s} .*

Démonstration. Il suffit de montrer que tout compact de \mathbb{R}^{r+s} intersecte Γ sur un ensemble fini. Soit donc C un compact de \mathbb{R}^{r+s} et soit $x \in \Gamma \cap C$. Alors il existe $x_0 \in \mathcal{O}_K$ et R tel que pour tout $\tau \in \text{hom}(K, \mathbb{C})$, $|\ln |\tau(x)|| \leq R$ et puis $e^{-R} \leq |\tau(x)| \leq e^R$. Comme précédemment, on en déduit que les coefficients du polynôme caractéristique de x sont bornés et puis que $\Gamma \cap C$ est fini. \square

Les résultats sur les sous-groupes discrets prouvent en particulier que Γ est un \mathbb{Z} -module libre de dimension inférieure ou égale à $r + s$. Ceci prouve que la suite exacte écrite au-dessus est scindée et donc que \mathcal{O}_K^* s'exprime comme produit direct de Γ par μ_K .

Il ne reste donc plus qu'à montrer que Γ est de dimension $r + s - 1$.

Il est facile de voir tout d'abord que la dimension de Γ est inférieure ou égale à $r + s - 1$.

Démonstration. Soit $x \in \mathcal{O}_K^*$, on a vu qu'alors $N(x) = 1$, et donc

$$\prod_{\tau \in \text{hom}(K, \mathbb{C})} |\tau(x)| = \left(\prod_{i=1}^r |\rho_i(x)| \right) \left(\prod_{j=1}^s |\sigma_j(x)|^2 \right) = 1.$$

Ceci prouve que Γ est inclus dans l'hyperplan d'équation $x_1 + \dots + x_r + 2(y_1 + \dots + y_s) = 0$. \square

Notons H l'hyperplan d'équation $x_1 + \dots + x_r + 2(y_1 + \dots + y_s) = 0$.

Lemme 7.2.5 *Il existe deux constantes C et α telles que pour tout w dans H , il existe un élément a de \mathcal{O}_K tel que $N(a) \leq \alpha$ et $\|w - L(a)\| \leq C$.*

Démonstration. Notons H_α l'hyperplan affine d'équation $x_1 + \dots + x_r + 2(y_1 + \dots + y_s) = \alpha$. Soit $v = (x_1, \dots, x_r, y_1, \dots, y_s) \in H_\alpha$. Considérons l'ensemble suivant :

$$X = \{(z_\tau) \in K_{\mathbb{R}} \mid |\rho_i| \leq e^{x_i}, |\sigma_j| \leq e^{y_j}\}$$

X est alors un ensemble compact, convexe et symétrique par rapport à 0. Le volume de X vaut $\pi^s e^{x_1} \dots e^{x_s} e^{2y_1} \dots e^{2y_s}$ soit $\pi^s e^\alpha$. Donc si on choisit α suffisamment grand, il va exister $a \in \mathcal{O}_K$ tel que $ja \in X$. Autrement dit, on aura $|\rho_i(a)| \leq e^{x_i}$ et $|\sigma_j(a)| \leq e^{y_j}$. On a alors $|N(a)| \leq e^\alpha$. D'autre part $a \in \mathcal{O}_K$ donc $|N(a)| \geq 1$ et puis :

$$|\rho_i(a)| = |N(a)| \left(\prod_{k \neq i} |\rho_k(a)| \right) \left(\prod_{l=1}^s |\sigma_l(a)|^2 \right) \geq \frac{e^{x_i}}{e^\alpha}$$

$$|\sigma_j(a)|^2 = |N(a)| \left(\prod_{k=1}^r |\rho_k(a)| \right) \left(\prod_{l \neq j} |\sigma_l(a)|^2 \right) \geq \frac{e^{2y_j}}{e^\alpha}$$

On en déduit que $-\alpha \leq \ln |\rho_i(a)| - x_i \leq 0$ et $-\frac{\alpha}{2} \leq \ln |\sigma_j(a)| - y_j \leq 0$. Ainsi $\|v - L(a)\| \leq \alpha \sqrt{r+s}$.

Remarquons finalement que le α peut être choisi indépendamment de v . \square

Lemme 7.2.6 *Modulo les éléments de \mathcal{O}_K^* , il n'y a qu'un nombre fini d'éléments de \mathcal{O}_K de norme donnée a priori.*

Démonstration. Notons q la valeur de la norme donnée a priori. Soit $x \in \mathcal{O}_K$, on a alors $\text{Card}(\mathcal{O}_K/\mathcal{O}_K x) = |N(x)| = |q|$. On en déduit que $q \in \mathcal{O}_K x$ (car l'ordre dans $\mathcal{O}_K/\mathcal{O}_K x$, $1 * q = 0$) et donc $\mathcal{O}_K q \subset \mathcal{O}_K x$, d'où $\mathcal{O}_K/\mathcal{O}_K x \subset \mathcal{O}_K/\mathcal{O}_K q$. Or $\mathcal{O}_K/\mathcal{O}_K q$ est fini donc l'ensemble de $\mathcal{O}_K x$ qui conviennent également. On en déduit le lemme annoncé. \square

On en déduit le résultat voulu de la façon suivante :

Démonstration. D'après le lemme précédent, il existe a_1, \dots, a_N des éléments de \mathcal{O}_K tels que si $|N(a)| \leq e^\alpha$, alors $a = ua_k$ où $u \in \mathcal{O}_K^*$. Notons B la boule de E de centre l'origine et de rayon C et posons :

$$M = \bigcup_{k=1}^N (B + L(a_k))$$

M est alors une partie bornée de E et si $w \in H$, alors il existe a de norme inférieure à α tel que $(w - L(a)) \in B$. D'autre part il existe $u \in \mathcal{O}_K^*$ tel que $a = ua_k$. On a alors $(w - L(a_k) - \lambda(u)) \in B$ et donc $(w - \lambda(u)) \in M$. On en déduit par la caractérisation des réseaux que Γ est de dimension $r + s - 1$. \square

8 L'exemple de $\mathbb{Q}[\sqrt{d}]$

Considérons d un entier positif non multiple d'un carré parfait. Prenons $K = \mathbb{Q}[\sqrt{d}]$.

Lemme 8.0.7 *Soit $x \in \mathbb{Q}$. On suppose que $x\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. Alors $x \in \mathbb{Z}$.*

Démonstration. Supposons que $x\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$, on a alors l'équation de dépendance intégrale $(x\sqrt{d})^n + a_{n-1}(x\sqrt{d})^{n-1} + \dots + a_0 = 0$. Si n est pair, on obtient puisque d n'est pas un carré parfait, l'équation $(x^2d)^{\frac{n}{2}} + \dots + a_0 = 0$. De même si n est impair, on obtient $x(x^2d)^{\frac{n-1}{2}} + \dots + a_1x = 0$ puis $(x^2d)^{\frac{n-1}{2}} + \dots + a_1 = 0$. Dans tous les cas, $x^2d \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]} \cap \mathbb{Q} = \mathbb{Z}$. Comme on a supposé que d n'est pas divisible par un carré parfait, il vient $x \in \mathbb{Z}$. \square

8.1 Cas où d n'est pas congru à 1 modulo 4

Proposition 8.1.1 *Si d n'est pas congru à 1 modulo 4, l'anneau des entiers est $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\sqrt{d}]$.*

Démonstration. On a $1 \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ et $\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. On en déduit que $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. Réciproquement, supposons que $x = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. Alors $Tr(x) = 2a \in \mathbb{Z}$. On en déduit que $2b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ et donc d'après le lemme précédent $2b \in \mathbb{Z}$. Ainsi x s'écrit $x = \frac{a'+b'\sqrt{d}}{2}$. Supposons a' et b' impairs. On a alors $N(x) = \frac{a'^2 - db'^2}{4} \in \mathbb{Z}$ et on en déduit que d est congru à 1 modulo 4 ce qui est supposé faux. On en déduit que a' ou b' est pair puis les deux par le lemme précédent. \square

Regardons les nombres premiers p en lesquels K se ramifie.

Proposition 8.1.2 *K se ramifie en p si et seulement si p divise d ou $p = 2$.*

Démonstration. Calculons le discriminant absolu de K , il vaut :

$$\begin{vmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr(d) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & d \end{vmatrix} = 4d$$

ce qui permet de conclure. \square

Essayons de déterminer les idéaux au-dessus de $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$.

Si p divise d , considérons l'idéal $\mathfrak{p} = p\mathbb{Z} + \sqrt{d}\mathbb{Z}$. Montrons que c'est un idéal premier. Pour cela, supposons que $(a + b\sqrt{d})(a' + b'\sqrt{d}) \in \mathfrak{p}$. On obtient alors p divise $aa' + dbb'$ et donc p divise aa' , soit p

divise a ou p divise a' , ce qui montre bien que \mathfrak{p} est premier. Finalement, on vérifie que $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathfrak{p}^2$ et donc \mathfrak{p} est le seul idéal premier au-dessus de $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$.

Si $p = 2$ et d est impair, considérons $\mathfrak{p} = \left\{ a + b\sqrt{d} \mid a \equiv b \pmod{2} \right\}$ et supposons que $(a + b\sqrt{d})(a' + b'\sqrt{d}) \in \mathfrak{p}$. On obtient alors $aa' + dbb' \equiv ab' + ba' \pmod{2}$. Si a est pair et b est impair, on obtient $db' \equiv a' \pmod{2}$ et donc $a' \equiv b' \pmod{2}$. Si a est impair et b est pair, on obtient directement $a' \equiv b' \pmod{2}$. On en déduit que \mathfrak{p} est un idéal premier. Il ne reste plus qu'à vérifier que $2\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathfrak{p}^2$ pour prouver qu'il s'agit du seul idéal premier au-dessus de $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$.

Dans le cas où p est différent de 2 et p ne divise pas d , on suppose de plus de d est un carré modulo p . On considère alors ω une racine carrée de d et $\mathfrak{p}_1 = \left\{ a + b\sqrt{d} \mid a \equiv \omega b \pmod{p} \right\}$ et supposons que $(a + b\sqrt{d})(a' + b'\sqrt{d}) \in \mathfrak{p}_1$. On obtient alors $aa' + dbb' \equiv \omega(ab' + ba') \pmod{p}$ qui s'écrit également $(a - \omega b)(a' - \omega b') \equiv 0 \pmod{p}$, ce qui prouve que \mathfrak{p}_1 est premier. De même, $\mathfrak{p}_2 = \left\{ a + b\sqrt{d} \mid a \equiv -\omega b \pmod{p} \right\}$ est un idéal premier. On vérifie alors que $\mathfrak{p}_1 \neq \mathfrak{p}_2$ et donc ce sont les seuls idéaux premiers au-dessus de $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$.

Une application du théorème des unités.

Le théorème des unités de Dirichlet permet ici de retrouver la forme des solutions de l'équation de Pell-Fermat $a^2 - db^2 = \pm 1$. En effet, le degré de l'extension K/\mathbb{Q} est clairement 2 et comme $K \subset \mathbb{R}$, on trouve $r = 2$ et $s = 0$. Ainsi $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}^*$ est isomorphe à $\{\pm 1\} \times \mathbb{Z}$.

Or les éléments de $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}^*$ sont exactement les $a + b\sqrt{d}$ avec $a^2 - db^2 = \pm 1$.

8.2 Cas où d est congru à 1 modulo 4

Proposition 8.2.1 *Si d est congru à 1 modulo 4, l'anneau des entiers est $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z} + \frac{1}{2}(1 + \sqrt{d})\mathbb{Z}$.*

Démonstration. On a $1 \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. D'autre part $\frac{1+\sqrt{d}}{2}$ est solution de l'équation $x^2 - x - \frac{d-1}{4} = 0$.

Réciproquement si $x = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$, on en déduit comme précédemment que x s'écrit $\frac{a'+b'\sqrt{d}}{2}$ où a' et b' sont des entiers et que 4 divise $a'^2 - db'^2$. En regardant, les congruences modulo 4, on trouve que a' et b' doivent être de même parité et donc le résultat voulu. \square

Proposition 8.2.2 *K se ramifie en p si et seulement si p se ramifie en d .*

Démonstration. Calculons le discriminant absolu de K , il vaut :

$$\begin{vmatrix} \text{Tr}(1) & \text{Tr}\left(\frac{1+\sqrt{d}}{2}\right) \\ \text{Tr}\left(\frac{1+\sqrt{d}}{2}\right) & \text{Tr}\left(\frac{d+1+2\sqrt{d}}{4}\right) \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{vmatrix} = d$$

ce qui permet de conclure. \square

8.3 Extension au cas général

Dans le cas général, si $d = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (où les p_i sont des nombres premiers distincts et les α_i des entiers strictement positifs), on remarque que $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d'}]$ avec $d' = p_1^{\beta_1} \dots p_k^{\beta_k}$ où β_i est le reste de la division euclidienne de α_i par 2. Mais d' n'est alors multiple d'aucun carré parfait et ainsi on est ramené au cas précédent.

Références

- [1] SAMUEL, Pierre, *Théorie algébrique des nombres*, Paris, Hermann, 1971, 130 p.
- [2] NEUKIRCH, Jürgen, *Algebraic number theory*, Berlin, Springer, 1999, p. 1-58
- [3] DOUADY, R. et A., *Algèbre et théories galoisiennes*, Paris, Cedic/Fernand Nathan, 1979, vol. 2