Théorie des nombres

Benjamin Schraen

28 août 2023

Table des matières

Tous les anneaux seront supposés commutatifs sauf éventuelle exception, auquel cas le caractère non commutatif sera précisé explicitement.

Chapitre 1

Anneaux de Dedekind et ramification

Référence : [Ser68].

1.1 Anneaux de Dedekind

1.1.1 Anneaux de valuation discrète

Définition 1.1.1. *Un* anneau de valuation discrète *est un anneau principal ayant un unique idéal premier non nul.*

Soit A un anneau de valuation discrète d'idéal premier non nul $\mathfrak{m}$. En particulier $\mathfrak{m}$ est l'unique idéal maximal de l'anneau A, qui est donc local. Comme A est principal, l'idéal $\mathfrak{m}$ est engendré par un élément π qui est non diviseur de zéro. En particulier A est factoriel et tout élément non nul de A s'écrit de façon unique sous la forme $u\pi^n$ pour $u \in A^\times$ et $n \in \mathbb{N}$. Soit K le corps des fractions de A. La décomposition ci-dessus implique que $K = A[\pi^{-1}]$ et donc que K est isomorphe au localisé de A relativement à la partie multiplicative $\{\pi^n \mid n \in \mathbb{N}\}$. Tout élément non nul de K s'écrit donc de façon unique sous la forme $u\pi^n$ où $u \in A^\times$ et $n \in \mathbb{Z}$.

On peut alors définir une application $v : K \longrightarrow \mathbb{Z} \cup \{+\infty\}$ en posant $v(x) = n$ si $x = u\pi^n$ avec $u \in A^\times$ et $n \in \mathbb{Z}$ et $v(0) = +\infty$. Cette application a les propriétés suivantes :

$$\forall (x, y) \in K^2, \quad \begin{cases} v(xy) = v(x) + v(y) \\ v(x + y) \geqslant \min\{v(x), v(y)\} \\ v(K \smallsetminus \{0\}) = \mathbb{Z}. \end{cases}$$

Une telle application est appelée une *valuation discrète* (normalisée) sur K. De plus, on a

$$A = \{x \in K \mid v(x) \geqslant 0\}.$$

Exercice 1.1.1. Vérifier que si v est une valuation discrète normalisée sur un corps K, alors, pour $x, y \in K$ tels que $v(x) < v(y)$, on a $v(x+y) = v(x)$.

Si K est un corps muni d'une valuation discrète v, on note K° l'ensemble $\{x \in K \mid v(x) \geqslant 0\}$. C'est un sous-anneau de K appelé *anneau de valuation* de (K, v).

Proposition 1.1.2. *Un anneau A est un anneau de valuation discrète si et seulement si il est isomorphe à l'anneau de valuation d'une valuation discrète d'un corps K. Le corps K est alors isomorphe au corps des fractions de A.*

Démonstration. La preuve est laissée en exercice. □

Exemple 1.1.3. Si A est un anneau principal et si $\mathfrak{p}$ est un idéal premier non nul de A, alors $A_\mathfrak{p}$ est un anneau de valuation discrète. En effet, le localisé d'un anneau principal est principal et $A_\mathfrak{p}$ est donc un anneau principal possédant un unique idéal maximal, qui est non nul. Comme les idéaux premiers non nuls d'un anneau principal sont maximaux, $A_\mathfrak{p}$ possède un unique idéal premier non nul et est donc de valuation discrète.

Exemple 1.1.4. Soit A un anneau factoriel et soit p un élément irréductible de A. On note v_p la valuation p-adique sur A. La propriété $v_p(xy) = v_p(x) + v_p(y)$ nous permet d'étendre v_p de façon unique en une application $v_p : K \to \mathbb{Z}$ en posant $v_p(a/b) = v_p(a) - v_p(b)$. L'application v_p est une valuation discrète de sorte que son anneau de valuation $\{x \in K \mid v_p(x) \geqslant 0\}$ est un anneau de valuation discrète. Il s'agit également du localisé $A_{(p)}$ de A en l'idéal premier (p).

Comme conséquence des deux exemples ci-dessus (au choix), on déduit que l'anneau $\mathbb{Z}_{(p)}$ des nombre rationnels de la forme a/b avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ premier à p est un anneau de valuation discrète. Si k est un corps le localisé de $k[X, Y]$ en l'idéal premier (P) où P est un polynôme irréductible est aussi un anneau de valuation discrète. Par exemple $\mathbb{C}[X, Y]_{(Y^2+X^2+X)}$ est un anneau de valuation discrète.

Le critère suivant est très utile pour vérifier qu'un anneau est un anneau de valuation discrète.

Proposition 1.1.5. *Un A est de valuation discrète si et seulement si c'est un anneau local noethérien qui est intègre et dont l'unique idéal maximal est engendré par un élément non nul.*

Démonstration. Soit π un générateur de l'unique idéal maximal de A. L'intersection $\bigcap_{n\geqslant 0}(\pi^n)$ est réduite à 0. En effet si x est un élément de cette intersection, on peut écrire $x = \pi^n x_n$ avec $x_n \in A$ pour tout $n \geqslant 0$. La suite des idéaux (x_n) est alors croissante et donc stationnaire. Cela implique que $x_{n+1} = ax_n$ avec $a \in A$ pour n assez grand. Ainsi $x_{n+1} = a\pi x_{n+1}$. Comme $\pi \notin A^\times$, on en conclut que $x_{n+1} = 0$ et donc $x = 0$.

Soit $x \in A \smallsetminus \{0\}$. Alors il existe un plus grand $n \geqslant 0$ tel que $x \in (\pi^n)$ de sorte que x s'écrit de façon unique sous la forme $\pi^n u$ avec $u \in A^\times$. On pose $v(x) = n$. On vérifie facilement que v se prolonge en une valuation discrète du corps des fractions de A et que A est l'anneau de cette valuation. □

Remarque 1.1.6. Dans la proposition 1.1.5 l'hypothèse d'intégrité sur A n'est pas nécessaire si on suppose que l'idéal maximal est engendré par un élément non nilpotent (voir [Ser68, Ch. I Prop. 2]).

Exemple 1.1.7. Posons $A = \mathbb{Z}_{(3)}[\sqrt[3]{2}] \subset \mathbb{Q}(\sqrt[3]{2})$. Il s'agit d'un anneau intègre et noethérien. En effet, il s'agit d'un $\mathbb{Z}_{(3)}$-module de type fini et $\mathbb{Z}_{(3)}$ est noethérien comme localisation de $\mathbb{Z}$. De plus, il suit du théorème A.3.1 que A est entier sur $\mathbb{Z}_{(3)}$. Vérifions qu'il possède un unique idéal maximal engendré par un élément non nul. Si $\mathfrak{m}$ est un idéal maximal de A, alors $\mathfrak{m} \cap \mathbb{Z}_{(3)}$ est un idéal maximal de $\mathbb{Z}_{(3)}$ par la proposition A.3.4. On en déduit que $\mathfrak{m} \cap \mathbb{Z}_{(3)} = 3$ et donc que $(3) \subset \mathfrak{m}$. Ainsi $\mathfrak{m}/(3)$ est un idéal maximal de $A/(3) \simeq \mathbb{F}_3[X]/(X^3 - 2) = \mathbb{F}_3[X]/(X + 1)^3$. Cet anneau a un unique idéal maximal qui est engendré par $(X + 1)$. On en déduit que A est local d'idéal maximal $\mathfrak{m} = (3, \sqrt[3]{2} + 1)$. Or

$$(\sqrt[3]{2} + 1)^3 = 2 + 3\sqrt[3]{2}^2 + 3\sqrt[3]{2} + 1 = 3(1 + \sqrt[3]{2} + \sqrt[3]{2}^2).$$

Comme $(1 + \sqrt[3]{2} + \sqrt[3]{2}^2)(\sqrt[3]{2} - 1) = 1$, on en déduit que $3 \in (\sqrt[3]{2} + 1)$ et donc que $\mathfrak{m} = (\sqrt[3]{2} + 1)$. Ainsi la proposition 1.1.5 implique que A est un anneau de valuation discrète. Sa valuation normalisée v vérifie $v(\sqrt[3]{2} + 1) = 1$ et $v(3) = 3$.

1.1.2 Anneaux de Dedekind

Définition 1.1.8. *On dit qu'un anneau A est un* anneau de Dedekind *s'il est intègre, noethérien et si, pour tout idéal premier $\mathfrak{p}$ non nul de A, $A_\mathfrak{p}$ est un anneau de valuation discrète.*

On a la caractérisation suivante des anneaux de Dedekind.

Proposition 1.1.9. *Un anneau A est un anneau de Dedekind si et seulement si il vérifie les conditions suivantes :*

— *l'anneau A est noethérien ;*
— *l'anneau A est intégralement clos ;*
— *tout idéal premier non nul de A est maximal.*

Démonstration. Voir [Ser68, Ch. I Prop. 4]. □

Exemple 1.1.10. Tout anneau principal est un anneau de Dedekind. En particulier tout corps est un anneau de Dedekind.

Exemple 1.1.11. Si A est un anneau de Dedekind et S est une partie multiplicative de A, alors A_S est un anneau de Dedekind.

Ainsi $\mathbb{Z}$, $k[X]$ pour un corps k, ainsi que leurs localisés sont des anneaux de Dedekind. Nous verrons d'autres exemples plus loin.

Rappelons qu'un idéal I d'un anneau intègre A est dit *inversible* s'il existe un sous-A-module J de son corps des fractions tel que $IJ = A$ (ici IJ désigne le plus petit sous-A-module de $\mathrm{Frac}(A)$ contenant les produits d'éléments de I par des éléments de J, c'est aussi l'ensemble des sommes finies de la forme $\sum x_i y_i$ où les x_i sont dans I et les y_j dans J).

Théorème 1.1.12. *Soit A un anneau de Dedekind. Alors*
— *tout idéal non nul de A est inversible et son inverse est unique ;*
— *tout idéal non nul de A s'écrit de façon unique (à l'ordre près) sous la forme d'un produit d'idéaux maximaux de A.*

Démonstration. Voir [Ser68, Ch. I Prop. 5 et 7]. □

Si A est un anneau de Dedekind, un sous-A-module de type fini du corps des fractions de A est appelé *idéal fractionnaire* de A. On peut additionner et multiplier les idéaux fractionnaires comme on additionne et multiplie les idéaux de A. On peut facilement généraliser le théorème 1.1.12 aux idéaux fractionnaires non nul de A. En effet, si $\mathfrak{p}$ est un idéal premier non nul de A, on note $\mathfrak{p}^{-1}$ son inverse et, pour tout $n \in \mathbb{Z}$, on pose $\mathfrak{p}^n = \mathfrak{p}^n$ si $n \geqslant 0$ et $\mathfrak{p}^n = (\mathfrak{p}^{-1})^{-n}$ si $n \leqslant 0$. On a alors le résultat suivant.

Corollaire 1.1.13. *Soit A un anneau de Dedekind et soit I un idéal fractionnaire non nul de A. Alors I s'écrit de façon unique sous la forme*

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$$

où les $\mathfrak{p}_i$ sont des idéaux maximaux de A et les n_i des entiers relatifs.

Si $\mathfrak{p}$ est un idéal premier non nul d'un anneau de Dedekind A, alors, pour tout $a \in K$, on note $v_{\mathfrak{p}}(a)$ l'exposant de $\mathfrak{p}$ dans la décomposition de l'idéal fractionnaire $(a) = Aa$.

Exercice 1.1.2. Vérifier que $v_{\mathfrak{p}}$ définit une valuation discrète sur le corps des fractions de A. Vérifier que l'anneau de valuation de $v_{\mathfrak{p}}$ est le localisé $A_{\mathfrak{p}}$.

Soit A un anneau de Dedekind. L'ensemble $I(A)$ des idéaux fractionnaires non nuls de A forme donc un groupe (commutatif) pour la multiplication. L'ensemble des idéaux fractionnaires *principaux* (c'est-à-dire de la forme Aa pour un $a \in K^\times$) forme un sous-groupe $P(A)$ de $I(A)$. Le groupe quotient $\mathrm{Cl}(A) \coloneqq I(A)/P(A)$ est appelé *groupe des classes d'idéaux* de A.

Exemple 1.1.14. Si A est un anneau de Dedekind, le groupe $\mathrm{Cl}(A)$ est trivial si et seulement si A est un anneau principal.

On utilisera souvent le résultat suivant :

Lemme 1.1.15. *Soit A un anneau de Dedekind. Soit $\mathfrak{p}$ un idéal premier non nul de A. Si I est un idéal fractionnaire non nul de A, on a un isomorphisme de A-modules $I/I\mathfrak{p} \simeq A/\mathfrak{p}$.*

Démonstration. Comme $\mathfrak{p}$ est un idéal maximal de A et I est inversible, il n'existe pas de A-module contenu strictement entre I et $I\mathfrak{p}$. Le A-module $I/I\mathfrak{p}$ est donc simple. Il est de plus non nul d'après la propriété d'unique factorisation des idéaux fractionnaires (corollaire 1.1.13). Il est donc isomorphe à un A-module de la forme A/J où J est un idéal de A. Comme $I/I\mathfrak{p}$ est annulé par $\mathfrak{p}$, on a $\mathfrak{p} \subset I$ et donc $\mathfrak{p} = I$ par maximalité de $\mathfrak{p}$. □

1.2 Extensions d'anneaux de Dedekind

1.2.1 Rappels sur les extensions de corps

Soit L/K une extension de corps, c'est-à-dire une inclusion $K \subset L$ entre corps telle que L est un K-espace vectoriel de dimension finie.

On dit qu'un élément $\alpha \in L$ est *séparable* sur K si son polynôme minimal est séparable, c'est-à-dire à racines simples ou encore premier avec son polynôme dérivé. On dit que L est *séparable* sur K si tous les éléments de L sont séparables sur K. Si K est de caractéristique 0, toute extension finie de K est séparable.

Si un corps K n'est pas de caractéristique 0, il est de caractéristique p pour un nombre premier p. Dans ce cas l'application $x \mapsto x^p$ est un endomorphisme de K appelé *endomorphisme de Frobenius*. C'est un endomorphisme injectif mais qui n'est pas toujours surjectif. On dit qu'un corps K est *parfait* s'il est de caractéristique 0 ou s'il est de caractéristique finie p et son endomorphisme de Frobenius est bijectif (de façons équivalente, surjectif).

Si K est un corps de caractéristique p, où p est un nombre premier, et si L est une extension finie de K, tout élément $\alpha \in L$ qui n'est pas séparable sur K a un polynôme minimal de la forme $P(X^p)$ avec $P \in K[X]$. On en déduit facilement que si K est parfait, tout extension finie de L est séparable.

Les corps finis sont des corps parfaits (car un endomorphisme injectif d'un corps fini est bijectif) et donc, toutes leurs extensions finies sont séparables.

Exemple 1.2.1. Soit $K = \mathbb{F}_p(T)$. Le polynôme $X^p - T$ est irréductible sur $\mathbb{F}_p(T)$ (pour le prouver, s'intéresser à la valuation T-adique du terme constant d'un diviseur de $X^p - T$). Ainsi un corps de rupture L de K est une extension finie de K qui n'est pas séparable. En effet, $L = K(T^{1/p})$ et le polynôme minimal de $T^{1/p}$ sur K est $X^p - T$ qui n'est pas séparable. En effet, dans L, on a $X^p - T = (X - T^{1/p})^p$.

On dit qu'une extension finie L/K est *radicielle* si K est de caractéristique p pour p premier et s'il existe $n \geqslant 1$ tel que $x^{p^n} \in K$ pour tout $x \in L$.

De façon générale, si L/K est une extension finie, il existe une plus grande sous-extension $K' \subset L$ telle que K'/K est séparable et L/K' est radicielle. L'extension K'/K est la plus grande sous-extension séparable de L/K.

On rappelle qu'une extension finie L/K est *normale* si le polynôme minimal de tout élément de L est scindé dans $L[X]$. Une extension est dite *galoisienne* si elle est séparable et normale. Dans ce cas on note $\mathrm{Gal}(L/K)$ le groupe des automorphismes de L qui fixent les points de K. Si M/K est une sous-extension de L/K, alors l'extension L/M est galoisienne (et non pas M/K comme je l'ai trop vu écrit dans les examens écrits) et $\mathrm{Gal}(L/M)$ est un sous-groupe de $\mathrm{Gal}(L/K)$. L'extension M/K est galoisienne si et seulement si le groupe $\mathrm{Gal}(L/M)$ est distingué dans $\mathrm{Gal}(L/K)$. Le théorème fondamental de la théorie de Galois affirme que $[L : K] = \mathrm{Card}(\mathrm{Gal}(L/K))$ et que l'application $(M/K) \mapsto \mathrm{Gal}(L/M)$ est une bijection décroissante de l'ensemble des sous-extensions de L/K sur l'ensemble des sous-groupes de $\mathrm{Gal}(L/M)$.

De façon générale, si L/K est une extension finie, on note $\mathrm{Aut}_K(L)$ le groupe des automorphismes de L qui fixent les éléments de K. Si L/K est galoisienne, on a $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$. Plus généralement, si L/K est normale, soit L' la plus grande sous-extension séparable de K. Alors L'/K est galoisienne, L' est stable par $\mathrm{Aut}_K(L)$ et la restriction $\sigma \mapsto \sigma|_{K'}$ induit un isomorphisme de groupes

$\mathrm{Aut}_K(L) \xrightarrow{\sim} \mathrm{Gal}(L'/K)$. Toujours dans le cas où L/K est normale, il existe une sous-extension radicielle K'/K de L/K telle que L/K' est séparable et même galoisienne. Le corps K' est obtenu comme le sous-corps $L^{\mathrm{Aut}_K(L)}$ des points fixes de L sous $\mathrm{Aut}_K(L)$.

Soit L/K une extension finie. Si $\alpha \in L$, on note m_α l'application K-linéaire

$$m_\alpha : \begin{array}{ccc} L & \longrightarrow & L \\ x & \longmapsto & \alpha x \end{array}.$$

On définit alors des éléments de K par les formules

$$\mathrm{Tr}_{L/K}(\alpha) \coloneqq \mathrm{Tr}(m_\alpha), \quad N_{L/K}(\alpha) \coloneqq \det(m_\alpha).$$

Ce sont des éléments de K que l'on appelle respectivement *trace* et *norme* de α relativement à L/K. On vérifie facilement que

$$\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta), \quad N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta).$$

De plus si $\alpha \in K$ et $\beta \in L$, on a $m_{\alpha\beta} = \alpha m_\beta$ de sorte que

$$\mathrm{Tr}_{L/K}(\alpha\beta) = \alpha\,\mathrm{Tr}_{L/K}(\beta), \quad N_{L/K}(\alpha\beta) = \alpha^{[L:K]}N_{L/K}(\beta).$$

Si L/K est radicielle et K de caractéristique p, alors il existe une tour d'extensions

$$K = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n = L$$

avec $[K_{i+1} : K_i] = p$ pour tout $1 \leqslant i \leqslant n-1$ et $K_{i+1} = K_i(x_i^{1/p})$ pour un certain $x_i \in K_i$. On en déduit que $\mathrm{Tr}_{L/K} = 0$ pour toute extension radicielle non triviale. On en déduit plus généralement que $\mathrm{Tr}_{L/K} = 0$ dès que l'extension finie est non séparable.

On note $b_{L/K}$ la forme K-bilinéaire sur L définie par $b_{L/K}(x,y) \coloneqq \mathrm{Tr}_{L/K}(xy)$ si $x, y \in L$.

Proposition 1.2.2. *Soit L/K une extension finie. Alors la forme $b_{L/K}$ est non dégénérée si et seulement si l'extension L/K est séparable.*

Démonstration. Supposons l'extension L/K séparable. Soit Σ l'ensemble des plongements K-linéaires de L dans une clôture normale $\tilde{L}$. Alors Σ est de cardinal $n = [L:K]$ et $\mathrm{Tr}_{L/K} = \sum_{\sigma\in\Sigma}\sigma$. Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ une base de L sur K et soit $M = (b_{L/K}(\alpha_i, \alpha_j))_{1\leqslant i,j\leqslant d}$ la matrice de $b_{L/K}$ dans la base $\underline{\alpha}$. On a alors $M = {}^tNN$ où $N = (\sigma(\alpha_i))_{\sigma\in\Sigma, 1\leqslant i\leqslant d}$. Ainsi $\det(M) = \det(N)^2$. Les morphismes $\sigma : L^\times \to \tilde{L}^\times$ forment une familles de caractères distincts de $L^\times$. Ainsi, par le lemme d'indépendance des caractères, ils forment une famille $\tilde{L}$-libre d'applications de $L^\times$ vers $\tilde{L}$. Ceci implique $\det(N) \neq 0$ et donc $\det(M) \neq 0$.

Supposons L/K non séparable. Le résultat est évident car alors $b_{L/K} = 0$ puisque $\mathrm{Tr}_{L/K} = 0$. □

Si $(\alpha_1, \ldots, \alpha_n) \in L^n$ est une base L sur K, on appelle *discriminant* de la famille $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ le déterminant de la matrice de $b_{L/K}$ dans $\underline{\alpha}$. Cest l'élément

$$\Delta_{L/K}(\underline{\alpha}) := \det((\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}}).$$

Exemple 1.2.3. Considérons le cas où K est de caractéristique différente de 2 et $L = L(\sqrt{d})$ avec $d \in K$ non carré. On a alors

$$\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d}) = 2a, \quad N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2.$$

De plus,

$$\Delta_{L/K}(1, \sqrt{d}) = 4d.$$

Supposons que $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ est une base de L sur K et que $\underline{\beta} = (\beta_1, \ldots, \beta_n)$ en est une autre. Soit $P \in \mathrm{GL}_n(K)$ la matrice de passage de $\underline{\alpha}$ à $\underline{\beta}$, c'est-à-dire $\underline{\beta} = \underline{\alpha}P$. On a alors :

$$\Delta_{L/K}(\underline{\beta}) = \det(P)^2\Delta_{L/K}(\underline{\alpha}). \tag{1.1}$$

1.2.2 Extensions finies d'un anneau de Dedekind

Soit A un anneau de Dedekind et soit K son corps des fractions. Soit L/K une extension finie de K. On note B la clôture intégrale de A dans L (définition A.3.6). Si $x \in L$, il existe un polynôme unitaire $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ tel que $P(x) = 0$. Comme K est le corps des fractions de A, il existe un élément $\alpha \in K^\times$ tel que $\alpha a_i \in A$ pour tout $0 \leqslant i \leqslant d-1$. L'élément αx est alors annulé par le polynôme $\alpha^d P(\alpha^{-1}X)$ qui est unitaire à coefficients dans A. Ainsi $\alpha x \in B$. On en déduit en particulier que L est le corps des fractions de B et que l'application $K \otimes_A B \to L$ donnée par la multiplication est surjective. Cette application est de plus injective compte tenu du fait que B est intègre et que $K \otimes_A B$ est le localisé de B en $A \smallsetminus \{0\}$ et L le localise de B en $B \smallsetminus \{0\}$. La multiplication induit donc un isomorphisme $K \otimes_A B \xrightarrow{\sim} L$.

Le résultat suivant est un moyen de commode de construire de nouveaux exemples d'anneaux de Dedekind.

Théorème 1.2.4. *Soit A un anneau de Dedekind et soit K son corps des fractions. Soit L/K une extension finie de K. Alors la clôture intégrale B de A dans L est un anneau de Dedekind. Si de plus l'extension L/K est séparable ou si A est isomorphe à $k[T]$ où k désigne un corps parfait, alors B est un A-module de type fini.*

Démonstration. Commençons par prouver que B est un anneau de Dedekind si B est un A-module de type fini. Nous prouverons ensuite que B est un A-module de type fini si L/K est séparable ou si A est isomorphe à $k[T]$ avec k parfait. Pour le cas général, nous renvoyons à [Bou85, Ch. VII §2], corollaire 2 à la proposition 5.

Si B est un A-module de type fini, alors B est un A-module noetherien et donc un B-module noethérien, c'est donc bien un anneau noethérien. Il est intégralement clos par construction. D'après la proposition 1.1.9, il reste donc à prouver que tout idéal premier non nul $\mathfrak{q}$ de B est maximal. Soit $\mathfrak{p}$ un tel idéal. L'idéal $\mathfrak{q} \coloneqq \mathfrak{p} \cap A$ est alors un idéal premier non nul de A d'après la proposition A.3.3. Comme A est de Dedekind, l'idéal $\mathfrak{q}$ est maximal. Ainsi $B/\mathfrak{p}$ est une $A/\mathfrak{q}$-algèbre de type fini qui est de plus intègre, c'est donc un corps. Ainsi $\mathfrak{p}$ est maximal.

Montrons à présent que si L/K est séparable, alors B est un A-module de type fini. D'après la proposition 1.2.2, si L/K est séparable, la forme K-bilinéaire $b : (x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ est non dégénérée. Ainsi pour toute K-base $(e_1, \ldots, e_d)$ de L, il existe une unique K-base $(e_1^*, \ldots, e_d^*)$ de L telle que $b(e_i, e_j^*) = \delta_{i,j}$ pour tous $1 \leqslant i, j \leqslant d$. Si M est un sous-A-module de L, on note M^* le sous-A-module $\{x \in K \mid \mathrm{Tr}(xM) \subset A\}$. Il est alors facile de vérifier que

$$\left(\bigoplus_i Ae_i\right)^* = \bigoplus_i Ae_i^*.$$

Comme $L \simeq B \otimes_A K$, il existe une K-base $(e_1, \ldots, e_d)$ de L sur K formée d'éléments de B. Ainsi

$$\bigoplus_i Ae_i \subset B \subset B^* \subset \bigoplus_i Ae_i^*,$$

ce qui implique que B est un sous-A-module d'un A-module de type fini. Comme A iest noethérien, le A-module B est de type fini.

Supposons à présent que $A = k[T]$ avec k corps parfait. Montrons que B est un A-module de type fini. Comme le cas séparable a déjà été traité, on peut se limiter au cas où k est un corps de caractéristique p pour p un nombre premier. Soit M la clôture normale de L/K et soit C be la clôture intégrale de A dans C. On a clairement $B \subset C$ ainsi, si C est un A-module de type fini, c'est aussi le cas de B puisque A est noethérien. Il suffit donc de prouver l'assertion lorsque l'extension L/K est normale. Dans ce cas il existe une sous-extension $K \subset N \subset L$ telle que L/N est séparable et N/K est radicielle. Soit D la clôture integrale de A dans N. Alors B est la clôture intégrale de D dans L. Comme L/N est séparable, le D-module B est de type fini d'après le cas séparable traité ci-dessus. On est donc ramené à prouver l'assertion lorsque l'extension L/K est radicielle. Supposons donc L/K radicielle, c'est-à-dire qu'il existe $n \geqslant 1$ tel que $x^{p^n} \in K$ pour tout $x \in L$. En raisonnant par récurrence sur le degré $[L : K]$, on peut supposer que

$n = 1$ et que L/K est de degré p. On est donc dans le cas où $K = k(T)$ k et $L = K(P(T)^{1/p}) = k(T, P(T)^{1/p})$ pour $P(T) \in K[X]$. Comme k est un corps parfait, on peut écrire $P(T)^{1/p} = P_1(T^{1/p})$ pour un polynôme $P_1 \in K[T]$. Ainsi $L \subset K(T^{1/p})$ et $L = k(T^{1/p})$ par un argument de degré. Comme l'anneau $k[T^{1/p}]$ est isomorphe à $k[T]$, il est principal et donc intégralement clos. On en conclut que $B = k[T^{1/p}]$ qui est bien un $A = k[T]$-module de rang fini. □

Remarque 1.2.5. Dans la situation du théorème 1.2.4, si B est un A-module de type fini, B est en particulier un A-module projectif. En effet, $B_\mathfrak{p}$ est un $A_\mathfrak{p}$-module sans torsion de type fini sur l'anneau principal $A_\mathfrak{p}$, il est donc libre et donc projectif. On conclut en utilisant le lemme A.2.2.

L'utilisation de discriminants peut être très utile pour déterminer explicitement la clôture intégrale d'un anneau de Dedekind dans une extension finie.

Proposition 1.2.6. *Soit A un anneau de Dedekind de corps des fractions K. Soit L/K une extension finie séparable. Soit B un sous-anneau de L contenant A. On suppose que B est un A-module de type fini et qu'il existe une K-base $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$ de L constituée d'éléments de B telle que, pour tout idéal premier non nul $\mathfrak{p}$ de A, $v_\mathfrak{p}(\Delta_{L/K}(\underline{\alpha})) \leqslant 1$. Alors B est la clôture intégrale de A dans L. En particulier B est un anneau de Dedekind. De plus B est un A-module libre de base $\underline{\alpha}$.*

Démonstration. Posons $M = \bigoplus_{i=1}^{n} A\alpha_i$. Soit C la clôture intégrale de A dans L. Comme B est un A-module de type fini, les éléments de B sont entiers sur A d'après le théorème A.3.1. Ainsi on a $M \subset B \subset C$. D'après le lemme A.2.1, il suffit de prouver que $M_\mathfrak{p} = C_\mathfrak{p}$ pour tout idéal maximal $\mathfrak{p}$ de A. Soit $\mathfrak{p}$ un idéal maximal de A. Si $\mathfrak{p} = 0$, alors $A = K$ et $B = L$, d'où le résultat. On peut donc supposer $\mathfrak{p} \neq 0$. Remarquons que $M_\mathfrak{p}$ et $C_\mathfrak{p}$ sont tous deux des $A_\mathfrak{p}$-modules de type fini, sans torsion, et donc des $A_\mathfrak{p}$-modules libres (puisque $A_\mathfrak{p}$ est principal) de même rang (puisque $B \otimes_A K = C \otimes_A K$). La famille $\underline{\alpha}$ forme une base de $M_\mathfrak{p}$ sur $A_\mathfrak{p}$. Soit $\underline{\beta} = (\beta_1, \dots, \beta_n)$ une $A_\mathfrak{p}$-base de $C_\mathfrak{p}$. Soit $P = P_{\underline{\beta},\underline{\alpha}}$ la matrice de passage de $\underline{\beta}$ à $\underline{\alpha}$. On a $P \in M_n(A_\mathfrak{p})$ puisque $M_\mathfrak{p} \subset C_\mathfrak{p}$ et $\Delta_{L/K}(\underline{\alpha}) = \det(P)^2 \Delta_{L/K}(\underline{\beta})$. Ainsi

$$2v_\mathfrak{p}(\det(P)) \leqslant 2v_\mathfrak{p}(\det(P)) + v_\mathfrak{p}(\Delta_{L/K}(\underline{\beta})) \leqslant v_\mathfrak{p}(\Delta_{L/K}(\underline{\alpha}) \leqslant 1.$$

On en déduit que $v_\mathfrak{p}(\det(P)) = 0$, c'est-à-dire $\det(P) \in \mathrm{GL}_n(A_\mathfrak{p})$. Ainsi $M_\mathfrak{p} = C_\mathfrak{p}$. □

1.2.3 Corps de nombres

On appelle *corps de nombres* une extension finie de $\mathbb{Q}$. L'*anneau des entiers* d'un corps de nombres K est la clôture intégrale de $\mathbb{Z}$ dans K. On le note $\mathcal{O}_K$. D'après le théorème 1.2.4, l'anneau $\mathcal{O}_K$ est un anneau de Dedekind et c'est même un $\mathbb{Z}$-module de type fini. Comme il est sans torsion et que $K \simeq \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}$, il s'agit d'un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$.

L'exercice suivant est indispensable.

Exercice 1.2.1. Soit K un corps de nombres de degré 2 (autrement dit *quadratique*).

1. Montrer qu'il existe un entier $d \in \mathbb{Z} \setminus \{0, 1\}$ sans diviseurs carrés tel que $K = \mathbb{Q}(\sqrt{d})$.

2. Montrer que

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{si } d \equiv 1 \bmod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2 \text{ ou } 3 \bmod 4. \end{cases}$$

Exemple 1.2.7. Soit $x \in \mathbb{C}$ une racine du polynôme $X^3 - X + 1$. Il s'agit d'un polynôme irréductible de $\mathbb{Q}[X]$ car il est de degré 3 et n'a pas de racine dans $\mathbb{Q}$. Ainsi $X^3 - X + 1$ est le polynôme minimal de x sur $\mathbb{Q}$. Posons $K = \mathbb{Q}(x)$, on a donc $[K : \mathbb{Q}] = 3$. La famille $\underline{\alpha} = (1, x, x^2)$ est une base du $\mathbb{Z}$-module $\mathbb{Z}[x]$. Un calcul direct montre que $\Delta_{K/\mathbb{Q}}(\underline{\alpha}) = -23$ est premier. On déduit donc de la proposition 1.2.6 que $\mathcal{O}_K = \mathbb{Z}[x]$.

Exemple 1.2.8. Déterminons l'anneau des entiers de $K = \mathbb{Q}(\sqrt[3]{2})$. Posons $B = \mathbb{Z}[\sqrt[3]{2}]$. Cette fois-ci $\Delta_{K/\mathbb{Q}}(1, \sqrt[3]{2}, \sqrt[3]{2}^2) = -27 \cdot 4$, on ne peut donc pas utiliser la proposition 1.2.6 pour conclure. En utilisant la proposition 1.2.6 avec $A = \mathbb{Z}_{(p)}$, $B = \mathbb{Z}[\sqrt[3]{2}]_{(p)}$ et $C = \mathcal{O}_{K,(p)}$ on voit que $\mathbb{Z}[\sqrt[3]{2}]_{(p)} = \mathcal{O}_{K,(p)}$ si p est différent de 2 et 3. Dans l'exemple 1.1.7, on a déjà montré que $\mathbb{Z}[\sqrt[3]{2}]_{(3)}$ est un anneau de valuation discrète. Il est donc intégralement clos et, comme son corps de fractions est K, contient la clôture algébrique $\mathcal{O}_K$ de $\mathbb{Z}$ dans K. Ainsi $\mathbb{Z}[\sqrt[3]{2}]_{(3)} = \mathcal{O}_{K,(3)}$. On montre de même que $\mathbb{Z}[\sqrt[3]{2}]_{(2)}$ est un anneau de valuation discrète et donc que $\mathbb{Z}[\sqrt[3]{2}]_{(2)} = \mathcal{O}_{K,(2)}$. Ainsi $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.

Exercice 1.2.2. Déterminer l'anneau des entiers de $\mathbb{Q}(\sqrt[3]{6})$.

Exercice 1.2.3. Montrer que l'anneau $\mathbb{Z}[\sqrt[3]{10}]$ n'est pas intégralement clos.

Soit K un corps de nombres et soit I un idéal non nul de $\mathcal{O}_K$. D'après le lemme A.3.3, il existe un élément non nul $d \in I \cap \mathbb{Z}$. En particulier I contient l'idéal (d)

qui est un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$. On en conclut que I est un sous-$\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$ dans $\mathcal{O}_K$ et que $\mathcal{O}_K/I$ est un anneau fini. On note $N(I)$ son cardinal que l'on appelle *norme* de l'idéal I.

L'ensemble Σ des morphismes de corps de K dans $\mathbb{C}$ est de cardinal $[K : \mathbb{Q}]$. Un élément $\sigma \in \Sigma$ est dit *réel* si $\sigma(K) \subset \mathbb{R}$. La conjugaison complexe de $\mathbb{C}$ agit sur l'ensemble Σ par $\sigma \mapsto \overline{\sigma}$ et l'ensemble des plongements réels est exactement l'ensemble des points fixes de cette action. Si on note r_1 le nombre de plongements réels de K, il existe donc un entier r_2 tel que $[K : \mathbb{Q}] = r_1 + 2r_2$.

Exercice 1.2.4. Soit K un corps de nombres. Montrer que si $(\alpha_1, \dots, \alpha_n)$ est une base du $\mathbb{Z}$-module libre $\mathcal{O}_K$, le discriminant $\Delta_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$ est indépendant du choix de la base $(\alpha_1, \dots, \alpha_n)$.

On le note Δ_K le discriminant étudié dans l'exercice ci-dessus, on l'appelle *discriminant* (absolu) du corps de nombres.

Nous admettons temporairement le résultat suivant, qui sera démontré plus tard.

Théorème 1.2.9. *Soit K un corps de nombres de degré n. Le groupe des classes $\mathrm{Cl}(\mathcal{O}_K)$ de l'anneau $\mathcal{O}_K$ est fini. Plus précisément tout élément de $\mathrm{Cl}(\mathcal{O}_K)$ contient un idéal I de $\mathcal{O}_K$ tel que*

$$N(I) \leqslant \sqrt{|\Delta_K|} \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}.$$

Corollaire 1.2.10. *Si K est un corps de nombres de degré n, on a*

$$\sqrt{|\Delta_K|} \geqslant \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}.$$

1.2.4 Exemples de décompositions dans un anneau de Dedekind

Proposition 1.2.11. *Soit A un anneau de Dedekind et soit K son corps de fractions. Soit L/K une extension finie et soit B la clôture intégrale de A dans L. On suppose qu'il existe $x \in B$ tel que $B = A[x]$. Soit $P \in K[X]$ le polynôme minimal de x sur K. On a $P \in A[X]$. Soit $\mathfrak{p}$ un idéal maximal de A et soit $\overline{P}$ l'image de P dans $k(\mathfrak{p})[X]$. On note $\overline{P} = \prod_{i=1}^{r} P_i^{e_i}$ la factorisation de $\overline{P}$ comme produit de polynômes irréductibles où les P_i sont distincts. Pour chaque $1 \leqslant i \leqslant r$, on choisit*

$\widetilde{P}_i$ un relevé de P_i dans $A[X]$ et note $\mathfrak{q}_i$ l'idéal $\mathfrak{p}_i B + (\widetilde{P}_i(x))$ de B. Les idéaux maximaux de B contenant $\mathfrak{p}B$ sont exactement les $\mathfrak{q}_i$ et on a

$$\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}.$$

Démonstration. Commençons par remarquer que les conjugués de x sur K sont entiers sur A, de sorte que les coefficients de P sont des éléments de K entiers sur A. Comme A est intégralement clos (1.1.9), on a bien $P \in A[X]$. On en déduit que l'application $Q(X) \mapsto Q(x)$ induit un isomorphisme de A-algèbres $A[X]/(P) \xrightarrow{\sim} B$.

Ainsi les idéaux maximaux de B contenant $\mathfrak{p}B$ sont en bijection avec les idéaux maximaux de l'anneau

$$B/\mathfrak{p}B \simeq k(\mathfrak{p})[X]/(\overline{P}) \simeq \prod_{i=1}^{r} k(\mathfrak{p})[X]/(P_i^{e_i})$$

eux-même en bijection avec les idéaux maximaux de l'anneau $k(\mathfrak{p})[X]$ contenant $(\overline{P})$. Comme $k(\mathfrak{p})[X]$ est principal, ces derniers sont les idéaux principaux (P_i). On en déduit que les idéaux maximaux de B divisant $\mathfrak{p}$ sont les $\mathfrak{q}_i = \mathfrak{p}B + (\widetilde{P}_i(x))$.

Supposons $\mathfrak{p} \neq 0$. Comme B est un anneau de Dedekind, on peut décomposer $\mathfrak{p}B$ en produit d'idéaux maximaux $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^{a_i}$ pour des entiers $a_i \geqslant 1$. On déduit du lemme A.4.3 un isomorphisme de A-algèbres

$$\prod_{i=1}^{r} k(\mathfrak{p})[X]/(P_i^{e_i}) \simeq B/\mathfrak{p}B \simeq \prod_{i=1}^{r} B/\mathfrak{q}_i^{a_i}.$$

Soit $1 \leqslant i \leqslant r$. En localisant cet isomorphisme en $\mathfrak{q}_i$, on obtient $k(\mathfrak{p})[X]/(P_i^{e_i}) \simeq B/\mathfrak{q}_i^{a_i}$ et donc $e_i = a_i$. On remarque immédiatement que l'énoncé reste vrai si $\mathfrak{p} = 0$. □

Exemple 1.2.12. Soit $K = \mathbb{Q}$. On a alors $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \simeq \mathbb{Z}[X]/(X^2 - X - 1)$. Dans $\mathbb{F}_{11}[X]$, on a $X^2 - X - 1 = (X-4)(X+3)$ et donc $(11) = \mathfrak{q}_1\mathfrak{q}_2$ dans $\mathcal{O}_K$ avec $\mathfrak{q}_1 = (11, \frac{1+\sqrt{5}}{2} + 3)$ et $\mathfrak{q}_2 = (11, \frac{1+\sqrt{5}}{2} - 4)$.

Exemple 1.2.13. Soit $K = \mathbb{Q}(\sqrt{17})$. On déduit du théorème 1.2.9 que tout élément de $\mathrm{Cl}(\mathcal{O}_K)$ contient un idéal de norme inférieure à $\frac{1}{2}\sqrt{17} < 3$. Si I est un idéal tel que $N(I) = 1$, alors $I = \mathcal{O}_K$ est principal. Si $N(I) = 2$, alors I divise l'idéal (2). Comme $\mathcal{O}_K \simeq \mathbb{Z}[X]/(X^2 - X - 4)$, on a $\mathcal{O}_K/(2) =\simeq \mathbb{F}_2[X]/(X(X-1))$ et donc $(2) = (2, \frac{1+\sqrt{17}}{2})(2, \frac{-1+\sqrt{17}}{2})$. Comme $2 = \frac{3+\sqrt{17}}{2}\frac{-3+\sqrt{17}}{2}$, on a $(2, \frac{1+\sqrt{17}}{2}) = (\frac{3+\sqrt{17}}{2})$ et $(2, \frac{-1+\sqrt{17}}{2}) = (\frac{-3+\sqrt{17}}{2})$. En particulier tous les idéaux de norme 2 sont principaux. Ainsi $\mathrm{Cl}(\mathcal{O}_K) = 1$ et l'anneau $\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ est principal.

1.2.5 Décomposition des idéaux dans une extension finie

Dans cette partie, on fixe A un anneau de Dedekind et K son corps des fractions. Soit L/K une extension finie et B la clôture intégrale de A dans L. D'après le théorème 1.2.4, l'anneau B est un anneau de Dedekind. On suppose de plus que B est un A-module de type fini.

Soit $\mathfrak{p}$ un idéal premier non nul de A. L'idéal $\mathfrak{p}B$ est un idéal non nul de B et peut donc être décomposé de façon unique comme produit d'idéaux maximaux de B :

$$\mathfrak{p}B = \prod_{\mathfrak{q}} \mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}.$$

Remarquons qu'un idéal maximal $\mathfrak{q}$ de B intervient dans cette décomposition si et seulement si $\mathfrak{p}B \subset \mathfrak{q}$, c'est-à-dire si et seulement si $\mathfrak{p} \subset \mathfrak{q}$. Dans ce cas on dit que l'idéal $\mathfrak{q}$ est un *diviseur* de $\mathfrak{p}$ ou encore que $\mathfrak{q}$ est *au-dessus* de $\mathfrak{p}$. On note cette relation $\mathfrak{q} \mid \mathfrak{p}$. L'entier $e_{\mathfrak{q}/\mathfrak{p}}$ est appelé *indice de ramification* de $\mathfrak{q}$ dans L/K. Comme B est un A-module de type fini, l'extension $k(\mathfrak{q})/k(\mathfrak{p})$ est finie. Son degré est noté $f_{\mathfrak{q}/\mathfrak{p}}$ est appelé *degré résiduel*. Si $e_{\mathfrak{q}/\mathfrak{p}} = 1$ et $k(\mathfrak{q})/k(\mathfrak{p})$ est une extension séparable, on dit que l'extension L/K est *non ramifiée* en $\mathfrak{q}$. Dans le cas contraire, elle est dite *ramifiée*.

Proposition 1.2.14. *Si $\mathfrak{p}$ est un idéal premier non nul de A, le nombre d'idéaux maximal de B divisant $\mathfrak{p}B$ est fini et on a l'égalité*

$$[L : K] = \sum_{\mathfrak{q}|\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} e_{\mathfrak{q}/\mathfrak{p}}.$$

Démonstration. Soient $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ les idéaux maximaux de B divisant $\mathfrak{p}$. Comme les idéaux $\mathfrak{q}_i$ sont distincts, on déduit du lemme A.4.4 un isomorphisme de A-algèbres

$$B/\mathfrak{p}B \xrightarrow{\sim} \prod_i B/\mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}.$$

Si I est un idéal non nul de B et $\mathfrak{q}$ un idéal maximal de B, il n'existe aucun idéal contenu strictement entre I et $I\mathfrak{q}$ de sorte que $I/I\mathfrak{q}$ est un $k(\mathfrak{q})$-espace vectoriel de dimension 1 et donc un $A/\mathfrak{p}$-espace vectoriel de dimension $f_{\mathfrak{q}/\mathfrak{p}}$. En considérant la suite décroissante d'idéaux de B :

$$B \supsetneq \mathfrak{q}_1 \supsetneq \mathfrak{q}_1^2 \supsetneq \cdots \supsetneq \mathfrak{q}_1^{e_{\mathfrak{q}_1/\mathfrak{p}}} \supsetneq \mathfrak{q}_1^{e_{\mathfrak{q}_1/\mathfrak{p}}}\mathfrak{q}_2 \supsetneq \cdots \supsetneq \mathfrak{q}_1^{e_{\mathfrak{q}_1/\mathfrak{p}}} \cdots \mathfrak{q}_r^{e_{\mathfrak{q}_r/\mathfrak{p}}} = \mathfrak{p}B,$$

et en utilisant le lemme 1.1.15, on voit que $B/B\mathfrak{p}$ est une extension successive de $e_{\mathfrak{q}_i/\mathfrak{p}}$ $A/\mathfrak{p}$-espaces vectoriels de dimension $f_{\mathfrak{q}_i/\mathfrak{p}}$ pour $1 \leqslant i \leqslant r$. Ceci implique que

$$\dim_{A/\mathfrak{p}}(B/B\mathfrak{p}) = \sum_{i=1}^{r} e_{\mathfrak{q}_i/\mathfrak{p}} f_{\mathfrak{q}_i/\mathfrak{p}}.$$

Pour conclure, il reste à vérifier que $B/B\mathfrak{p}$ est un $k(\mathfrak{p}) = A/\mathfrak{p}$-espace vectoriel de dimension $[L : K]$. Comme $A_\mathfrak{p}$ est un anneau principal, le $A_\mathfrak{p}$-module $B_\mathfrak{p} \simeq B \otimes_A A_\mathfrak{p}$ est libre de type fini. De plus $L \simeq B \otimes_A K \simeq B_\mathfrak{p} \otimes_{A_\mathfrak{p}} K$ de sorte que le rang de $B_\mathfrak{p}$ comme $A_\mathfrak{p}$-module est égal à $[L : K]$. Enfin, on a

$$B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} \simeq B \otimes_A (A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}) \simeq B \otimes_A (A/\mathfrak{p}) \simeq B/\mathfrak{p}B,$$

ce qui montre que $\dim_{k(\mathfrak{p})}(B/\mathfrak{p}B) = [L : K]$. □

1.2.6 Extensions galoisiennes

Soient A un anneau de Dedekind, K son corps de fractions et L une extension *galoisienne* de K. Soit B la clôture intégrale de A dans L. C'est un A-module de type fini d'après le théorème 1.2.4. Comme les conjugués d'un élément entier sur A sont entiers sur A, l'action du groupe de Galois $\mathrm{Gal}(L/K)$ sur L préserve le sous-anneau B. De plus, si $\mathfrak{q}$ est un idéal maximal de B et si $\sigma \in \mathrm{Gal}(L/K)$, on a

$$\sigma(\mathfrak{q} \cap A) = \mathfrak{q} \cap A = \sigma(\mathfrak{q}) \cap A$$

de sorte que $\sigma(\mathfrak{q})$ est un idéal maximal divisant $\mathfrak{p} \coloneqq \mathfrak{q} \cap A$. Ainsi, pour tout idéal maximal ideal $\mathfrak{p}$ de A, l'action du groupe $\mathrm{Gal}(L/K)$ préserve l'ensemble fini des idéaux maximaux de B divisant $\mathfrak{p}$.

Proposition 1.2.15. *Si $\mathfrak{p}$ est un idéal maximal de A, l'action de $\mathrm{Gal}(L/K)$ sur l'ensemble des diviseurs de $\mathfrak{p}$ est transitive.*

Démonstration. Soit $\mathfrak{q}$ un idéal maximal de B au-dessus de $\mathfrak{p}$. Supposons par l'absurde qu'il existe un idéal maximal $\mathfrak{q}'$ différent de tous les $\sigma(\mathfrak{q})$ pour $\sigma \in \mathrm{Gal}(L/K)$. D'après le lemme A.4.2, on a

$$B = \mathfrak{q}' + \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{q})$$

de sorte que l'on peut écrire $1 = x + y$ avec $x \in \mathfrak{q}'$ et $y \in \sigma(\mathfrak{q})$ pour tout $\sigma \in \mathrm{Gal}(L/K)$. On a donc $x \in \mathfrak{q}' \setminus \sigma(\mathfrak{q})$ pour tout σ. Soit $z \coloneqq N_{L/K}(x) = \prod_\sigma \sigma(x)$. Comme $x \in B$, on a $z \in \mathfrak{q} \cap A = \mathfrak{p}$ et comme $\mathfrak{p} = \mathfrak{q} \cap A$,

$$z = \prod_\sigma \sigma(x) \in \mathfrak{q}.$$

Ainsi il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(x) \in \mathfrak{q}$ et donc $x \in \sigma^{-1}(\mathfrak{q})$. C'est une contradiction. □

Corollaire 1.2.16. *Soit $\mathfrak{p}$ un idéal premier non nul de A et $B\mathfrak{p} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}$ la décomposition de $B\mathfrak{p}$ en produit d'idéaux maximaux. Les entiers $e_{\mathfrak{q}/\mathfrak{p}}$ et $f_{\mathfrak{q}/\mathfrak{p}}$ ne dépendent pas du choix de $\mathfrak{q} \mid \mathfrak{p}$ mais uniquement de $\mathfrak{p}$. On les note $e_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$. On a donc*

$$[L : K] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$$

où $g_{\mathfrak{p}}$ désigne le nombre d'idéaux maximaux de B divisant $\mathfrak{p}$.

Soit $\mathfrak{p}$ un idéal maximal de A et $\mathfrak{q}$ un idéal maximal de B divisant $\mathfrak{p}$. Le *groupe de décomposition* de $\mathfrak{q}$ est le stabilisateur $D_{\mathfrak{q}}$ de $\mathfrak{q}$ dans $\mathrm{Gal}(L/K)$. Un élément $\sigma \in \mathrm{Gal}(L/K)$ induit un iomorphisme de corps $\overline{\sigma} : B/\mathfrak{q} \xrightarrow{\sim} B/\sigma(\mathfrak{q})$. Si $\sigma \in D_{\mathfrak{q}}$, alors $\overline{\sigma}$ est un automorphisme de $k(\mathfrak{q})$ qui fixe les éléments de $k(\mathfrak{p})$.

Théorème 1.2.17. *On suppose de plus que $k(\mathfrak{q})/k(\mathfrak{p})$ est une extension séparable. Alors c'est une extension galoisienne et l'application $\sigma \mapsto \overline{\sigma}$ induit un morphisme surjectif de groupes de $D_{\mathfrak{q}}$ sur $\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$.*

Démonstration. Démontrons dans un premier temps que l'extension $k(\mathfrak{q})/k(\mathfrak{p})$ est galoisienne. Comme elle est déjà supposée séparable, il suffit de prouver qu'elle est normale. Soit $x \in k(\mathfrak{q})$. Il suffit de prouver que x est racine d'un polynôme de $k(\mathfrak{p})[X]$ scindé dans $k(\mathfrak{q})[X]$. Soit $\widetilde{x} \in B$ un élément relevant x et posons $P(X) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (X - \sigma(\widetilde{x}))$. Alors $P \in A[X]$ et, puisque P est scindé dans B, la réduction mod $\mathfrak{p}$ de P est scindée dans $B/\mathfrak{q} = k(\mathfrak{q})$ et annule x, ce que l'on recherchait. Notons au passage que cela prouve que tout conjugué de x sur $k(\mathfrak{p})$ est la réduction mod $\mathfrak{q}$ d'un conjugué de $\widetilde{x}$ sur K.

Démontrons à présent que le morphisme de groupes $D_{\mathfrak{q}} \to \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ est surjectif. Soit $x \in k(\mathfrak{q})$ un élément primitif de $k(\mathfrak{p})$ (qui existe puisque l'extension est séparable). Soit $\tau \in \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$. L'automorphisme τ est alors complètement déterminé par sa valeur sur x. Soit $\widetilde{x}$ un relevé de x à B. Le lemme A.4.2 montre que $B = \mathfrak{q} + \prod_{\sigma(\mathfrak{q}) \neq \mathfrak{q}} \sigma(\mathfrak{q})$ et donc que l'on peut écrire $\widetilde{x} = x_1 + x_2$ avec $x_1 \in \mathfrak{q}$ et $x_2 \in \prod_{\sigma(\mathfrak{q}) \neq \mathfrak{q}} \sigma(\mathfrak{q})$. Ainsi x_2 est un relevé de x tel que de plus $x_2 \in \sigma(\mathfrak{q})$ pour $\sigma(\mathfrak{q}) \neq \mathfrak{q}$. Comme remarqué ci-dessus, il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(x_2)$ relève $\tau(x)$ modulo $\mathfrak{q}$ de sorte que $\sigma(x_2) \notin \mathfrak{q}$, c'est-à-dire $x_2 \notin \sigma^{-1}(\mathfrak{q})$. On a donc $\sigma^{-1}(\mathfrak{q}) = \mathfrak{q}$, c'est-à-dire $\sigma \in D_{\mathfrak{q}}$. □

Le noyau $I_{\mathfrak{q}}$ du morphisme de groupes $D_{\mathfrak{q}} \to \mathrm{Aut}_{k(\mathfrak{p})}(k(\mathfrak{q}))$ est appelé le *sous-groupe d'inertie* en $\mathfrak{q}$. Supposons $\mathfrak{q}$ (et donc $\mathfrak{p}$) non nul. Comme $D_{\mathfrak{q}}$ est le stabilisateur de $\mathfrak{q}$ et que l'orbite de $\mathfrak{q}$ sous $\mathrm{Gal}(L/K)$ est de cardinal $g_{\mathfrak{p}}$, le cardinal du groupe $D_{\mathfrak{q}}$ vaut $e_{\mathfrak{p}} f_{\mathfrak{p}}$. Si l'extension $k(\mathfrak{q})/k(\mathfrak{p})$ est séparable, le cardinal du groupe $\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ est égal à $[k(\mathfrak{q}) : k(\mathfrak{p})] = f_{\mathfrak{p}}$ de sorte que le cardinal du sous-groupe d'inertie $I_{\mathfrak{q}}$ est $e_{\mathfrak{p}}$.

1.2.7 Différente et discriminant

Soit A un anneau de Dedekind et soit K son corps de fractions. On fixe L une extension finie séparable de K et on note B la clôture intégrale de A dans L. D'après le théorème 1.2.4, B est un A-module de type fini.

Rappelons que la proposition 1.2.6 implique que la forme K-bilinéaire $b_{L/K}$ est non dégénérée. Si M est un sous-A-module de L, on a défini $M^* := \{x \in L \mid \mathrm{Tr}_{L/K}(xM) \subset A\}$. Au cours de la démonstration du théorème 1.2.4, on a prouvé que B^* est un sous-B-module de L contenant B et qui est de type fini comme A-module. Il s'agit donc d'un idéal fractionnaire non nul de B dont l'inverse est appelé *différente* de B sur A et noté $\mathcal{D}_{B/A}$. Comme $B \subset \mathcal{D}_{B/A}^{-1}$, on a $\mathcal{D}_{B/A} \subset B^{-1} = B$ de sorte que $\mathcal{D}_{B/A}$ est un idéal non nul de B. De façon équivalente $\mathcal{D}_{B/A}$ est l'idéal annulateur du B-module B^*/B.

Rappelons que l'on a défini les groupes des idéaux fractionnaires $I(B)$ et $I(A)$ des anneaux de Dedekind B et A (voir section 1.1.2). On définit un morphisme de groupes $N_{L/K} : I(B) \to I(A)$ appelé *norme* en posant, pour tout idéal maximal $\mathfrak{q}$ de B, $N_{L/K}(\mathfrak{q}) := \mathfrak{p}^{f_\mathfrak{q}}$ où $\mathfrak{p} := \mathfrak{q} \cap A$. Ce morphisme est bien défini car $I(B)$ est un groupe abélien libre de base formée par les idéaux maximaux de B.

Remarque 1.2.18. Si $A = \mathbb{Z}$ et $K = \mathbb{Q}$, alors pour tout idéal non nul I de B, l'anneau quotient B/I est fini et $N_{K/\mathbb{Q}}(I) = (N(I)) = \mathbb{Z}N(I)$ où $N(I) = |B/I|$.

Proposition 1.2.19. *Si $I = (b)$ est un idéal fractionnaire principal de B, alors $N_{L/K}(I) = (N_{L/K}(b))$ est l'idéal fractionnaire principal de A engendré par $N_{L/K}(b)$.*

Démonstration. Il suffit de vérifier le résultat après localisation en idéal premier non nul de A. On peut donc supposer que l'anneau A est principal. On se ramène également facilement au cas où $b \in B$ est non nul. Soit $(b) = \prod_{i=1}^r \mathfrak{q}_i$ la décomposition de (b) en produit d'idéaux maximaux de B. Tout idéal non nul I de B est un réseau de A de rang n et de plus, pour $\mathfrak{q}$ idéal maximal de B, on a $[I : I\mathfrak{q}] = [B : \mathfrak{q}]$ (voir la section A.6 pour la notion de réseau). Posant $\mathfrak{p} = \mathfrak{q} \cap A$, comme $B/\mathfrak{q}$ est un $A/\mathfrak{p}$-espace vectoriel de dimension $f_{\mathfrak{q}/\mathfrak{p}}$, on en déduit que $[B : \mathfrak{q}] = (\pi^{f_{\mathfrak{q}/\mathfrak{p}}}) = N_{L/K}(\mathfrak{q})$. On déduit de la proposition A.6.1 que

$$[A : (b)] = \prod_{i=1}^{r} N_{L/K}(\mathfrak{q}_i) = N_{L/K}((b)).$$

Par ailleurs, le théorème des diviseurs élémentaires montre que $[A : (b)]$ est l'idéal de A engendré par le déterminant de l'application A-linéaire $m_b : B \to B$. On en déduit que $[A : (b)] = (N_{L/K}(b))$, ce qui achève la preuve. □

On définit l'*idéal discriminant* $\Delta_{B/A}$ de B sur A en posant $\Delta_{B/A} \coloneqq N_{L/K}(\mathcal{D}_{B/A})$. Il s'agit d'un idéal non nul de A.

Lemme 1.2.20. *Soit S une partie multiplicative de A. Alors $\mathcal{D}_{B/A}B_S = \mathcal{D}_{B_S/A_S}$ et $\Delta_{B/A}A_S = \Delta_{B_S/A_S}$. En particulier si $\mathfrak{p}$ est un idéal premier de A, on a $\mathcal{D}_{B/A}B_\mathfrak{p} = \mathcal{D}_{B_\mathfrak{p}/A_\mathfrak{p}}$ et $\Delta_{B/A}A_\mathfrak{p} = \Delta_{B\mathfrak{p}/A_\mathfrak{p}}$.*

Démonstration. Il suffit de prouver la première égalité. En effet la seconde provient de la première et de l'égalité $N_{L/K}(I)_S = N_{L/K}(I_S)$ pour tout idéal I de B. Pour prouver la première égalité, il suffit de vérifier que $(B_S)^* = (B^*)_S$, ce qui suit du caractère K-linéaire de $\mathrm{Tr}_{L/K}$. □

Proposition 1.2.21. *L'idéal $\Delta_{B/A}$ de A est l'idéal engendré par les éléments $\Delta_{L/K}(\underline{\alpha})$ où $\underline{\alpha}$ varie parmi les K-bases de L dont les éléments sont contenus dans B.*

Démonstration. Soit I l'idéal de A engendré par les éléments $\Delta(\underline{\alpha})$) où $\underline{\alpha}$ est une K-base de L contenue dans B. Pour démontrer que $\Delta_{B/A} = I$, il suffit (lemme A.2.1) de démontrer que $\Delta_{B/A,\mathfrak{p}} = I_\mathfrak{p}$ pour tout idéal premier non nul $\mathfrak{p}$ de A. Comme $A_\mathfrak{p}$ est principal, l'idéal $I_\mathfrak{p}$ est principal. On en déduit que $I_\mathfrak{p} = (\Delta(\underline{\alpha}))$ où $\underline{\alpha}$ est une K-base de L formée d'éléments de $B_\mathfrak{p}$. Comme $\Delta_{B/A,\mathfrak{p}} = \Delta_{B_\mathfrak{p}/A_\mathfrak{p}}$ (lemme 1.2.20), il suffit de démontrer le résultat lorsque l'anneau A est principal, et même un anneau de valuation discrète.

Supposons donc que A est un anneau de valuation discrète d'idéal maximal $\mathfrak{p} = (\pi)$. Alors le A-module B est libre de type fini et il existe une K-base de L qui est également une A-base of B. La formule de changement de base pour les discriminants (1.1) montre que I est l'idéal principal engendré par $\Delta(\underline{\alpha})$ pour tout A-base $\underline{\alpha}$ de B. On a de plus une inclusion de A-modules libres de même rang $B \subset B^*$ de sorte qu'il existe une A-basis $(\alpha_1, \dots, \alpha_n)$ de B^* et des éléments non nuls $d_1 \mid d_2 \mid \cdots \mid d_n$ de A tels que $(d_1e_1, \dots, d_ne_n)$ est une A-base de B. Soit maintenant $(\alpha_1^*, \dots, \alpha_n^*)$ la base duale de $(\alpha_1, \dots, \alpha_n)$ pour la forme $b_{L/K}$. C'est une A-base de B. Soit P la matrice de passage de la base $(d_1\alpha_1, \dots, d_n\alpha_n)$ à la base $(\alpha_1^*, \dots, \alpha_n^*)$. On a alors $P \in \mathrm{GL}_n(A)$ et

$$\begin{aligned}\Delta(\alpha_1^*, \dots, \alpha_n^*) &= \det(b_{L/K}(\alpha_i^*, \alpha_j^*))_{1\leqslant i,j\leqslant n} = \det(P)\det(b_{L/K}(\alpha_i^*, d_j\alpha_j))_{1\leqslant i,j\leqslant n} \\ &= \det(P)\prod_{j=1}^n a_j \det(b_{L/K}(\alpha_i^*, \alpha_j))_{1\leqslant i,j\leqslant n} = \det(P)\prod_{j=1}^n a_j.\end{aligned}$$

On en déduit que $I = (\prod_j a_j)$. De plus l'égalité $B = B^*\mathcal{D}_{B/A}$ et le lemme 1.1.15 montrent que B^*/B possède une filtration de Jordan-Hölder par des sous-B-modules dont les sous-quotients successifs sont isomorphes aux $B/\mathfrak{q}_i$ où $\mathcal{D}_{B/A} =$

$\mathfrak{q}_1 \cdots \mathfrak{q}_r$ (les $\mathfrak{q}_i$ ne sont pas nécessairement distincts ici). Comme $\mathfrak{q}_i \cap A = (\pi)$, les diviseurs élémentaires du A-module $B/\mathfrak{q}_i$ sont les $\pi, \ldots, \pi$ (comptés $f_{\mathfrak{q}_i/(\pi)}$ fois). Cela prouve que le produit des diviseurs élémentaires du A-module B^*/B est $\pi^{\sum_i f_{\mathfrak{q}_i/(\pi)}}$ qui est un générateur de l'idéal $N_{L/K}(\mathcal{D}_{B/A})$. Cela implique finalement que

$$\Delta_{B/A} = (\prod_{j=1}^{d} a_j) = I. \qquad \square$$

Théorème 1.2.22. *Soit $\mathfrak{q}$ un idéal premier non nul de B. Alors $\mathfrak{q}$ est ramifié dans L/K si et seulement si $\mathfrak{q}$ est un diviseur de $\mathcal{D}_{B/A}$.*

Démonstration. Posons $\mathfrak{p} := \mathfrak{q} \cap A$. Le B-module B^*/B est de type fini et a pour annulateur l'idéal $\mathcal{D}_{B/A}$. Ainsi un idéal maximal $\mathfrak{q}$ vérifie $\mathcal{D}_{B/A} \subset \mathfrak{q}$ si et seulement si $(B^*/B)_\mathfrak{q} \neq 0$. Comme $(B^*/B)_\mathfrak{q}$ est un $B_\mathfrak{q}$-module de type fini, le lemme A.1.2 implique que $\mathcal{D}_{B/A} \subset \mathfrak{q}$ si et seulement si $(B^*/B)_\mathfrak{q} \otimes_{B_\mathfrak{q}} B_\mathfrak{q}/\mathfrak{p}B_\mathfrak{q} \neq 0$ autrement dit $((B^*/B) \otimes_B B/\mathfrak{p})_\mathfrak{q} \neq 0$. Par exactitude à droite du foncteur $\otimes_B B/\mathfrak{p}$ et exactitude du foncteur de localisation, on en déduit que $\mathcal{D}_{B/A} \subset \mathfrak{q}$ si et seulement si l'inclusion de B dans B^* induit un morphisme de $B_\mathfrak{q}$-module $(B/\mathfrak{p}B)_\mathfrak{q} \to (B^*/\mathfrak{p}B^*)_\mathfrak{q}$ de conoyau non nul. Notons f le morphisme de B^* dans $\mathrm{Hom}_A(B, A)$ définit par $f(x) = \mathrm{Tr}_{L/K}(x-)$. Comme la forme $b_{L/K}$ est non dégnérée (proposition 1.2.2), le morphisme f est un isomorphisme de B-module par définition de B^*. De plus, on déduit de la remarque 1.2.5 que B est un A-module projectif de type fini, on a donc un isomorphisme naturel de B-modules $\mathrm{Hom}_A(B, A) \otimes_A k(\mathfrak{p}) \simeq \mathrm{Hom}_A(B, k(\mathfrak{p}))$, et donc un isomorphisme de $B/\mathfrak{p}$-modules $\overline{f} : B^* \otimes_A k(\mathfrak{p}) \simeq \mathrm{Hom}_{k(\mathfrak{p})}(B/\mathfrak{p}, k(\mathfrak{p}))$. On vérifie que le morphisme $B/\mathfrak{p} \to \mathrm{Hom}_{k(\mathfrak{p})}(B/\mathfrak{p}, k(\mathfrak{p}))$ déduit de la composition de $B/\mathfrak{p} \to B^*/\mathfrak{p}$ et de $\overline{f}$ est donné explicitement par $x \mapsto \mathrm{Tr}_{(B/\mathfrak{p})/k(\mathfrak{p})}(x-)$ (voir la section A.5 pour la définition de Tr dans ce contexte). Comme $B/\mathfrak{p}$ est une $k(\mathfrak{p})$-algèbre de dimension finie, la $k(\mathfrak{p})$-algèbre $(B/\mathfrak{p})_\mathfrak{q}$ (localisé en $\mathfrak{q}$) est un facteur direct de $B/\mathfrak{p}$ (voir proposition A.5.1) et le morphisme naturel $B^*/{\to}(B^*/\mathfrak{p})_\mathfrak{q}$ correspond à la projection sur le facteur direct $\mathrm{Hom}_{k(\mathfrak{p})}((B/\mathfrak{p})_\mathfrak{q}, k(\mathfrak{p}))$ de $\mathrm{Hom}_{k(\mathfrak{p})}((B/\mathfrak{p}), k(\mathfrak{p}))$ et le diagramme suivant est commutatif

$$\begin{array}{ccc} (B/\mathfrak{p})_\mathfrak{q} & \longrightarrow & (B^*/\mathfrak{p})_\mathfrak{q} \\ & \searrow^{x \mapsto \mathrm{Tr}_{(B/\mathfrak{p})_\mathfrak{q}/k(\mathfrak{p})}(x-)} & \downarrow \overline{f}_\mathfrak{q} \\ & & \mathrm{Hom}_{k(\mathfrak{p})}((B/\mathfrak{p})_\mathfrak{q}, k(\mathfrak{p})). \end{array}$$

On en déduit que $\mathcal{D}_{B/A} \subset \mathfrak{q}$ si et seulement si le morphisme $x \mapsto \mathrm{Tr}_{(B/\mathfrak{p})_\mathfrak{q}/k(\mathfrak{p})}(x-)$ n'est pas surjectif, ou de façon équivalente n'est pas bijectif. L'idéal $\mathfrak{p}B$ se décompose en produit d'idéaux maximaux $\mathfrak{p}B = \prod_\mathfrak{q} \mathfrak{q}^{v_\mathfrak{q}(\mathfrak{p}B)}$. On déduit alors du lemme

A.4.4 la décomposition

$$B/\mathfrak{p}B \simeq \prod_{\mathfrak{q}} B/\mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{p}B)}$$

et donc l'isomorphisme $(B/\mathfrak{p})_{\mathfrak{q}} \simeq B/\mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{p}B)}$. Au final on déduit de la proposition A.5.2 que $\mathcal{D}_{B/A} \subset \mathfrak{q}$ si et seulement si $v_{\mathfrak{q}}(\mathfrak{p}B) = 1$ et $k(\mathfrak{q}) = B/\mathfrak{q}$ est une extension séparable de $k(\mathfrak{p})$, c'est-à-dire $\mathfrak{q}$ non ramifié dans L/K. □

Corollaire 1.2.23. *1) Si $\mathfrak{q}$ est un idéal premier non nul de B, alors L/K est ramifiée en $\mathfrak{q}$ si et seulement si $\mathfrak{q} \mid \mathcal{D}_{B/A}$.*

2) Si $\mathfrak{p}$ est un idéal premier non nul de A, alors L/K est ramifiée en $\mathfrak{p}$ si et seulement si $\mathfrak{p} \mid \Delta_{B/A}$.

3) Le nombre d'idéaux premiers non nuls de A qui sont ramifiés dans L est fini.

Remarque 1.2.24. On peut montrer que $\mathcal{D}_{B/A}$ est l'annulateur du B-module $\Omega^1_{B/A}$.

Supposons que M/L est une extension finie séparable et soit C la clôture intégrale de B dans M, il s'agit également de la clôture intégrale de A dans M.

Proposition 1.2.25. *1) Si I est un idéal non nul de C, on a $N_{C/A}(I) = N_{B/A}(N_{C/B}(I))$.*

2) On a $\mathcal{D}_{C/A} = \mathcal{D}_{C/B}\mathcal{D}_{B/A}$.

3) On a $\Delta_{C/A} = N_{B/A}(\Delta_{C/B})\Delta_{B/A}^{[M:L]}$.

Démonstration. Le point 1) est immédiat à partir de la définition de la norme. Démontrons le point 2). Le point 3) s'en déduit immédiatement. Posons $C^* = \{x \in M \mid \mathrm{Tr}_{M/K}(xC) \in A\}$, $C' = \{x \in M \mid \mathrm{Tr}_{M/L}(xC) \in B\}$ et $B^* = \{x \in L \mid \mathrm{Tr}_{L/K}(xB) \in A\}$. Soit $x \in M$. On a $\mathrm{Tr}_{M/K}(x) \in A$ si et seulement si $\mathrm{Tr}_{M/L}(x) \in B^* = \mathcal{D}_{B/A}^{-1}$. Ainsi $\mathrm{Tr}_{M/L}(x) \in A$ si et seulement si $\mathrm{Tr}_{M/L}(x\mathcal{D}_{B/A}) \subset B$, c'est-à-dire si et seulement si $x\mathcal{D}_{B/A} \subset C'$. D'où $C' = C^*\mathcal{D}_{B/A}$, c'est-à-dire $\mathcal{D}_{C/B}^{-1} = \mathcal{D}_{C/A}^{-1}\mathcal{D}_{B/A}$. On en déduit le résultat. □

Exemple 1.2.26. Soit $n \geqslant 1$ un entier et posons $\zeta = e^{\frac{2\pi i}{n}}$ (tout ce qui suit resterait valable avec une autre racine primitive n-ième de l'unité). Posons $K = \mathbb{Q}(\zeta_n)$. Soit p un nombre premier ne divisant pas n. Comme ζ_n est annulé par $X^n - 1$, on a $\zeta_n \in \mathcal{O}_K$ et, si Φ_n désigne le polynôme minimal de ζ_n sur $/Q$, on a $\mathbb{Z}[\zeta_n] \subset \mathcal{O}_K$ et $\mathbb{Z}[\zeta_n] \simeq \mathbb{Z}[X]/(\Phi_n)$ (en fait on a $\mathbb{Z}[\zeta_n] = \mathcal{O}_K$ et $\deg(\Phi_n) = \varphi(n)$, voir TD). Posons $d_n = \deg(\Phi_n)$. Alors la famille $(A, \zeta_n, \ldots, \zeta_n^{d_n-1})$ est une $\mathbb{Z}$-base de $\zeta[\zeta_n]$ et

$$\Delta_{\mathcal{O}_K/\mathbb{Z}} \mid \Delta_{K/\mathbb{Q}}(1, \zeta_n, \ldots, \zeta_n^{d_n-1}) = \mathrm{Disc}(\Phi_n).$$

Notons $\overline{\Phi_n}$ la réduction de Φ_n modulo p. Comme $\Phi_n \mid X^n - 1$ et que le polynôme $X^n - 1$ est séparable dans $\mathbb{F}_p[X]$ (car $(X^n - 1, nX^{n-1}) = 1$ dans $\mathbb{F}_p[X]$), on a $\mathrm{Disc}(\overline{\Phi_n}) \in \mathbb{F}_p^\times$. En particulier, $p \nmid \Delta_{\mathcal{O}_K/\mathbb{Z}}$. Ceci implique que p est non ramifié dans $K/\mathbb{Q}$. En utilisant la proposition 1.2.6, on montre au passage que $\mathbb{Z}[\zeta_n]_{(p)} = \mathcal{O}_{K,p}$ si $p \nmid n$. On peut montrer que si $p \mid n$, alors p est effectivement ramifié dans $K/\mathbb{Q}$ (voir TD).

1.3 Anneaux de Dedekind résiduellement finis

1.3.1 Éléments de Frobenius

Soit A un anneau de Dedekind ring de corps de fractions K. Soit L une extension galoisienne finie de K et soit B la clôture intégrale de A dans L. Soit $\mathfrak{q}$ un idéal maximal B et posons $\mathfrak{p} \coloneqq \mathfrak{q} \cap A$, un idéal maximal de A. Supposons que le corps résiduel $k(\mathfrak{p})$ est un corps fini de cardinal q. Le corps résiduel $k(\mathfrak{q})$ est alors finie et, puisque $k(\mathfrak{p})$ est en particulier un corps parfait, l'extension $k(\mathfrak{q})/k(\mathfrak{p})$ est alors séparable. Si l'on suppose de plus que l'idéal $\mathfrak{q}$ est non ramifié dans L/K, alors le morphisme $\sigma \mapsto \overline{\sigma}$ de $D_\mathfrak{q}$ vers $\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ est un isomorphisme de groupes.

Le groupe de Galois $\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ est cyclique de cardinal $f_{\mathfrak{q}/\mathfrak{p}}$ et engendré par l'endomorphisme de Frobenius endomorphism $x \mapsto x^q$. On note $(\mathfrak{q}, L/K) \in D_\mathfrak{q} \subset \mathrm{Gal}(L/K)$ l'image inverse de l'endomorphisme de Frobenius dans $D_\mathfrak{q}$. Cet élément est appelé *élément de Frobenius* en $\mathfrak{q}$. Il peut être caractérisé comme l'unique élément σ de $\mathrm{Gal}(L/K)$ tel que

— $\sigma(\mathfrak{q}) = \mathfrak{q}$;

— $\forall b \in B, \quad \sigma(b) \equiv b^q \bmod \mathfrak{q}$.

De plus l'élément $(\mathfrak{q}, L/K) \in \mathrm{Gal}(L/K)$ est d'ordre exactement $f_{\mathfrak{q}/\mathfrak{p}}$. En particulier, $f_{\mathfrak{q}/\mathfrak{p}} = 1$ et si et seulement si $(\mathfrak{q}, L/K) = 1$.

Remarque 1.3.1. La construction de l'élément $(\mathfrak{q}, L/K)$ est compatible à la localisation : si S est une partie multiplicative disjointe de $\mathfrak{p}$, on a $(\mathfrak{q}_S, L/K) = (\mathfrak{q}, L/K)$ in $\mathrm{Gal}(L/K)$.

Remarque 1.3.2. Si $\sigma \in \mathrm{Gal}(L/K)$, alors $(\sigma(\mathfrak{q}), L/K) = \sigma(\mathfrak{q}, L/K)\sigma^{-1}$. En particulier, si l'extension L/K est abélienne, c'est-à-dire $\mathrm{Gal}(L/K)$ est abélien, alors $(\mathfrak{q}, L/K)$ depend uniquement de $\mathfrak{p}$. On peut donc le noter $(\mathfrak{p}, L/K)$.

Proposition 1.3.3. *Soit $M \subset L$ une sous-extension de L/K (c'est-à-dire $K \subset M$). Soit $C = B \cap M$ la clôture intégrale de A dans M et soit $\mathfrak{r} \coloneqq \mathfrak{q} \cap C$. Soit $D'_\mathfrak{q}$ le groupe de décomposition de $\mathfrak{q}$ dans L/M.*

1) L'idéal maximal $\mathfrak{q}$ *est non ramifié dans* L/M*. De plus* $D'_{\mathfrak{q}} = D_{\mathfrak{q}} \cap \mathrm{Gal}(L/M)$ *et* $(\mathfrak{q}, L/M) = (\mathfrak{q}, L/K)^{f_{\mathfrak{r}/\mathfrak{p}}}$*.*

2) Si de plus M/K *est galoisienne, alors l'image de* $(\mathfrak{q}, L/K)$ *dans* $\mathrm{Gal}(M/K)$ *est* $(\mathfrak{r}, M/K)$*.*

Démonstration. On a $1 = e_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{q}/\mathfrak{r}} e_{\mathfrak{r}/\mathfrak{p}}$ de sorte que $e_{\mathfrak{q}/\mathfrak{r}} = 1$ et $\mathfrak{q}$ est non ramifié dans L/M. Il est clair que $D'_{\mathfrak{q}} = D_{\mathfrak{q}} \cap \mathrm{Gal}(L/M)$. Comme $k(\mathfrak{p})$ est un corps fini, les extensions $k(\mathfrak{q})/k(\mathfrak{p})$ et $k(\mathfrak{r})/k(\mathfrak{p})$ sont galoisiennes. Soit $H \subset D_{\mathfrak{q}}$ le noyau de l'application de restriction $D_{\mathfrak{q}} \simeq \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \twoheadrightarrow \mathrm{Gal}(k(\mathfrak{r})/k(\mathfrak{p}))$. Autrement dit on a

$$H = \{\sigma \in D_{\mathfrak{q}} \mid \sigma(x + \mathfrak{q}) = x + \mathfrak{q} \ \forall x \in C\}.$$

On a clairement $D'_{\mathfrak{q}} \subset H$. Par ailleurs le cardinal de $D'_{\mathfrak{q}}$ est égal à $f_{\mathfrak{q}/\mathfrak{r}}$ et le cardinal de H est égal au cardinal de $\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{r}))$, c'est-à-dire $f_{\mathfrak{q}/\mathfrak{r}}$. On en déduit que $H = D'_{\mathfrak{q}}$. Ainsi l'élément $(\mathfrak{q}, L/K)^{f_{\mathfrak{r}/\mathfrak{p}}}$ est dans $D'_{\mathfrak{q}}$ et il coïncide avec l'endomorphisme $x \mapsto x^{q^{f_{\mathfrak{r}/\mathfrak{p}}}}$ modulo $\mathfrak{q}$. Comme $q^{f_{\mathfrak{r}/\mathfrak{p}}} = \mathrm{Card}(k(\mathfrak{r}))$, on a bien $(\mathfrak{q}, L/M) = (\mathfrak{q}, L/M)^{f_{\mathfrak{r}/\mathfrak{p}}}$. Ceci prouve le point 1).

Le point 2) est laissé en exercice. □

Exemple 1.3.4. Soit $n \geqslant 1$ un entier et soit $K = \mathbb{Q}(\zeta_n)$. L'extension $K/\mathbb{Q}$ est galoisienne car les conjugués de ζ_n sur $\mathbb{Q}$ sont des racines de $X^n - 1$ et appartiennent donc à K. Soit $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Alors il existe un élément $c(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\sigma(\zeta_n) = \zeta_n^{c(\sigma)}$. De plus, l'application $\sigma \mapsto c(\sigma)$ est un morphismes de groupes de $\mathrm{Gal}(K/\mathbb{Q})$ vers $(\mathbb{Z}/n\mathbb{Z})^\times$. Soit p un nombre premier ne divisant pas n. Alors, comme vu dans l'exemple 1.2.26, le nombre premier p est non ramifié dans $K/\mathbb{Q}$. Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$ divisant p et soit $\overline{\zeta_n}$ l'image de ζ_n dans $k(\mathfrak{p})$. Posons $c = c((\mathfrak{p}, K/\mathbb{Q}))$. Par définition de l'élément de Frobenius $(\mathfrak{p}, K/\mathbb{Q})$, on a $\overline{\zeta_n}^c = \overline{\zeta_n}^p$. En réduisant la décomposition $X^n - 1 = \prod_{i=0}^{n-1}(X - \zeta_n^i)$ dans $k(\mathfrak{p})$, on voit que les éléments $\overline{\zeta_n}^i$, pour $0 \leqslant i \leqslant n-1$ sont les racines de $X^n - 1$ dans $k(\mathfrak{p})$. Comme $k(\mathfrak{p})$ est de caractéristique p et que $X^n - 1$ est séparable dans $\mathbb{F}_p[X]$, on en conclut que ces éléments sont distincts. Ainsi $i \equiv p \bmod n$ et on en déduit que $c((\mathfrak{q}, K/\mathbb{Q})) = p$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Cet exemple est en fait fondamental et le résultat mérite d'être énoncé sous forme de théorème.

Théorème 1.3.5. *Soit* $n \geqslant 1$ *un entier et soit* $K = \mathbb{Q}(\zeta_n)$*. L'extension* $K/\mathbb{Q}$ *est galoisienne, abélienne de degré* $\varphi(n)$*. De plus le morphisme de groupes* $c : \mathrm{Gal}(K/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ *défini dans l'exemple 1.3.4 est un isomorphisme. Si* p *est un nombre premier ne divisant pas* n*,* p *est non ramifié dans* $K/\mathbb{Q}$ *et, pour tout idéal maximal de* $\mathcal{O}_K$ *au-dessus de* p*, on a* $c((p, K/\mathbb{Q})) = p$*.*

Démonstration. On a déjà vu au cours de l'exemple 1.3.4 que si $p \nmid n$, alors p est non ramifié dans $K/\mathbb{Q}$ et que $c((\mathfrak{p}, K/\mathbb{Q})) = p$ pour tout idéal maximal $\mathfrak{p}$ au-dessus de p. Ainsi l'image de c contient es classes de tous les nombres premiers ne divisant pas n. Comme tout élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ est un produit de telles classes, on en déduit que c est un morphisme surjectif. Comme par ailleurs, tout conjugué de ζ_n est une racine primitive n-ième de l'unité et que ces racines sont au nombre de $\varphi(n)$. On a $[K : \mathbb{Q}] = \mathrm{Card}(\mathrm{Gal}(/\mathbb{Q})) \leqslant \varphi(n) = \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^\times)$. On en conclut que c est bijective, que $[K : \mathbb{Q}] = \varphi(n)$ et que $K/\mathbb{Q}$ est une extension abélienne. □

Exemple 1.3.6. Soit $K = \mathbb{Q}(\zeta_n)$ avec $n \geqslant 1$. Soit p un nombre premier ne divisant pas n. Alors f_p est l'ordre de $(p, K/\mathbb{Q})$ dans $\mathrm{Gal}(K/\mathbb{Q})$. On en conclut que f_p est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Ainsi p est complètement décomposé dans $\mathcal{O}_K$, c'est-à-dire que $p\mathcal{O}_K$ se décompose en un produit de $\varphi(n)$ idéaux maximaux si et seulement si $p \equiv 1 \bmod n$.

1.3.2 La loi de réciprocité quadratique

Soit p un nombre premier impair. D'après l'exemple 1.2.26, l'extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ est non ramifiée hors de p. De plus, d'après le théorème 1.3.5, cette extension est cyclique de degré $p - 1$. On en conclut qu'il existe une unique sous-extension $K_p \subset \mathbb{Q}(\zeta_p)$ de degré 2 sur $\mathbb{Q}$. Ainsi $K_p = \mathbb{Q}(\sqrt{d})$ pour un entier $d \in \mathbb{Z} \smallsetminus \{0, 1\}$ sans diviseur carré et

$$\Delta_{K_p/\mathbb{Q}} = \begin{cases} d & \text{si } d \equiv 1 \bmod 4 \\ 4d & \text{sinon.} \end{cases}$$

On déduit du corollaire 1.2.23 que $d = \pm p$ et $d \equiv 1 \bmod 4$, c'est-à-dire $d = (-1)^{\frac{p-1}{2}} p$. Notons p^* cet entier. Soit q un nombre premier différent de p. D'après la proposition 1.3.3, l'élément de Frobenius $(q, K_p/\mathbb{Q})$ est l'image de $(q, \mathbb{Q}(\zeta_p)/\mathbb{Q})$ dans $\mathrm{Gal}(K_p/\mathbb{Q})$. Ainsi $(q, K_p/\mathbb{Q}) = 1$ si et seulement si $(q, \mathbb{Q}(\zeta_p)/\mathbb{Q})$ est dans le noyau de $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathrm{Gal}(K_p/\mathbb{Q})$. Le théorème 1.3.5 montre que ceci est encoyre équivalent à ce que q appartienne à l'unique sous-groupe d'indice 2 de $(\mathbb{Z}/p\mathbb{Z})^\times$, c'est-à-dire q est un résidu quadratique modulo p. Par ailleurs $(q, K_p/\mathbb{Q}) = 1$ si et seulement si q est décomposé dans $K_p/\mathbb{Q}$. On a donc prouvé que q est un résidu quadratique modulo p si et seulement si q est décomposé dans $K_p/\mathbb{Q}$.

Par ailleurs $\mathcal{O}_{K_p} = \mathbb{Z}[\frac{1+\sqrt{p^*}}{2}] \simeq \mathbb{Z}[X]/(X^2 - X + \frac{1-p^*}{4})$. On déduit donc de la proposition 1.2.11 que q est décomposé dans $K_p/\mathbb{Q}$ si et seulement si le polynôme $X^2 - X + \frac{1-p^*}{4}$ a une racine dans $\mathbb{F}_q$. Si $q \neq 2$, ce polynôme a une racine si et seulement si son discriminant est un carré, c'est-à-dire si et seulement si p^* est

un carré dans $\mathbb{F}_q$. On a donc prouvé que $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. Il découle des propriétés du symbole de Legendre que $\left(\frac{p^*}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$. Si $q = 2$, le polynôme $X^2 - X + \frac{1-p^*}{4}$ est séparable et est décomposé dans $\mathbb{F}_2$ si et seulement si il a pour racines 0 et 1, c'est-à-dire si et seulement si $p^* \equiv 1 \bmod 8$, c'est-à-dire si et seulement si $p \equiv \pm 1 \bmod 8$. On a donc prouvé la loi de réciprocité quadratique.

Théorème 1.3.7 (Loi de réciprocité quadratique)**.** *Soient p et q deux nombre premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Si p est un nombre premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.*

Chapitre 2

Corps globaux et corps locaux

Un *corps global* est un corps qui est une extension finie de $\mathbb{Q}$ ou une extension finie du corps des fractions rationnelles $\mathbb{F}_p(t)$ à coefficients dans le corps fini $\mathbb{F}_q$.

Lors que K est une extension finie de $\mathbb{Q}$, on dit que K est un *corps de nombres*. L'ensemble des éléments de K qui sont entiers sur $\mathbb{Z}$ forme alors un sous-anneau $\mathcal{O}_K$ appelé *anneau d'entiers* de K. Il s'agit d'un *anneau de Dedekind* c'est-à-dire qu'il est noethérien, intégralement clos et de dimension 1 (ou de façon équivalente, tous ses idéaux premiers non nuls sont maximaux). Le corps K est alors le corps des fractions de $\mathcal{O}_K$.

Lorsque K est une extension finie de $\mathbb{F}_q(t)$, on dit que K est un *corps de fonctions*. L'ensemble des éléments de K qui sont entiers sur $\mathbb{F}_q[t]$ est également un anneau de Dedekind dont K est le corps des fractions. Cependant, il faut noter une différence avec le cas des corps de nombres : cet anneau dépend du choix de l'extension $K/\mathbb{F}_q(t)$. En effet, K peut être extension finie de $\mathbb{F}_q(t)$ de plusieurs façons différentes, il suffit de choisir un élément transcendant (sur $\mathbb{F}_p$) de K. Cet anneau d'entiers dépend alors du choix de l'extension $K/\mathbb{F}_q(t)$. La théorie des places va nous permettre de nous affranchir de ce choix dans l'étude des propriétés arithmétiques de K.

Dans tous les cas, les corps globaux ont la propriété commune d'être des corps de fractions d'anneaux de Dedekind dont les corps résiduels des idéaux maximaux sont finis.

2.1 Valeurs absolues

2.1.1 Places d'un corps

Définition 2.1.1. *Une* valeur absolue *d'un corps K est une application $|\cdot| : K \to \mathbb{R}_{\geqslant 0}$ telle que*

— $\forall x \in K, \quad |x| = 0 \Leftrightarrow x = 0$;

— $\forall (x, y) \in K^2, \quad |xy| = |x||y|$;

— $\forall (x, y) \in K^2, \quad |x + y| \leqslant |x| + |y|$.

Une valeur absolue $|\cdot|$ est dite ultramétrique *(ou encore non archimédienne) si elle vérifie la propriété plus forte*

$$\forall (x, y) \in K^2, \quad |x + y| \leqslant \max(|x|, |y|).$$

Un corps valué $(K, |\cdot|)$ *est la donnée d'un corps K et d'une valeur absolue $|\cdot|$ sur K.*

Exemple 2.1.2. a) La *valeur absolue triviale* est la valeur absolue définie par $|x| = 1 \Leftrightarrow x \neq 0$.

b) Si $K = \mathbb{Q}$, la valeur absolue usuelle est une valeur absolue :

$$|x| = \max\{x, -x\}.$$

Cette valeur absolue n'est pas ultramétrique, on l'appelle aussi valeur absolue *archimédienne* ou encore *réelle*.

c) Si p est un nombre premier et $x \in \mathbb{Q}$, on pose

$$|x|_p = p^{-v_p(x)}$$

où $v_p(x)$ est la valaution p-adique de x, avec la convention $|0|_p = 0$. Il s'agit d'une valeur absolue ultramétrique appelée *valeur absolue p-adique*.

d) Plus généralement soit A un anneau de Dedekind, $\mathfrak{p}$ un idéal premier non nul de A et K le corps des fractions de A. L'application $x \mapsto e^{-v_{\mathfrak{p}}(x)}$ est une valeur absolue sur K (voir exercice 1.1.2).

Si K est un corps et $|\cdot|$ une valeur absolue sur K, la fonction $(x, y) \mapsto |x - y|$ définit une distance sur K.

Lemme 2.1.3. *Muni de la topologie définie par une valeur absolue, un corps K est un corps topologique (voir section B.4). De plus la topologie est discrète si et seulement si la norme est triviale.*

Démonstration. Pour prouver que K est un corps topologique, il suffit de prouver que les applications de $K \times K$ dans K définies par $(x, y) \mapsto x-y$ et $(x, y) \mapsto xy$ sont continues ainsi que l'application de $K^\times$ dans $K^\times$ définie par $x \mapsto x^{-1}$. Vérifions-le pour la dernière application. Soit $x_0 \in K^\times$ et $\varepsilon > 0$. On a

$$|x^{-1} - x_0^{-1}| \leqslant \frac{1}{|x||x_0|}|x - x_0|.$$

Si $|x - x_0| < \min(\frac{|x_0|}{2}, \frac{\varepsilon|x_0|^2}{2})$, on a $|x^{-1}x_0^{-1}| < \varepsilon$.

Si la valeur absolue est triviale, la topologie est discrète car tous les singletons de K sont des ouverts. Si la valeur absolue n'est pas triviale, il existe $x \in K^\times$ tel que $|x| \neq 1$. Quitte à remplacer x par son inverse, on peut supposer $|x| < 1$ et la suite $(x^n)_{n\geqslant 0}$ tend vers 0 alors que $x^n \neq 0$ pour tout $n \geqslant 0$. Le singleton $|0|$ n'est donc pas ouvert et la topologie n'est pas discrète. □

Définition 2.1.4. *On dit que deux valeurs absolues sur K sont* équivalentes *si elles définissent la même topologie sur K. On appelle* place *de K une classe d'équivalence de valeurs absolues non triviales sur K.*

Lemme 2.1.5. *Soient $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur K. Elles sont équivalentes si et seulement si il existe un nombre réel $\alpha > 0$ tel que $|\cdot|_2 = |\cdot|_1^\alpha$.*

Démonstration. Commençons par remarquer que si $|\cdot|$ est une norme de K, les ensembles $\{x \in K \mid |x| > 1\}$ et $\{x \in K \mid |x| < 1\}$ ne dépendent que de la topologie définie par $|\cdot|$. En effet $|x| < 1$ si et seulement si la suite $(x^n)_{n\geqslant 0}$ tend vers 0.

Supposons alors que les normes $|\cdot|_1$ et $|\cdot|_2$ définissent la même topologie sur K. La remarque ci-dessus implique que, pour $x, y \in K$, on a $|x|_1 \leqslant |y|_1$ si et seulement si $|x|_2 \leqslant |y|_2$. Il est clair que $|\cdot|_1$ est triviale si et seulement si $|\cdot|_2$ est triviale. On peut donc supposer $|\cdot|_1$ et $|\cdot|_2$ non triviales et choisir $x_0 \in K$ tel que $|x_0|_1 > 1$. Ainsi $|x_0|_2 > 1$. Il existe donc $\alpha > 0$ tel que $|x_0|_2 = |x_0|_1^\alpha$. Soit $x \in K$ tel que $|x|_1 > 1$. On peut alors écrire $|x|_1 = |x_0|_1^a$ et $|x|_2 = |x_0|_2^b$ pour $a, b > 0$. Soit $\frac{p}{q} \in \mathbb{Q}$ tel que $\frac{p}{q} \leqslant a$. On a alors

$$|x_0|_1^{\frac{p}{q}} \leqslant |x_0|_1^a = |x|_1$$

de sorte que $|x_0^p|_1 \leqslant |x^q|_1$ et donc $|x_0^p|_2 \leqslant |x^q|_2$. On en déduit $|x|_2^{\frac{p}{q}} \leqslant |x|_2 = |x_0|_2^b$. Ceci étant vrai pour tout $\frac{p}{q} \leqslant a$, on en déduit que $a \leqslant b$. En inversant les rôles de $|\cdot|_1$ et $|\cdot|_2$, on montre de même que $b \leqslant a$ et donc que $a = b$. Ainsi $|x|_2 = |x|_1^a$ pour tout x tel que $|x|_1 > 1$. Les propriétés des valeurs absolues impliquent facilement que cette égalité est vérifiée pour tout $x \in K$. □

2.1.2 Valeurs absolues ultramétriques

Proposition 2.1.6. *Une valeur absolue non triviale $|\cdot|$ est ultramétrique si et seulement si $|n| \leqslant 1$ pour tout $n \in \mathbb{Z}$. En particulier, si K est de caractéristique non nulle, toute valeur absolue de K est ultramétrique.*

Démonstration. Supposons $|\cdot|$ ultramétrique. Alors $|n| = |\underbrace{1 + \cdots + 1}_{n}| \leqslant |1| = 1$.

Réciproquement supposons que $|n| \leqslant 1$ pour tout $n \in \mathbb{Z}$. Soient $x, y \in K$ tels que $|x|, |y| \leqslant 1$. La formule du binôme implique que, pour $n \geqslant 0$

$$|(x+y)^n| \leqslant \sum_{i=0}^{n} \left| \binom{n}{i} \right| |x|^i |y|^{n-i} \leqslant n+1.$$

Ainsi $|x+y| \leqslant (n+1)^{\frac{1}{n}}$. En faisant tendre n vers $+\infty$, on en déduit que $|x+y| \leqslant 1$. Supposons à présent que x et y sont deux éléments quelconques de K. On va vérifier que $|x+y| \leqslant \max\{|x|, |y|\}$. Si $x = y = 0$ c'est évident. Supposons donc $|x| \leqslant |y| \neq 0$. Alors

$$|x+y| = |y||1 + xy^{-1}| \leqslant |y|.$$

Si la caractéristique de K est un nombre premier p, alors $\mathbb{Z}1_K = \mathbb{F}_p \subset K$. On en déduit que si $x \in \mathbb{Z}1_K$ est non nul, alors $x^{p-1} = 1$ et donc $|x| = 1$. Ainsi $|\cdot|$ est ultramétrique. □

Définition 2.1.7. *On dit qu'une valeur absolue ultramétrique de K est* discrète *si l'image de $K^\times$ est un sous-groupe discret de $\mathbb{R}_{>0}$.*

Comme les sous-groupes discrets de $\mathbb{R}_{>0}$ sont de la forme $a^{\mathbb{Z}}$ pour un certain $a \in \mathbb{R}$ tel que $0 < a \leqslant 1$, on en déduit que si $|\cdot|$ est discrète et non triviale, alors $|K^\times|$ est un groupe isomorphe à $\mathbb{Z}$.

Voici quelques propriétés des valeurs absolues ultramétriques.

Proposition 2.1.8. *1) Pour $x, y \in K$, tels que $|x| > |y|$, on a $|x+y| = |x|$.*

2) Une boule ouverte $B(x,r) = \{y \in K \mid |y-x| < r\}$ est à la fois ouverte et fermée dans K.

3) Une boule fermée $\overline{B}(x,r) = \{y \in K \mid |y-x| \leqslant r\}$ de rayon non nul est à la fois ouverte et fermée dans K.

4) Les sphères de K de rayon non nul sont à la fois ouvertes et fermées dans K.

5) Deux boules fermées (resp. ouvertes) de K sont disjointes ou incluses l'une dans l'autre.

Démonstration. Démontrons la propriété 2). Il est clair qu'une boule ouverte est ouverte, montrons qu'elle est fermée. Il suffit de prouver que son complémentaire est ouvert. Si $|y-x| \geqslant r$, alors si $|z| < r$, on a $|y+z-x| = |y-x| \geqslant r$, de sorte que $B(y,r) \subset K \smallsetminus B(x,r)$.

Démontrons la propriété 5). Soient $\overline{B}(x,r)$ et $\overline{B}(x',r')$ deux boules fermées et supposons $r \leqslant r'$. Supposons de plus que $\overline{B}(x,r) \cap \overline{B}(x',r') \neq \emptyset$ et soit $y \in \overline{B}(x,r) \cap \overline{B}(x',r')$. Si $z \in \overline{B}(x,r)$, on a

$$|z-x'| \leqslant \max\{|z-y|, |y-x|\} \leqslant r'$$

de sorte que $z \in \overline{B}(x',r')$ et $\overline{B}(x,r) \subset \overline{B}(x',r')$.

Les autres points sont laissés en exercice. □

Si $|\cdot|$ est une valeur absolue ultramétrique sur K, on note

$$\mathcal{O} = \{x \in K \mid |x| \leqslant 1\} \quad \text{et} \quad \mathfrak{p} = \{x \in K \mid |x| < 1\}.$$

Les propriétés d'une valeur absolue ultramétrique montrent que $\mathcal{O}$ est un sous-anneau de K appelé *anneau de valuation associé à* $|\cdot|$ et que $\mathfrak{p}$ est un idéal de $\mathcal{O}$.

Proposition 2.1.9. *Soit $|\cdot|$ une valeur absolue ultramétrique sur K.*

(i) L'anneau $\mathcal{O}$ est local et l'idéal $\mathfrak{p}$ est l'unique idéal maximal de $\mathcal{O}$.

(ii) L'idéal $\mathfrak{p}$ est principal si et seulement si la valuation $|\cdot|$ est discrète. Dans ce cas, l'anneau $\mathcal{O}$ est principal.

(iii) L'anneau $\mathcal{O}$ est un anneau de valuation discrète si et seulement si $|\cdot|$ est discrète et non triviale.

Démonstration. Remarquons qu'un élément $x \in \mathcal{O}$ est inversible dans $\mathcal{O}$ si et seulement si $|x| = 1$. Ainsi $\mathcal{O}^\times = \mathcal{O} \smallsetminus \mathfrak{p}$. Ceci implique que tout idéal non trivial de $\mathcal{O}$ est inclus dans $\mathfrak{p}$. Comme de plus, $\mathfrak{p} \subsetneq \mathcal{O}$, l'idéal $\mathfrak{p}$ est le plus grand élément de l'ensemble des idéaux non triviaux de $\mathcal{O}$, il s'agit donc de l'unique idéal maximal de $\mathcal{O}$, ce qui prouve (i).

Notons Γ le sous-groupe $|K^\times|$ de $\mathbb{R}_{>0}$ et prouvons (ii). Si $|\cdot|$ est triviale, alors $\mathcal{O} = K$ et $\Gamma = \{1\}$, (ii) est trivialement vérifié. On peut donc supposer $|\cdot|$ non triviale.

Supposons que l'idéal $\mathfrak{p}$ est principal et soit π un générateur de $\mathfrak{p}$. Alors $\Gamma \cap]|\pi|, |\pi|^{-1}[= \{1\}$. Le sous-groupe Γ est donc discret dans $\mathbb{R}_{>0}$.

Réciproquement supposons Γ discret et non réduit à $\{1\}$. Il existe donc $a \in]0,1[$ tel que $|K^\times| = a^{\mathbb{Z}}$. Posons $v(x) = \frac{\log|x|}{\log a}$ si $x \neq 0$ et $v(0) = +\infty$. L'application v est

alors une valuation discrète normalisée de K. Les points (ii) et (iii) se déduisent alors de la proposition 1.1.2. □

Si $(K, |\cdot|)$ est un corps valué ultramétrique, le corps $\mathcal{O}/\mathfrak{p}$ est appelé *corps résiduel* de $(K, |\cdot|)$.

Si v est une valuation discrète d'un corps K, alors $x \mapsto e^{-v(x)}$ est une valeur absolue discrète de K. On déduit facilement le résultat suivant du lemme 2.1.5 :

Proposition 2.1.10. *La construction $v \mapsto e^{-v(-)}$ induit une bijection entre l'ensemble des valuations discrètes normalisées sur K et l'ensemble des places ultramétriques discrètes non triviales de K.*

2.1.3 Valeurs absolues de certains corps globaux

Soit $\mathbb{F}_q$ un corps fini de cardinal q. Soit $P \in \mathbb{F}_q[T]$ un polynôme irréductible. L'anneau $\mathbb{F}_q[T]$ est un anneau factoriel, on peut donc définir la valuation P-adique d'un élément de $\mathbb{F}_q(T)$ et définir $|\cdot|_P = q^{-v_P(\cdot)\deg(P)}$. Il s'agit d'une valeur absolue ultramétrique sur $\mathbb{F}_q(T)$. On peut également définir, pour $R, S \in \mathbb{F}_q[T]$, avec $S \neq 0$,

$$\left|\frac{R}{S}\right|_\infty := q^{\deg(R)-\deg(S)}.$$

Il s'agit d'une valeur absolue ultramétrique correspondant au choix $P = T^{-1}$ sur $\mathbb{F}_q(T^{-1}) = \mathbb{F}_q(T)$. On peut donc également la noter $|\cdot|_{T^{-1}}$.

Théorème 2.1.11. *Les places de $\mathbb{F}_q(T)$ sont associées aux valeurs absolues de la forme $|\cdot|_P$ ou $|\cdot|_\infty$. De plus ces places sont deux à deux distinctes.*

Démonstration. Soit $|\cdot|$ une valeur absolue non triviale sur $K = \mathbb{F}_q(T)$. Supposons dans un premier temps que $|\mathbb{F}_q[T]| \leqslant 1$. Comme $|\cdot|$ est non triviale, l'ensembles $\{Q \in \mathbb{F}_q[T] \mid |Q| < 1\}$ est un idéal premier non nul de $\mathbb{F}_q[T]$. Il est donc engendré par un polynôme irréductible P. Ainsi pour $Q \in \mathbb{F}_q[T] \smallsetminus P\mathbb{F}_q[T]$, on a$|Q| = 1$. Si $R \in \mathbb{F}_q(T)$, on écrit $R = P^{v_P(R)}\frac{Q_1}{Q_2}$ avec $Q_1, Q_2 \in \mathbb{F}_q[T] \smallsetminus P\mathbb{F}_q[T]$. On en déduit que $|R| = |P|^{v_P(R)}$ et donc que $|\cdot|$ est équivalente à $|\cdot|_P$.

Supposons à présent qu'il existe $Q \in \mathbb{F}_q[T]$ tel que $|Q| > 1$. Comme $|a| = 1$ pour $a \in \mathbb{F}_q^\times$ et que $|\cdot|$ est ultramétrique d'après la proposition 2.1.6, on a nécessairement $|T| > 1$. On en déduit que $|\mathbb{F}_q[T^{-1}]| \leqslant 1$ et que $|T^{-1}| < 1$. Le raisonnement précedent mené avec $\mathbb{F}_q[T^{-1}]$ montre alors que $|\cdot|$ est équivalente à $|\cdot|_{T^{-1}}$.

Les valeurs absolues $|\cdot|_P$ et $|\cdot|_{T^{-1}}$ sont non équivalentes deux-à-deux. En effet, le raisonnement ci-dessus montre que $|P| < 1$ implique $|\cdot| \sim |\cdot|_P$ et $|T^{-1}| < 1$ implique $|\cdot| \sim |\cdot|_{T^{-1}}$. □

Théorème 2.1.12. *Les places de $\mathbb{Q}$ sont celles qui sont associées aux valeurs absolues $|\cdot|_\infty$ et $|\cdot|_p$ pour p premier. De plus ces places sont deux à deux distinctes.*

Démonstration. Soit $|\cdot|$ une valeur absolue ultramétrique non triviale. Soit $\mathcal{O}$ son anneau de valuation et $\mathfrak{p}$ son idéal maximal. L'idéal $\mathfrak{p}\cap\mathbb{Z}$ est alors un idéal premier de $\mathbb{Z}$. Si $\mathfrak{p}\cap\mathbb{Z}=(0)$, alors $|x|=1$ pour tout $x\in\mathbb{Z}\smallsetminus\{0\}$ et donc $|\mathbb{Q}^\times|=\{1\}$, ce qui contredit le fait que $|\cdot|$ est non triviale. Il existe donc un nombre premier p tel que $\mathfrak{p}\cap\mathbb{Z}=(p)$. On en déduit que si $m\in\mathbb{Z}$ est premier à p, alors $|m|=1$ et donc que $|p^\alpha\frac{r}{s}|=|p|^\alpha$ pour tout $\alpha\in\mathbb{Z}$, $r,s\in\mathbb{Z}$ premiers à p. On en conclut que $|\cdot|$ est équivalente à $|\cdot|_p$.

Supposons à présent $|\cdot|$ non ultramétrique et posons $f(x)=\sup\{0,\log|x|\}$ pour $x\in\mathbb{Z}$. Il existe donc $m\in\mathbb{Z}$ tel que $f(m)>0$. Pour tous $(m,n)\in\mathbb{Z}$ et $k\in\mathbb{N}$, on a

$$f(m^k)=kf(m),\quad f(mn)\leqslant f(m)+f(n),\quad f(m+n)\leqslant\log(2)+\sup\{f(m),f(n)\}.$$

Soient a et b deux entiers tels que $a,b>1$. On peut écrire le développement a-adique de b qui donne

$$b=x_0+x_1a+\cdots+x_na^n$$

avec $0\leqslant x_i\leqslant a-1$ et $x_n\neq 0$. Posons $c=\sup\{f(i)\mid 0\leqslant i<a\}$. On a donc $f(x_ia^i)\leqslant c+if(a)$ pour tout i et donc

$$f(b)\leqslant n\log(2)+nf(a)+c.$$

Comme $a^n\leqslant b$, on a $n\log(a)\leqslant\log(b)$ et donc

$$\frac{f(b)}{\log(b)}\leqslant\frac{\log(2)+f(a)}{\log(a)}+\frac{c}{\log(b)}.$$

Quitte à remplacer b par b^k et à faire tendre k vers $+\infty$, on obtient

$$\frac{f(b)}{\log(b)}\leqslant\frac{\log(2)+f(a)}{\log(a)}.$$

En faisant de même avec a, on obtient

$$\frac{f(b)}{\log(b)}\leqslant\frac{f(a)}{\log(a)}.$$

Quitte à échanger les rôles de a et b, on voit que $a\mapsto\frac{f(a)}{\log(a)}$ est constante sur $\mathbb{Z}_{\geqslant 2}$, elle est donc égale à un réel $\alpha>0$, ce qui prouve le résultat. □

2.2 Corps complets, corps locaux

2.2.1 Corps complets

Soit $(K, |\cdot|)$ un corps valué. On dit que K est *complet* s'il est complet pour la distance induite par $|\cdot|$.

Si $(K, |\cdot|)$ est un corps valué, on note $\widehat{K}$ le complété de K pour la topologie induite par $|\cdot|$. Pour tout $x, y \in K$, on a $||x|-|y|| \leqslant |x-y|$ de sorte que l'application $|\cdot| : K \to \mathbb{R}$ est uniformément continue et se prolonge donc en une application continue $|\cdot|_{\widehat{K}} : \widehat{K} \to \mathbb{R}$.

Lemme 2.2.1. *L'ensemble $\widehat{K}$ est muni d'une unique structure de corps topologique induisant sur K la structure de corps topologique issue de $|\cdot|$.*

Démonstration. Le fait que $\widehat{K}$ est muni d'une unique structure d'anneau topologique compatible à celle de K, je renvoie à la Proposition 7 [Bourbaki, Topologie Générale, §III.6]. Il reste à vérifier que $\widehat{K}$ est un corps. Pour cela, il faut vérifier que si $(x_n)_{n\geqslant 0}$ est une suite de Cauchy de K ne tendant pas vers 0, alors la suite $(x_n^{-1})_{n\geqslant 0}$ est de Cauchy. On le vérifie en utilisant l'égalité

$$\forall x, y \in K, \quad |x^{-1} - y^{-1}| = |x^{-1}||y^{-1}||x - y|. \qquad \square$$

Lemme 2.2.2. *L'application $|\cdot|_{\widehat{K}}$ est une valeur absolue sur $\widehat{K}$.*

Démonstration. La plupart des propriétés des valeurs absolues se vérifient facilement par passage à la limite. Il reste essentiellement à vérifier que si $|x|_{\widehat{K}} = 0$, alors $x = 0$. Supposons en effet que $|x|_{\widehat{K}} = 0$, il existe alors une suite $(x_n)_{n\geqslant 0}$ de K convergeant vers x et telle que $|x_n|$ converge vers 0. Ceci implique que $(x_n)_{n\geqslant 0}$ converge vers 0 dans K, et donc que $x = 0$. $\square$

La valeur absolue $|\cdot|_{\widehat{K}}$ est donc l'unique prolongement continue de $|\cdot|$ à K, on la note $|\cdot|$ par abus de langage.

Le complété d'un corps valué possède une propriété universelle.

Proposition 2.2.3. *Soit $(K, |\cdot|)$ un corps valué, L un corps valué complet et $f : K \to L$ un morphisme de corps topologiques, il existe alors un unique morphisme de corps topologiques $\widehat{f} : \widehat{K} \to L$ dont la restriction à K est égale à f.*

Démonstration. Un morphisme de corps topologiques est uniformément continu, l'existence de $\widehat{f}$ est donc une propriété universelle de la complétion d'un espace métrique. On vérifie facilement que $\widehat{f}$ est bien un morphisme de corps. $\square$

Corollaire 2.2.4. *Si $(K, |\cdot|)$ est un corps valué et $(L, |\cdot|')$ un corps valué contenant K tel que la restriction de $|\cdot|'$ à K est équivalente à $|\cdot|$ et tel que K est dense dans L, alors $(L, |\cdot|')$ est isomorphe au complété de K.*

Exemple 2.2.5. 1. Le complété de $\mathbb{Q}$ pour la norme $|\cdot|_\infty$ est isomorphe à $\mathbb{R}$.

2. Soit k un corps et $K = k(T)$. Soit v la valuation T-adique sur $k(T)$. Le complété de K pour la valuation v est isomorphe au corps $k(\!(T)\!)$ des séries de Laurent, c'est-à-dire

$$k(\!(T)\!) = \left\{ \sum_{n=-N}^{+\infty} a_n T^n \mid N \in \mathbb{N},\, a_n \in k \right\}.$$

Définition 2.2.6. *Soit p un nombre premier. Le complété de $\mathbb{Q}$ pour la norme $|\cdot|_p$ est appelé* corps des nombres p-adiques *et est noté $\mathbb{Q}_p$. On note $\mathbb{Z}_p$ l'anneau des entiers de $\mathbb{Q}_p$, ses éléments sont appelés* entiers p-adiques.

2.2.2 Corps complets ultramétriques

Lemme 2.2.7. *Soit K un corps complet ultramétrique. Soit $(x_n)_{n\geqslant 0}$ une suite d'éléments de K. Alors*

- *la suite $(x_n)_{n\geqslant 0}$ converge dans K si et seulement si la suite $(x_{n+1} - x_n)_{n\geqslant 0}$ tend vers 0 ;*
- *la série $\sum_{n\geqslant 0} x_n$ converge dans K si et seulement si la suite $(x_n)_{n\geqslant 0}$ tend vers 0.*

Démonstration. Les deux assertions sont visiblement équivalentes. Prouvons la première. Il suffit de prouver que si la suite $(x_{n+1} - x_n)_{n\geqslant 0}$ tend vers 0, alors la suite $(x_n)_{n\geqslant 0}$ est de Cauchy. Soit $\varepsilon > 0$ et soit $N \in \mathbb{N}$ tel que $n \geqslant N$ implique $|x_{n+1} - x_n| < \varepsilon$. Alors, pour tout $k \geqslant 1$,

$$|x_{n+k} - x_n| \leqslant \max(|x_{n+1} - x_n|, \ldots, |x_{n+k} - x_{n+k-1}|) < \varepsilon.$$

Ainsi la suite $(x_n)_{n\geqslant 0}$ est de Cauchy. □

Soit K un corps complet pour une valeur absolue ultramétrique. On note $\mathcal{O}_K$ son anneau d'entiers, $\mathfrak{p}_K$ l'idéal maximal de $\mathcal{O}_K$ et k le corps résiduel $\mathcal{O}_K/\mathfrak{p}_K$.

Proposition 2.2.8. *Soit $(K, |\cdot|)$ un corps valué complet ultramétrique.*

(i) On a $|K^\times| = |\widehat{K}^\times|$.

(ii) L'ensemble $\mathcal{O}_{\widehat{K}}$ est l'adhérence de $\mathcal{O}_K$ dans $\widehat{K}$.

(iii) L'application naturelle

$$\mathcal{O}_K/\mathfrak{p}_K \to \mathcal{O}_{\widehat{K}}/\mathfrak{p}_{\widehat{K}}$$

est un isomorphisme.

Démonstration. Démontrons (i). Soit $r = |a| \in |\widehat{K}^\times|$ et soit $b \in K$ tel que $|a-b| < |a|$. On a alors $|b| = |a| = r$ de sorte que $r \in |K^\times|$.

Pour (ii), on remarque que l'idéal maximal $\mathfrak{p}_{\widehat{K}}$ est ouvert dans $\mathcal{O}_{\widehat{K}}$, on a donc $\mathcal{O}_{\widehat{K}} = \mathcal{O}_K + \mathfrak{p}_{\widehat{K}}$.

Le point (iii) se déduit donc de (ii) et de l'égalité

$$\mathfrak{p}_{\widehat{K}} \cap \mathcal{O}_K = \{x \in K \mid |x| < 1\} = \mathfrak{p}_K. \qquad \square$$

Supposons désormais que $(K, |\cdot|)$ est un corps valué complet ultramétrique et que $|\cdot|$ est discrète. Il existe un nombre réel $\varepsilon < 1$ tel que $|K^\times| = \varepsilon^{\mathbb{Z}}$. On appelle *uniformisante de* K un élément $\pi \in \mathcal{O}_K$ tel que $|\pi| = \varepsilon$. De façon équivalente, π est un élément de K tel que $\mathfrak{p}_K = (\pi)$.

Proposition 2.2.9. *Soit Σ un ensemble de représentants de k dans $\mathcal{O}_K$. Alors tout élément de $\mathcal{O}_K$ s'écrit de façon unique sous la forme d'une série convergente*

$$x_0 + x_1\pi + \cdots + x_n\pi^n + \cdots$$

où les x_i sont des éléments de Σ.

Démonstration. Remarquons qu'une telle série converge dans K puisque $|x_i\pi^i| \leqslant |\pi|^i \to_{n\to+\infty} 0$.

Prouvons tout d'abord l'existence d'un tel développement. Soit $x_0 \in \Sigma$ tel que x et x_0 ont la même classe dans k. Alors $x - x_0 \in \mathfrak{p} = (\pi)$, il existe donc $y \in \mathcal{O}_K$ tel que $x = x_0 + y\pi$. En remplaçant x par y, il existe $x_1 \in \Sigma$ tel que $x - (x_0 + x_1 y) \in (\pi^2)$. Par récurrence, on obtient l'existence d'une suite $(x_n)_{n\geqslant 0}$ telle que

$$x - (x_0 + x_1\pi + \cdots + x_n\pi^n) \in (\pi^{n+1})$$

pour tout $n \geqslant 0$, de sorte que la série $\sum_{n\geqslant 0} x_n\pi^n$ converge vers x.

Prouvons l'unicité. Supposons que l'on puisse écrire $x = \sum_{n\geqslant 0} x_n\pi^n = \sum_{n\geqslant 0} x'_n\pi^n$ avec $x_n, x'_n \in \Sigma$ et soit m le plus petit entier tel que $x_m \neq x'_m$. Alors

$$x_m\pi^m - x'_m\pi^m \in (\pi^{m+1})$$

de sorte que $x_m - x'_m \in (\pi)$. Ceci contredit $x_m \neq x'_m$ et le fait que Σ est un système de représentants de k dans $\mathcal{O}_K$. $\square$

Corollaire 2.2.10. *Soit Σ un ensemble de représentants de k dans $\mathcal{O}_K$. Tout élément de K s'écrit de façon unique sous la forme d'une série convergente*

$$\sum_{n \geqslant -N} x_n \pi^n$$

où les x_n sont des éléments de Σ et $N \in \mathbb{N}$.

Démonstration. Comme $\mathcal{O}_K$ est un anneau de valuation discrète, on a $K = \mathcal{O}_K[\pi^{-1}]$ et on utilise la proposition 2.2.9. □

Exemple 2.2.11. L'anneau $\mathbb{Z}_p$ est l'adhérence de l'anneau $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a \in \mathbb{Z},\, b \in \mathbb{Z} \smallsetminus p\mathbb{Z}\}$ qui est aussi le localisé de $\mathbb{Z}$ relativement à l'idéal premier (p). D'après la proposition 2.2.8, la valuation de $\mathbb{Q}_p$ est discrète et le corps résiduel de $\mathbb{Q}_p$ est isomorphe au corps $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{F}_p$. On peut donc choisir comme système de représentants de $\mathbb{F}_p$ l'ensemble $\Sigma = \{0, 1, \ldots, p-1\}$. Par ailleurs p est une uniformisante de $\mathbb{Q}_p$. On en conclut que tout entier p-adique s'écrit de façon unique sous forme d'une série convergente

$$\sum_{n \geqslant 0} a_n p^n$$

où $a_n \in \{0, 1, \ldots, p-1\}$.

2.2.3 Corps locaux

Un corps valué est dit *local* s'il est localement compact en tant qu'espace topologique et si sa valeur absolue est non triviale. Un corps local est donc en particulier complet (voir proposition B.3.2).

Lemme 2.2.12. *Soit $(K, |\cdot|)$ un corps valué de valuation non triviale. Les assertions suivantes sont équivalentes.*

(i) Le corps K est un corps local.

(ii) Il existe $r > 0$ tel que la boule fermée $\overline{B}(0, r)$ est compacte.

(iii) La boule unité fermée $\overline{B}(0, 1)$ est compacte.

(iv) Toutes les boules fermées de K sont compactes.

De plus lors que K est ultramétriques, ces conditions sont encore équivalentes à ce que $\mathcal{O}_K$ est compact.

Démonstration. Il est clair que (i) implique (ii). Montrons que (ii) implique (iii). Soit $r > 0$ tel que $\overline{B}(0, r)$ est compacte. Comme $|\cdot|$ est non discrète, il existe $a \in K^\times$

tel que $|a| > 1/r$. Comme l'application $x \mapsto ax$ est continue, l'ensemble $a\overline{B}(0,r)$ est compact. De plus il contient $\overline{B}(0,1)$. Ainsi $\overline{B}(0,1)$ est un fermé d'un compact et est donc compact. Montrons que (iii) implique (iv). On démontre comme précédemment que la compacité de $\overline{B}(0,1)$ implique la compacité de $\overline{B}(0,r)$ pour tout $r > 0$. Comme l'application $x \mapsto x+y$ est continue pour tout $y \in K$, on en conclut que $\overline{B}(y,r)$ est compact pour tout $y \in K$ et tout $r > 0$. Le cas $r = 0$ est immédiat car les ensembles finis sont compacts. Enfin il est clair que (iv) implique (i) car les boules fermées de centre x forment un système de voisinages de x pour tout $x \in K$.

La dernière assertion provient du fait que $\overline{B}(0,1) = \mathcal{O}_K$ lorsque $|\cdot|$ est ultramétrique. □

Proposition 2.2.13. *Soit K un corps valué complet ultramétrique. Alors K est local si et seulement si sa valuation est discrète et son corps résiduel est fini.*

Démonstration. Supposons que K est local. Prouvons que sa valuation est discrète. On peut écrire

$$\mathcal{O}_K = \overline{B}(0,1) = S(0,1) \coprod_{0<r<1} \overline{B}(0,r).$$

Comme $\mathcal{O}_K$ est compact d'après le lemme 2.2.12 et que la sphère $S(0,1)$ ainsi que les boules fermées $\overline{B}(0,r)$ sont ouvertes, cette union est en réalité finie et il existe $0 < r < 1$ tel que

$$\mathcal{O} = S(0,1) \coprod \overline{B}(0,r).$$

Ainsi $|K^\times| \cap]r,1[= \emptyset$ et $|K^\times|$ est un sous-groupe discret de $\mathbb{R}_+^\times$.

Montrons que le corps résiduel de K est fini. Comme $\mathcal{O}_K$ est une boule fermée de K, c'est une partie compacte. De plus l'idéal maximal $\mathfrak{p}_K = B(0,1)$ est une partie ouverte de K. Soit Σ un système de représentants de $k = \mathcal{O}_K/\mathfrak{p}_K$ dans $\mathcal{O}_K$. On a alors

$$\mathcal{O}_K = \coprod_{x\in\Sigma} (x + \mathfrak{p}_K)$$

où chaque $x + \mathfrak{p}_K$ est une partie ouverte de K. On déduit de la compacité de $\mathcal{O}_K$ que Σ, et donc k, est fini.

Réciproquement supposons que la valuation est discrète et que k est un corps fini et fixons Σ un ensemble de représentants de k dans $\mathcal{O}$, ainsi qu'une uniformisante π. Montrons que $\mathcal{O}_K$ est précompact. Soit $0 < r < 1$ et soit $n \in \mathbb{N}$ tel que $|\pi^n| < r$. Si $x \in \mathcal{O}_K$, on peut écrire

$$x \in x_0 + x_1\pi + \cdots + x_{n-1}\pi^{n-1} + (\pi^n) = \overline{B}(x_0 + x_1\pi + \cdots + x_{n-1}\pi^{n-1}, |\pi|^n)$$

d'après la proposition 2.2.9. On en déduit que $\mathcal{O}_K$ possède un recouvrement fini par des boules ouvertes de rayon r. Ainsi $\mathcal{O}_K$ est précompact. Comme de plus $\mathcal{O}_K$

est une partie fermée de l'espace métrique K, on en déduit que $\mathcal{O}_K$ est compact. On conclut en utilisant le lemme 2.2.12. □

Exemple 2.2.14. On déduit de l'exemple 2.2.11 et de la proposition 2.2.13 que $\mathbb{Q}_p$ est un corps local et que $\mathbb{Z}_p$ est un espace compact.

2.2.4 Le Lemme de Hensel

Théorème 2.2.15. *Soit K un corps complet ultramétrique. Soit $f \in \mathcal{O}_K[X]$ et soit $x \in \mathcal{O}_K$ tel que $\left|\frac{f(x)}{f'(x)^2}\right| < 1$. Alors il existe un unique $y \in \mathcal{O}_K$ telle que $f(y) = 0$ et $|y - x| \leqslant \left|\frac{f(x)}{f'(x)}\right|$.*

Démonstration. Soit $\alpha_0 \in \mathcal{O}_K$ tel que $\left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1$. Posons

$$\alpha_1 \coloneqq \alpha_0 - \frac{f(\alpha_0)}{f'(\alpha_0)}.$$

On a $|\frac{f(\alpha_0)}{f'(\alpha_0)}| < |f'(\alpha_0)| \leqslant 1$ de sorte que $\alpha_1 \in \mathcal{O}_K$. Posons

$$\varepsilon_0 \coloneqq |\alpha_1 - \alpha_0| = \left|\frac{f(\alpha_0)}{f'(\alpha_0)}\right|, \quad \eta_0 \coloneqq |f'(\alpha_0)|.$$

Lemme 2.2.16. *On a $|f(\alpha_1)| \leqslant \varepsilon_0^2$ et $|f'(\alpha_1)| = \eta_0$.*

Démonstration. Comme $f(\alpha_0 + X) \in \mathcal{O}_K[X]$, on a, en posant $h \coloneqq -\frac{f(\alpha_0)}{f'(\alpha_0)}$,

$$f(\alpha_1) = f(\alpha_0) + hf'(\alpha_0) + h^2R$$

où $R \in \mathcal{O}_K$. On en déduit

$$|f(\alpha_1)| \leqslant |h|^2 = \varepsilon_0^2.$$

De même

$$f'(\alpha_1) \in f'(\alpha_0) + h\mathcal{O}_K$$

de sorte que $|f'(\alpha_1) - f'(\alpha_0)| \leqslant |h| = \varepsilon_0$. Comme $\varepsilon_0 < \eta_0 = |f'(\alpha_0)|$, on a bien

$$|f'(\alpha_1)| = |f'(\alpha_0)| = \eta_0.$$ □

On en déduit en particulier que

$$\left|\frac{f(\alpha_1)}{f'(\alpha_1)}\right| \leqslant \frac{\varepsilon_0^2}{\eta_0} < \eta_0 = |f'(\alpha_1)|$$

de sorte que $\left|\frac{f(\alpha_1)}{f'(\alpha_1)^2}\right| < 1$. Ceci nous permet de définir par récurrence une suite d'éléments de $\mathcal{O}_K$ en posant $\alpha_{n+1} \coloneqq \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$ pour tout $n \geqslant 0$. En posant $\varepsilon_n \coloneqq |\alpha_{n+1} - \alpha_n|$, on a

$$\forall n \in \mathbb{N}, \quad |f(\alpha_{n+1})| \leqslant \varepsilon_n^2, \quad |f'(\alpha_n)| = \eta_0, \quad \varepsilon_n < \eta_0.$$

Ainsi $\varepsilon_{n+1} \leqslant \frac{\varepsilon_n^2}{\eta_0} < \varepsilon_n$ et, par récurrence on obtient

$$\forall n \in \mathbb{N}, \quad \varepsilon_n \leqslant \frac{\varepsilon_0^{2^n}}{\eta_0^{2^n-1}} = \eta_0 \left(\frac{\varepsilon_0}{\eta_0}\right)^{2^n}.$$

Comme $\varepsilon_0 < \eta_0$, on en déduit que $\varepsilon_n \to 0$ et donc que la suite $(\alpha_n)_{n\geqslant 0}$ converge vers un élément $\alpha \in \mathcal{O}_K$ tel que $f(\alpha) = 0$ et $|\alpha - \alpha_0| \leqslant \varepsilon_0 = |\frac{f(\alpha_0)}{f'(\alpha_0)}|$. En posant $\alpha_0 = x$, on peut choisir $y = \alpha$.

Démontrons l'unicité de y. Supposons que y_1 et y_2 vérifient les conditions requises. On a alors, pour $i \in \{1, 2\}$, $f'(y_i) = f'(x) + (y_i - x)R_i$ avec $R_i \in \mathcal{O}_K$. On en déduit que

$$|f'(y_i) - f'(x)| \leqslant |y_i - x| \leqslant |\tfrac{f(x)}{f'(x)}| < |f'(x)|.$$

Ainsi $|f'(y_i)| = |f'(x)|$. On déduit que

$$0 = f(y_2) = f(y_1) + (y_2 - y_1)f'(y_1) + (y_2 - y_1)^2 S$$

pour un $S \in \mathcal{O}_K$. Supposons par l'absurde $y_2 - y_1 \neq 0$. On en déduit $f'(y_1) \in (y_2 - y_1)\mathcal{O}_K$ et donc

$$|f'(x)| = |f'(y_1)| \leqslant |y_2 - y_1| \leqslant \max\{|y_1 - x|, |y_2 - x|\} \leqslant \left|\frac{f(x)}{f'(x)}\right|$$

ce qui contredit l'hypothèse $|\frac{f(x)}{f'(x)^2}| < 1$. Ainsi $y_2 = y_1$. □

Corollaire 2.2.17. *Soit K un corps valué complet. Soit $f \in \mathcal{O}_K[X]$ de réduction $\overline{f} \in k[X]$ et soit $\overline{x} \in k$ une racine de $\overline{f}$ telle que $\overline{f}'(\overline{x}) \neq 0$. Il existe $x \in \mathcal{O}_K$ relevant $\overline{x}$ et tel que $f(x) = 0$.*

Démonstration. On applique le théorème 2.2.15 à $x_0 \in \mathcal{O}_K$ relevant $\overline{x}$. On a alors $|f'(x_0)| = 1$ et $|f(x_0)| < 1$. On peut donc trouver $x \in \mathcal{O}_K$ tel que $|x - x_0| \leqslant |f(x_0)| < 1$ et $f(x) = 0$. On a de plus $0 = f(x_0) + (x - x_0)f'(x_0) + (x - x_0)^2 R$ pour un certain $R \in \mathcal{O}_K$. On en déduit de cette égalité et de $|f'(x_0)|$ que $|(x-x_0)f'(x_0) + (x - x_0)^2 R| = |(x - x_0)f'(x_0)| = |x - x_0|$. Ainsi $|x - x_0| = |f(x_0)| = |\frac{f(x_0)}{f'(x_0)}|$ et l'unicité de x se déduit de l'unicité dans le théorème 2.2.15. □

Exemple 2.2.18. Soit K un corps local ultramétrique. Son corps résiduel est un corps fini $\mathbb{F}_q$ de cardinal q. Soit $\zeta \in \mathbb{F}_q^\times$. Il s'agit d'une racine du polynôme $f(X) = X^{q-1} - 1$. Comme $f'(\zeta) \neq 0$ dans $\mathbb{F}_q$, on en déduit qu'il existe un unique élément $[\zeta] \in \mathcal{O}_K$ tel que $[\zeta] \in \mu_{q-1}(K)$ et $[\zeta]$ se réduit sur ζ dans $\mathbb{F}_q$. L'unicité de $[\zeta]$ implique la multiplicativité de l'application $[\cdot]$: on a $[\zeta\zeta'] = [\zeta][\zeta']$ pour tout $\zeta \in \mathbb{F}_q^\times$. L'élément $[\zeta]$ est appelé *relèvement de Teichmüller de* ζ.

On en déduit en particulier que l'application de réduction $\mathcal{O}_K^\times \to \mathbb{F}_q^\times$ possède une section donnée par $[\cdot]$. Comme son noyau est le sous-groupe $1 + (\pi)$ où π désigne une uniformisante de K. On en déduit un isomorphisme de groupes

$$\mathcal{O}_K^\times(1 + (\pi)) \times \mathbb{F}_q^\times \simeq (1 + (\pi)) \times \mu_{q-1}(K).$$

Soit π une uniformisante de K. Si $x \in K^\times$, il existe un unique n tel que $|x| = |\pi|^n$ et donc tel que $x \in \pi^n \mathcal{O}_K^\times$. On en déduit les isomorphismes de groupes

$$K^\times \simeq \mathcal{O}_K^\times \times \mathbb{Z} \simeq (1 + (\pi)) \times \mathbb{F}_q^\times \times \mathbb{Z}.$$

Remarque 2.2.19. La structure du groupe $1 + (\pi)$ est plus compliquée. On peut cependant remarquer qu'il possède une filtration par les sous-groupes $1 + (\pi^i)$ qui vérifie les propriétés suivantes

a) $\bigcap_{i \geqslant 1}(1 + (\pi^i)) = \{1\}$;

b) pour tout $i \geqslant 1$, le quotient $(1 + (\pi^i))/(1 + (\pi^{i+1}))$ est un p-groupe où p est la caractéristique du corps résiduel de K. En effet, on vérifie que l'application $1 + \pi^i u \mapsto \overline{u}$ induit un isomorphisme de groupes

$$\mathbb{F}_q \xrightarrow{\sim} (1 + (\pi^i))/(1 + (\pi^{i+1})).$$

2.2.5 Extensions de corps complets

Soit $(K, |\cdot|)$ un corps valué. Un *K-espace vectoriel normé* est la donnée d'un couple $(V, \|\cdot\|)$ où V est un K-espace vectoriel et $\|\cdot\| : V \to \mathbb{R}_{\geqslant 0}$ est une application vérifiant

— $\forall v \in V$, on a $\|v\| = 0$ si et seulement si $v = 0$;
— $\forall (\lambda, v) \in K \times V$, on a $\|\lambda v\| = |\lambda|\|v\|$;
— $\forall (v, w) \in V^2$, on a $\|v + w\| \leqslant \|v\| + \|w\|$.

Remarque 2.2.20. Lorsque la valeur absolue $|\cdot|$ est ultramétrique, on impose souvent la condition plus forte

$$\forall (v, w) \in V^2, \quad \|v + w\| \leqslant \sup\{\|v\|, \|w\|\}.$$

On dit alors que la norme est *ultramétrique*.

Exemple 2.2.21. Si $n \in \mathbb{N}$, on peut munir l'espace vectoriel K^n, de la norme

$$\|(x_1, \ldots, x_n)\|_\infty = \sup\{|x_i|,\, i = 1, \ldots, n\}.$$

Si V est un K-espace vectoriel de dimension finie, on dit que deux normes $\|\cdot\|_1$ et $\|\cdot\|_2$ sont équivalentes s'il existe des nombres réels $0 < C < C'$ tels que

$$C\|\cdot\|_2 \leqslant \|\cdot\|_1 \leqslant C'\|\cdot\|_2.$$

Proposition 2.2.22. *Soit K un corps complet et soit $(V, \|\cdot\|)$ un K-espace vectoriel normé de dimension finie d. Alors pour tout isomorphisme K-linéaire f de K^d sur V, il existe des réels $0 < C_1 \leqslant C_2$ tels que $C_1\|x\|_\infty \leqslant \|f(x)\| \leqslant C_2\|x\|_\infty$ pour tout $x \in K^d$. En particulier V est un espace métrique complet. Sur un K-espace vectoriel de dimension finie, toutes les normes sont équivalentes.*

Démonstration. Les deux dernières assertions sont des conséquences immédiates de la première. Nous allons prouver la première assertion par récurrence sur d. Comme tous les automorphismes K-linéaires de K^d sont continus, il suffit de prouver qu'il existe un isomorphisme de K^d sur V qui est un homéomorphisme.

Si $d = 1$ c'est évident. En effet on choisit un élément non nul $v \in V$. On a alors $V = Kv$ et on peut choisir $C_1 = C_2 = \|f(1)\|$. Supposons le résultat démontré pour d et soit V un K-espace vectoriel normé de dimension $d + 1$. Soit $(e_1, \ldots, e_{d+1})$ la base canonique de K^{d+1}. Posons $v = f(e_{d+1})$ et H le supplémentaire de Kv dans V engendré par les vecteurs $f(e_i)$ pour $1 \leqslant i \leqslant d$. Par récurrence, $(H, \|\cdot\|_H)$ est un espace vectoriel normé de dimension d et est donc complet. C'est donc un sous-espace vectoriel fermé de V. Montrons que la projection μ de V sur Kv parallèlement à H est continue. En effet si $(w_n)_{n\geqslant 0}$ est une suite de V convergeant vers 0, on écrit $w_n = \lambda_n v + h_n$ avec $\lambda_n \in K$ et $h_n \in H$ pour tout $n \geqslant 0$ et il faut vérifier que la suite (λ_n) converge vers 0. Si ce n'est pas le cas, il existe une suite extraite $(\lambda_{\varphi(n)})$ de (λ_n) qui est bornée inférieurement par $\alpha > 0$. On en déduit que v est la limite de la suite $(\lambda_n^{-1}h_n)_{n\geqslant 0}$, à valeurs dans H et donc que $v \in \overline{H} = H$, ce qui est faux. Il existe donc $D > 0$ tel que $|\mu(v)| \leqslant D\|v\|$ pour tout $v \in V$. Soient $0 < C_1' \leqslant C_2'$ obtenus par récurrence tels que $C_1'\|x\|_\infty \leqslant \|f(x)\| \leqslant C_2'\|x\|_\infty$ pour tout $x \in K^d \subset K^{d+1}$. On a alors, pour tout $x \in K^{d+1}$,

$$\inf\left\{\frac{C_1'}{1 + D\|f(e_{d+1})\|}, D^{-1}\right\}\|x\|_\infty \leqslant \|f(x)\| \leqslant (C_2' + \|v\|)\|x\|_\infty. \qquad \square$$

Théorème 2.2.23. *Soit $(K, |\cdot|_K)$ un corps valué complet ultramétrique et soit L une extension finie de K. Il existe alors une unique norme sur L dont la restriction à K coïncide avec $|\cdot|_K$. De plus L est complet pour cette norme.*

Démonstration. L'unicité est une conséquence de la proposition 2.2.22.

Soit $(e_1, \dots, e_d)$ une base de L sur K et soit $|\cdot|_1$ la norme sup de L sur K correspondant à ce choix de base, c'est-à-dire

$$\left|\sum_{i=1}^{d} x_i e_i\right|_1 = \sup_{i=1\dots d} |x_i|.$$

Il s'agit d'une norme ultramétrique de K-espace vectoriel sur L. Si de plus on pose $C = \sup_{1\leqslant i,j\leqslant d}|e_i e_j|$, on a $|xy|_1 \leqslant C|x|_1|y|_1$ pour tout x et y dans L.

Posons alors, pour $x \in L$, $|x|_2 \coloneqq \inf\{|x^n|_1^{\frac{1}{n}} \mid n \geqslant 1\}$. On vérifie cette fois que $|\cdot|_2$ est une norme de K-espace vectoriel prolongeant $|\cdot|_K$, sous-multiplicative et vérifiant de plus $|x^n|_2 = |x|_2^n$ pour tout $x \in L$ et $n \geqslant 1$.

Montrons dans un premier temps que $|x|_2 = \liminf_{n\to+\infty}|x^n|_1^{\frac{1}{n}}$. Soit $x \in L$ et soit $\varepsilon > 0$. Si $m \geqslant 1$ est tel que $|x^m|_1^{\frac{1}{m}} \leqslant |x|_2 + \varepsilon$. Alors si $n \geqslant 1$, on effectue la division euclidienne de n par m. On obtient $n = qm+r$ avec $0 \leqslant r \leqslant m-1$ et donc $|x^n|_1 \leqslant C^q|x^m|_1^q|x^r|_1$ de sorte que $|x^n|_1^{\frac{1}{n}} \leqslant C^{\frac{q}{n}}(|x|_2+\varepsilon)^{\frac{mq}{n}}|x^r|^{\frac{1}{n}}$. On peut choisir m suffisamment grand pour que $|x|_1^{\frac{1}{m}} \leqslant |x|_2 + \varepsilon$ et $C^{\frac{q}{n}} \leqslant C^{\frac{1}{m}} \leqslant 1+\varepsilon$. Il existe alors $n_0 \geqslant m$ tel que $|x^r|_1^{\frac{1}{n_0}} \leqslant (1+\varepsilon)$ pour tout $r \leqslant m-1$. On a alors, pour $n \geqslant n_0$,

$$|x^n|_1^{\frac{1}{n}} \leqslant (1+\varepsilon)^2(|x|_2+\varepsilon)^{1-\frac{r}{n}}.$$

On en déduit que la suite $(|x^n|_1^{\frac{1}{n}})_{n\geqslant 1}$ converge vers $|x|_2$. On en déduit immédiatement que $|x^n|_2 = |x|_2^n$ pour tout $n \geqslant 1$. Prouvons que $|\cdot|_2$ est sous-multiplicative. Si $x, y \in L$, on a $|(xy)^n|_1^{\frac{1}{n}} \leqslant C^{\frac{1}{n}}|x^n|_1^{\frac{1}{n}}|y^n|_1^{\frac{1}{n}}$ pour tout $n \geqslant 1$, ce qui implique facilement $|xy|_2 \leqslant |x|_2|y|_2$. Montrons à présent que $|x|_2 \neq 0$ si $x \neq 0$. Il suffit de remarquer que si $x \in K$, alors

$$|x|_2 = \lim_{n\to+\infty}|x^n|_1^{\frac{1}{n}} = |x|_K \lim_{n\to+\infty}|1|_1^{\frac{1}{n}} = |x|_K.$$

Ainsi, pour $x \in L^\times$, $1 = |1|_2 \leqslant |x|_2|x^{-1}|_2$ et donc $|x|_2 \neq 0$. Enfin vérifions que $|\cdot|_2$ est ultramétrique. Si x et y sont dans L, supposons $|x|_2 \geqslant |y|_2 \neq 0$. On a alors $|x+y|_2 \leqslant |y|_2|1+y^{-1}x|_1$ et il suffit de prouver que $|1+x|_2 \leqslant 1$ pour $|x|_2 \leqslant 1$. Fixons donc $x \in L$ tel que $|x|_2 \leqslant 1$. Pour tout $n \geqslant 1$, on a

$$|(1+x)^n|_1^{\frac{1}{n}} \leqslant \sup_{0\leqslant k\leqslant n}|x^k|_1^{\frac{1}{k}}.$$

Soient $\varepsilon > 0$ et $N \geqslant 1$ tels que $|x^n|^{\frac{1}{n}} \leqslant 1+\varepsilon$ pour $n \geqslant N$. Si $m \geqslant n \geqslant N$, on a donc

$$|x^n|_1^{\frac{1}{m}} = (|x^n|_1^{\frac{1}{n}})^{\frac{n}{m}} \leqslant (1+\varepsilon)^{\frac{m}{n}} \leqslant 1+\varepsilon.$$

En choisissant m assez grand pour que $|x^k|_1^{\frac{1}{m}} \leqslant 1+\varepsilon$ pour $0 \leqslant k \leqslant n$, on obtient donc $|(1+x)^m|_1^{\frac{1}{m}} \leqslant 1+\varepsilon$. Ainsi $|x|_2 \leqslant 1$.

Il reste donc à prouver que $|\cdot|_2$ est multiplicative. Pour cela, on démontre dans un premier temps que $|\cdot|_2$ est l'unique norme de K-espace vectoriel sur L vérifiant $|x^n|_2 = |x|_2^n$ pour tout $x \in L$ et pour tout $n \geqslant 1$. En effet deux telles normes $|\cdot|_2$ et $|\cdot|_2'$ doivent être équivalentes d'après la proposition 2.2.22. Il existe donc des réels $0 < C_1 \leqslant C_2$ tels que $C_1|x|_2 \leqslant |x|_2' \leqslant C_2|x|_2$ pour tout $x \in L$. En remplaçant x par x^n, on en déduit que $C_1^{\frac{1}{n}}|x|_2 \leqslant |x|_2' \leqslant C_2^{\frac{1}{n}}|x|_2$ et en faisant tendre n vers $+\infty$, on obtient $|x|_2 = |x|_2'$ pour tout $x \in L$.

Soit $a \in L^\times$. Comme la norme $|\cdot|_2$ est sous-multiplicative, pour tout $x \in L$, la suite $(|xa^n|_2|a|_2^{-n})$ est décroissante et bornée inférieurement par $|x|_2$. On pose donc, pour $x \in L$,

$$|x|_a \coloneqq \lim_{n\to+\infty} |xa^n|_2|a|_2^{-n}.$$

On vérifie facilement que $|\cdot|_a$ est une norme ultramétrique de K-espace vectoriel sur L. Vérifions par exemple que $x \neq 0$ implique $|x|_a \neq 0$. On a $|a|_a = |a|_2 \neq 0$ et, pour $x, y \in L$,

$$|xy|_a = \lim_{n\to+\infty} |xya^{2n}|_2|a|_2^{-2n} \leqslant |x|_a|y|_a.$$

Ainsi $\{x \in L \mid |x|_a = 0\}$ est un idéal premier de L et donc est réduit à 0. De plus on a, pour $n \geqslant 1$ et $x \in L$,

$$|x^n|_a = \lim_{m\to+\infty} |x^n a^{nm}|_2|a|_2^{-nm} = \lim_{m\to+\infty} |xa^m|_2^n|a|_2^{-nm} = |x|_a^n.$$

On en conclut que $|\cdot|_a = |\cdot|_2$. De plus, on a $|ax|_a = |a|_2|x|_a$ pour tout $x \in L$, et ceci pour tout $a \in L^\times$, on en conclut que $|\cdot|_2$ est multiplicative et est donc le prolongement cherché de $|\cdot|_K$ à L. □

Remarque 2.2.24. Le théorème 2.2.23 reste vrai sans supposer la norme de K ultramétrique. On peut plus précisément démontrer que les seuls corps complets pour une valeur absolue non ultramétrique sont $\mathbb{R}$ et $\mathbb{C}$. Il s'agit d'une conséquence du théorème de Gelfand-Mazur :

Théorème 2.2.25 (Gelfand-Mazur)**.** *Soit A une $\mathbb{R}$-algèbre de Banach qui est un corps. Alors A est de dimension finie sur $\mathbb{R}$.*

Pour une très jolie preuve ce théorème basée sur l'analyse complexe, voir [Rud75, Thm. 18.7]. Une preuve plus élémentaire figure dans [Bou85, Ch. VI §6 Thm. 1].

Corollaire 2.2.26. *Soit $(K, |\cdot|_K)$ un corps valué complet et soit $\overline{K}$ une clôture algébrique de K. Il existe alors une unique valeur absolue sur $\overline{K}$ prolongeant $|\cdot|_K$.*

Exemple 2.2.27. Soit $\overline{\mathbb{Q}_p}$ une clôture algébrique de $\mathbb{Q}_p$. Il existe donc une unique valeur absolue $|\cdot|_p$ sur $\overline{\mathbb{Q}_p}$ prolongeant $|\cdot|_p$. On note $\mathbb{C}_p$ le complété de $\overline{\mathbb{Q}_p}$ pour cette valeur absolue. Il s'agit d'un corps complet ultramétrique dont la valeur absolue est non discrète. En effet, on a $|p^{\frac{1}{n}}|_p = p^{-\frac{1}{n}}$ pour tout $n \geqslant 1$.

2.2.6 Le Lemme de Krasner

Théorème 2.2.28 (Lemme de Krasner)**.** *Soit K un corps valué complet ultramétrique et $\overline{K}$ une clôture algébrique de K. Soient α et β deux éléments de $\overline{K}$ tels que α est séparable sur $K(\beta)$ et tels que*

$$|\alpha - \beta| < \min\{|\alpha - \alpha_i| \mid 2 \leqslant i \leqslant d\}$$

où $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ sont les conjugués distincts de α sur K.

Démonstration. Soit $L/K(\beta)$ l'extension engendrée par tous les conjugués de α. Il s'agit d'une extension galoisienne puisque α est séparable sur $K(\beta)$. On a donc $L^{\mathrm{Gal}(L/K(\beta))} = K(\beta)$. Il suffit donc de prouver que α est fixé par tous les éléments de $\mathrm{Gal}(L/K(\beta))$. Si $\sigma \in \mathrm{Gal}(L/K(\beta))$, l'élément $\sigma(\alpha)$ est l'un des α_i. On a donc

$$\begin{aligned} |\sigma(\alpha) - \alpha| = |\sigma(\alpha) - \beta + \beta - \alpha| &= |\sigma(\alpha) - \sigma(\beta) + \beta - \alpha| \\ &\leqslant \sup\{|\sigma(\alpha - \beta)|, |\beta - \alpha|\} = |\beta - \alpha| \\ &< \min\{|\alpha - \alpha_i| \mid 2 \leqslant i \leqslant dq\}. \end{aligned}$$

On en conclut que $\sigma(\alpha) = \alpha$ et donc que $\alpha \in K(\beta)$. □

Corollaire 2.2.29. *Soit K un corps valué complet ultramétrique et soit P un polynôme irréductible et séparable de degré d. Soit $\|\cdot\|$ une norme de K-espace vectoriel sur l'espace $K_d[X]$ des polynômes de degré inférieur à d. Il existe un réel $\delta > 0$ tel que si $Q \in K_d[X]$ vérifie $\|P - Q\| < \delta$, alors Q est irréductible et séparable et les corps de ruptures de P et Q sont isomorphes.*

Démonstration. On se ramène facilement au cas où P est un polynôme unitaire. On peut alors écrire $P = \prod_{i=1}^{r}(X - \alpha_i)$ où les α_i sont distincts. Posons $\varepsilon := \min\{|\alpha_1 - \alpha_j| \mid 1 < j \leqslant r\}$. Comme $K_d[X]$ est un K-espace vectoriel de dimension finie, les applications K-linéaires $K_d[X] \to K(\alpha_1)$ définies par $Q \mapsto Q(\alpha_1)$ et $\sum_i b_i X^i \mapsto b_d$ sont continues. Il existe donc $\delta > 0$ tel que $\|P - Q\| < \delta$ implique $|Q(\alpha_1)| < \varepsilon^d$ et $|b_d - 1| < \frac{1}{2}$, où b_d désigne le coefficient dominant de Q. Pour un tel polynôme Q, posons $Q = b_d \prod_i (X - \beta_i)$. On a donc $\prod_i |\alpha_1 - \beta_i| < \varepsilon^d$. Il existe donc $1 \leqslant i \leqslant d$ tel que $|\beta_i - \alpha_1| < \varepsilon$. Le Lemme de Krasner implique donc que $K(\alpha_1) \subset K(\beta_i)$. Comme $\deg Q = d$, on a $[K(\beta_i) : K] \leqslant d = [K(\alpha_1) : K]$. En

particulier $K(\beta_i) = K(\alpha_1)$, ce qui implique que le polynôme Q est irréductible et que les corps de ruptures de P et Q sont isomorphes. De plus, puisque P est séparable, il en est de même de Q. □

Exemple 2.2.30. Si p est un nombre premier, le corps $\mathbb{C}_p$ est algébriquement clos. En effet soit $P = \sum_i a_i X^i \in \mathbb{C}_p[X]$ un polynôme irréductible. Soit $d = \deg(P)$. D'après le corollaire 2.2.29, il existe $\delta > 0$ tel que si $|p_i - q_i| < \delta$ pour $0 \leqslant i \leqslant d$, le polynôme $\sum_i q_i X^i$ est irréductible dans $\mathbb{C}_p[X]$. Cependant $\overline{\mathbb{Q}_p}$ est dense dans $\mathbb{C}_p$, on peut donc choisir les q_i dans $\overline{\mathbb{Q}_p}$. Comme $\overline{\mathbb{Q}_p}[X]$ est algébriquement clos, on a nécessairement $d = 1$. Tout polynôme irréductible de $\mathbb{C}_p[X]$ est de degré 1, le corps $\mathbb{C}_p$ est donc algébriquement clos.

2.2.7 Classification des corps locaux

Théorème 2.2.31. *Soit K un corps local. Alors K est isomorphe à l'un des corps valués suivants :*

- *$\mathbb{R}$ ou $\mathbb{C}$ si K n'est pas ultrametrique ;*
- *une extension finie de $\mathbb{Q}_p$ pour p un nombre premier si K est de caractéristique 0 et ultrametrique ;*
- *$k((T))$ où k est un corps fini et K est de caractéristique non nulle.*

Démonstration. Soit $(K, |\cdot|)$ un corps local. Supposons dans un premier temps que K est de caractéristique nulle. Ainsi K contient $\mathbb{Q}$ (il existe un unique plongement de $\mathbb{Q}$ dans K). La restriction de $|\cdot|$ à $\mathbb{Q}$ est non triviale. En effet dans le cas contraire, on sait que $|\cdot|$ est ultramétrique d'après la proposition 2.1.6 et $\mathbb{Q}$ est isomorphe à un sous-corps du corps résiduel de K, ce qui contredit la proposition 2.2.13. Ainsi la restriction de $|\cdot|$ à $\mathbb{Q}$ est une des valeurs absolues $|\cdot|_\infty$, $|\cdot|_p$, p premier d'après le théorème 2.1.12. L'adhérence $\widehat{\mathbb{Q}}$ de $\mathbb{Q}$ dans K est localement compact et non discret, donc un corps local. Alors K est un $\widehat{\mathbb{Q}}$-espace vectoriel localement compact et le théorème de Riesz Theorem (voir TD) implique que K est un $\widehat{\mathbb{Q}}$-espace vectoriel de dimension finie. Si la valeur absolue de K n'est pas ultramétrique, sa restriction à $\mathbb{Q}$ ne l'est pas non (par exemple en utilisant la proposition 2.1.6) et $\widehat{\mathbb{Q}} \simeq \mathbb{R}$ de sorte que K est isomorphe à $\mathbb{R}$ ou $\mathbb{C}$. Si K est ultramétrique, il en est de même de $\widehat{\mathbb{Q}}$ et il existe donc un nombre premier p tel que $\widehat{\mathbb{Q}} \simeq \mathbb{Q}_p$.

Supposons désormais que K est de caracteristique p pour p un nombre premier. Alors K est ultramétrique et le corps résiduel k de K est un corps fini de cardinal q, où q est une puissance de p. On considère le relevé de Teichmüller (exemple 2.2.18) $[\cdot] : k \hookrightarrow K^\times$ que l'on étend à k en posant $[0] = 0$. On a alors $[xy] = [x][y]$

pour tous x et y dans k. On a de plus $[x+y] = [x]+[y]$. En effet, il suffit de vérifier que $[x] + [y] = 0$ quand $x + y = 0$ et une racine $q - 1$-ième de 1 lorsque $x + y \neq 0$. Le premier cas est immédiat car $x = -y$ implique $[x] = [-y] = [-1][y] = -[y]$. Le second cas se déduit de la relation

$$([x] + [y])^q = [x]^q + [y]^q = [x^q] + [y^q] = [x] + [y]$$

valable dans un corps de caractéristique p. On a donc un morphisme de corps $[\cdot] : k \hookrightarrow K$. On choisit une uniformisante π de K et l'on étend ce morphisme en un morphisme de corps $k((T)) \to K$ défini par

$$\sum_{n \geqslant -N} a_n T^n \longmapsto \sum_{n \geqslant -N} [a_n]\pi^n.$$

L'unicité du développement π-adique d'un élément de K (corollaire 2.2.10) montre qu'il s'agit d'un isomorphisme de corps valués. □

Définition 2.2.32. *Soit K un corps local. La* valeur absolue normalisée *de K est l'unique valeur absolue $|\cdot|_K$ continue sur K et telle que*

- *si K est ultramétrique, $|\pi_K|_K = (\mathrm{Card}(k))^{-1}$, où π_K est une uniformisante de K et k son corps résiduel ;*
- *si $K = \mathbb{R}$, $|x|_{\mathbb{R}} = \sup\{x, -x\}$ pour $x \in \mathbb{R}$;*
- *si $K = \mathbb{C}$, $|x|_{\mathbb{C}} = |x\overline{x}|_{\mathbb{R}}$ pour $x \in \mathbb{C}$.*

Remarque 2.2.33. Lorsque $K = \mathbb{C}$, la fonction $|\cdot|_{\mathbb{C}}$ n'est pas une valeur absolue car elle ne vérifie pas l'inégalité triangulaire, cependant $|\cdot|_{\mathbb{C}}^{\frac{1}{2}}$ est une valeur absolue.

Soit K un corps local et soit $|\cdot|_K$ sa valeur absolue normalisée. Soit μ un mesure de Haar le groupe topologique $(K, +)$ dont l'existence est assurée par le théorème B.5.2.

Exemple 2.2.34.
- Si $K = \mathbb{R}$, on peut choisir pour μ la mesure de Lebesgue dx.
- Si $K = \mathbb{C}$, on peut choisir pour μ le produit des mesures de Lebesgue selon les coordonnées, c'est-à-dire la mesure $dx\,dy$ où l'on décompose un élément de $\mathbb{C}$ sous la forme $x + iy$ avec $x, y \in \mathbb{R}$.
- Si K est ultramétrique et si π_K est une unitormisante de K, on vérifie, en utilisant l'invariance de μ par translation, que pour tout $n \in \mathbb{Z}$ et tout $a \in K$, on a $\mu(a + \pi_K^n \mathcal{O}_K) = \mathrm{Card}(k)^{-n}\mu(\mathcal{O}_K)$.

Soit $a \in K^\times$. On déduit des descriptions explicites de l'exemple 2.2.34 que la mesure $A \mapsto \mu(aA)$ est une mesure de Haar pour $(K, +)$ et que $\mu(aA) = |a|_K \mu(A)$ pour toute partie mesurable de K. En particulier la mesure $|\cdot|_K^{-1}\mu$ est une mesure de Haar pour le groupe localement compact $(K^\times, \times)$.

Remarque 2.2.35. Soit L/K une extension finie de corps locaux. Si $|\cdot|_K$ et $|\cdot|_L$ sont les mesures de Haar normalisées de K et L, alors on a $|\cdot|_L = |\cdot|_K N_{L/K}(-)$.

2.3 Ramification dans les corps complets

2.3.1 Extensions

Soit $(K, |\cdot|_K)$ un corps complet ultramétrique pour une valuation discrète non triviale. On note $\mathcal{O}_K$ son anneau de valuation. C'est un anneau de valuation discrète d'après la proposition 1.1.2. C'est donc en particulier un anneau de Dedekind. Soit L/K une extension finie de K. D'après le théorème 2.2.23, il existe une unique valeur absolue $|\cdot|_L$ sur L qui étend $|\cdot|_K$. De plus $(L, |\cdot|_L)$ est complet.

Proposition 2.3.1. *La clôture intégrale de $\mathcal{O}_K$ dans L coïncide avec l'anneau de valuation $\mathcal{O}_L$ de L. De plus $\mathcal{O}_L$ est un $\mathcal{O}_K$-module libre de rang $[L : K]$.*

Démonstration. Soit B la clôture intégrale de $\mathcal{O}_K$ dans L. Montrons dans un premier temps que $\mathcal{O}_K \subset B$. Soit $\widetilde{L}$ une clôture normale de L sur K. L'extension $\widetilde{L}/K$ est finie et, toujours en utilisant le théorème 2.2.23, il existe une unique valeur absolue $|\cdot|_{\widetilde{L}}$ prologeant $|\cdot|_K$ (et $|\cdot|_L$). Si $\sigma \in \mathrm{Aut}_K(\widetilde{L})$, alors $|\sigma(\cdot)|_{\widetilde{L}}$ est une autre extension de $|\cdot|_K$ à $\widetilde{L}$ de sorte que $|\sigma(\cdot)|_{\widetilde{L}} = |\cdot|_{\widetilde{L}}$. Si $x \in L$ et si $P \in K[X]$ est le polynôme minimal de x sur L, alors P est déployé sur $\widetilde{L}$ et, si $x' \in \widetilde{L}$ est une autre racine de P, il existe $\sigma \in \mathrm{Aut}_K(\widetilde{L})$ tel que $\sigma(x) = x'$. On en déduit $|x|_{\widetilde{L}} = |x'|_{\widetilde{L}}$. Ainsi, si $x \in \mathcal{O}_L$, on a $|x'|_{\widetilde{L}} \leqslant 1$ pour toute racine x' de P. Les relations coefficients-racines impliquent donc que les coefficients de P sont des éléments a_i de K tels que $|a_i|_{\widetilde{L}} = |a_i|_K \leqslant 1$. On en déduit que $P \in \mathcal{O}_K[X]$ et donc que x est entier sur $\mathcal{O}_K$.

Comme $\mathcal{O}_L$ est un anneau de valuation discrète, il est donc principal et intégralement clos. Comme L est le corps des fractions de $\mathcal{O}_L$, on doit donc avoir $B = \mathcal{O}_L$.

Montrons à présent que $\mathcal{O}_L$ est un $\mathcal{O}_K$-module de type fini. On fixe une base $(e_1, \ldots, e_d)$ de L sur K. Et on considère la norme associée à cette base :

$$\left\| \sum_{i=1}^{d} x_i e_i \right\|_\infty := \sup_{1 \leqslant i \leqslant d} |x_i|_K.$$

Alors $\|\cdot\|_\infty$ et $|\cdot|_L$ sont deux normes de K-espace vectoriel sur L. On déduit de la proposition 2.2.22 qu'elles sont équivalentes, c'est-à-dire qu'il existe des nombres

réels $0 < C_1 \leqslant C_2$ tels que $C_1\|\cdot\|_\infty \leqslant |\cdot|_L \leqslant C_2\|\cdot\|_\infty$. Soit π une uniformisante de L et $n \geqslant 1$ tel que $|\pi|^n \leqslant C_1$. On en déduit que

$$\mathcal{O}_L = \{x \in L \mid |x|_L \leqslant 1\} \subset \{x \in L \mid \|x\|_\infty \leqslant C_1^{-1}\} = \bigoplus_{i=1}^{d} \mathcal{O}_K \pi^{-n} e_i.$$

Ainsi $\mathcal{O}_L$ est un sous-$\mathcal{O}_K$-module d'un $\mathcal{O}_K$-module de type fini. Comme $\mathcal{O}_K$ est noethérien on en déduit que $\mathcal{O}_L$ est un $\mathcal{O}_K$-module de type fini. La dernière assertion se déduit du fait que $\mathcal{O}_K$ est un anneau principal et de l'isomorphisme $L \simeq K \otimes_{\mathcal{O}_K} \mathcal{O}_L$. □

Si L/K est une extension finie de corps complets, on note $f_{L/K}$ le de degré de l'extension résiduelle k_L/k_K. Si π_K est une uniformisante de K et π_L une uniformisante de L, on note $e_{L/L}$ l'entier tel que $\pi_K \mathcal{O}_L = \pi_L^{e_{L/K}} \mathcal{O}_L$.

Corollaire 2.3.2. *On a* $[L : K] = f_{L/K} e_{L/K}$.

Démonstration. C'est une conséquence de la proposition 1.2.14. En effet l'anneau $\mathcal{O}_K$ est un anneau de valuation discrète, il existe donc un unique idéal premier non nul au-dessus de $\pi_K \mathcal{O}_K$. □

2.3.2 Extensions non ramifiées de corps complets

Soit $(K, |\cdot|_K)$ un corps complet ultramétrique pour une valeur absolue discrète. Soit L/K une extension finie. On suppose que l'extension résiduelle k_L/k_K est séparable.

Proposition 2.3.3. *Il existe une unique sous-extension non ramifiée* K^{nr}/K *de* L/K *de degré* $f_{L/K}$. *Elle contient toutes les sous-extensions non ramifiées de* L/K. *De plus, si l'extension* k_L/k_K *est galoisienne alors l'extension* K'/K *l'est aussi et on a un isomorphisme de groupes de Galois* $\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(k_L/k_L)$.

Démonstration. Comme l'extension k_L/k_K est séparable, le théorème de l'élément primitif implique qu'il existe un polynôme unitaire irréductible $P \in k_K[X]$ tel que $k_L \simeq k_K[X]/(P)$. Soit $\widetilde{P} \in \mathcal{O}_K[X]$ un polynôme unitaire relevant P. Si $\alpha \in k_L$ est une racine de P, cette racine est de multiplicité un et donc $P'(\alpha) \neq 0$. Le corollaire 2.2.17 implique qu'il existe une unique racine $\widetilde{\alpha} \in \mathcal{O}_L$ de $\widetilde{P}$ dont la réduction modulo π_L est α. Soit $K' \coloneqq K(\alpha)$. Alors $[K' : F] = \deg(\widetilde{P}) = \deg(P) = [k_L : k_K]$. De plus l'application $\mathcal{O}_{K'} \subset \mathcal{O}_L \to k_L$ est surjective de sorte que $k_{K'} = k_K$ et donc K'/K est non ramifiée.

Soit $K'' \subset L$ une sous-extension de L/K qui est non ramifiée sur K. Le corps résiduel de $k_{K''}$ de K'' est alors isomorphe à un sous-corps de k_L contenant k_K. Soit $Q \in k_K[X]$ unitaire irréductible tel que $k_{K''} \simeq k_K[X]/(Q)$. On conclut comme précédemment que K'' est engendré par une racine α d'un relevé $\widetilde{Q}$ de Q. Soit $\overline{\alpha}$ l'image de α dans $k_{K''}$. Le corollaire 2.2.17 implique par ailleurs qu'il existe une unique racine $\beta \in K'$ de $\widetilde{Q}$ se réduisant sur $\overline{\alpha}$. Par unicité on a $\beta = \alpha$ et donc $K'' \subset K'$.

Supposons que l'extension k_L/k_K est galoisienne Galois. Ainsi le polynôme P est scindé à racines simples dans $k_L[X]$. On déduit encore du corollaire 2.2.17 que le polynôme $\widetilde{P}$ est scindé à racines simples dans K', ce qui prouve que K'/K est galoisienne. L'isomorphisme entre groupes de Galois est alors une conséquence du théorème 1.2.17. □

Remarque 2.3.4. Si les extensions L/K et k_L/k_K sont toutes deux galoisiennes, alors K^{nr} est le sous-corps de L fixé par le noyau de $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k_K)$.

Corollaire 2.3.5. *Supposons que K est un corps local ultramétrique. Soit $\overline{K}$ une clôture algébrique de K. Pour tout $d \geqslant 1$, il existe un unique sous-corps de $\overline{K}$ non ramifié et de degré d sur K.*

Démonstration. En effet le corps résiduel k_K de K est fini d'après la proposition 2.2.13 et possède donc, à isomorphisme près, une unique extension finie de degré d. □

2.3.3 Extension des valeurs absolues

Soit L/K une extension finie de corps. Soit v une place de K et $|\cdot|_v$ une valeur absolue de la classe v. On note K_v le complété de K pour $|\cdot|_v$ (qui ne dépend que de v). On dit qu'une place w de L est une extension de v à L ou encore au-dessus de v si une valeur absolue de classe w restreinte à K est dans la classe v. On note $w \mid v$. Dans ce cas, l'adhérence de K dans L_w est isomorphe à K_v et fournit un plongement naturel de K_v dans L_w.

D'après la proposition 2.1.6, si $w \mid v$ la place w est ultramétrique si et seulement si v est ultramétrique. De plus, si w et v sont ultramétrique, la place w est discrète (associée à une valeur absolue discrète) si et seulement si la place v est discrète. En effet, on montre facilement que si L est de la forme $K(a)$ et si $|\cdot|_w$ est une valeur absolue de L prolongeant $|\cdot|_v$, le groupe $|L^\times|_w$ est engendré par $|K^\times|_v$ et $|a|_w$, on raisonne alors par récurrence sur le nombre de générateurs de L sur K. Plus précisément, on a

Proposition 2.3.6. *Soit v une place ultramétrique discrète de K. Soit $\mathcal{O}_v$ l'anneau de valuation de v et soit B_v la clôture intégrale de $\mathcal{O}_v$ dans L. Alors l'application $w \mapsto \mathfrak{p}_w := \{x \in L \mid |x|_w < 1\}$ induit une bijection de l'ensemble des places $w \mid v$ de L avec l'ensemble des idéaux maximaux de B_v. De plus la place w contient la valeur absolue associée à la valuation dicrète $v_{\mathfrak{p}_w}$ de L. De plus $\mathcal{O}_w$ coïncide avec la localisation de B_v en $\mathfrak{p}_w$.*

Démonstration. Si $w \mid v$, l'idéal $\mathfrak{p}_w$ est un idéal premier de B_v. Comme B_v est entier sur $\mathcal{O}_v$ et que $\mathfrak{p}_w \cap \mathcal{O}_v$ est un idéal maximal de $\mathcal{O}_v$, on déduit de la proposition A.3.4 que $\mathfrak{p}_w$ est un idéal maximal de B_v. Si $\mathfrak{p}$ est un idéal maximal de B_v, alors $\mathfrak{p} \cap \mathcal{O}_v$ est un idéal maximal de $\mathcal{O}_v$ (toujours par la proposition A.3.4) de sorte que la restriction de $|\cdot|_{\mathfrak{p}}$ à K est dans la place v et $\mathfrak{p}_{|\cdot|_{\mathfrak{p}}} = \mathfrak{p}$. Ainsi l'application $w \mapsto \mathfrak{p}_w$ est surjective. Pour conclure que l'application est injective, il suffit donc de prouver que si $w \mid v$ et $|\cdot|_w$ est une valeur absolue de la place w, les valeurs absolues $|\cdot|_{\mathfrak{p}_w}$ et $|\cdot|_w$ sont équivalentes. Notons $\mathcal{O}_w$ l'anneau de valaution de w. Remarquons que $B_v \subset \mathcal{O}_w$. En effet, l'anneau $\mathcal{O}_w$ est un anneau intégralement clos contenant $\mathcal{O}_v$, il contient donc B_v. De plus les éléments de $B_v \smallsetminus \mathfrak{p}_w$ sont inversibles dans $\mathcal{O}_w$, on a donc $(B_v)_{\mathfrak{p}_w} \subset \mathcal{O}_w$. On conclut que $(B_v)_{\mathfrak{p}_w} = \mathcal{O}_w$ au moyen du lemme ci-dessous. Ainsi les normes $|\cdot|_{\mathfrak{p}_w}$ et $|\cdot|_w$ ont les mêmes boules unités, elles sont donc équivalentes. □

Lemme 2.3.7. *Soit K un corps et soit $A \subset B$ deux sous-anneaux de valuation discrète de K d'idéaux maximaux $\mathfrak{m}_A$ et $\mathfrak{m}_B$ tels que $\mathrm{Frac}(A) = \mathrm{Frac}(B) = K$ et $\mathfrak{m}_A \subset \mathfrak{m}_B \cap A$. Alors $A = B$.*

Démonstration. Soient $\mathfrak{m}_A$ et $\mathfrak{m}_B$ les anneaux de valuations discrètes de A et B. Pour $x \in K^\times$, on a $x \notin A \Leftrightarrow x^{-1} \in \mathfrak{m}_A$ et idem pour B. Donc si $x \notin A$, alors $x^{-1} \in \mathfrak{m}_A \subset \mathfrak{m}_B$, donc $x \notin B$. □

Corollaire 2.3.8. *Soit K un corps de nombres. L'application $\mathfrak{p} \mapsto |\cdot|_{\mathfrak{p}}$ induit une bijection de l'ensemble des idéaux maximaux de $\mathcal{O}_K$ sur l'ensemble des places ultramétriques de K.*

Théorème 2.3.9. *Soit L/K une extension finie et soit v une place de K.*

(i) La place v admet au plus $[L : K]$ extensions distinctes à L : $w_1, \ldots, w_g$.

(ii) Il existe un morphisme surjectif de (L, K_v)-algèbres

$$f : L \otimes_K K_v \twoheadrightarrow \prod_{i=1}^{g} L_{w_i}.$$

(iii) Si $w \mid v$, alors L_w est un K_v-espace vectoriel de dimension finie. Si de plus, v est ultramétrique discrète, alors $e_{\mathfrak{q}_w/\mathfrak{p}_v} = e_{L_w/K_v}$ et $f_{\mathfrak{q}_w/\mathfrak{p}_v} = f_{L_w/K_v}$.

(iv) Si l'extension K est un corps global, alors f est un isomorphisme et

$$[L : K] = \sum_{i=1}^{g} [L_{w_i} : K_v].$$

Démonstration. L'anneau $A \coloneqq L \otimes_K K_v$ est une K_v-algèbre de dimension finie. En particulier ses idéaux premiers sont maximaux. D'après la proposition A.5.1 ses idéaux sont en nombre fini. Notons les $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ et l'application naturelle

$$f : A \twoheadrightarrow \prod_{i=1}^{g} A/\mathfrak{p}_i$$

est surjective. Ainsi $r \leqslant \dim_{K_v} A = [L : K]$. Posons $L_i \coloneqq A/\mathfrak{p}_i$ pour $1 \leqslant i \leqslant g$. On le munit de la structure de K_v-algèbre fournie par f.

Montrons que pour tout $1 \leqslant i \leqslant r$, L est dense dans L_i. Les K_v-algèbres A et L_i sont de dimension finie et l'application f est K_v-linéaire. Comme K_v est complet, elle est nécessairement continue. Le choix d'une base de L sur K permet d'identifier L à K^d et A à K_v^d. L'image de L dans A par l'application $x \mapsto x \otimes 1$ s'identifie alors à K^d dans K_v^d et est donc une partie dense de A. Comme l'application f est surjective, l'image de L dans $\prod_i L_i$ est dense et en particulier l'image de L dans L_i est dense. On utilise cette application pour identifier L à un sous-corps dense de L_i. Comme L_i est une extension finie de K_v, il est muni d'une unique classe d'équivalence de valeurs absolues induisant la classe d'équivalence de $|\cdot|_v$ sur K_v. Ces normes induisent donc une place w_i sur L qui prolonge v et telle que $L_{w_i} \simeq L_i$.

Montrons que les places $w_1, \ldots, w_r$ sont distinctes. Supposons au contraire qu'il existe $1 \leqslant i \neq j \leqslant r$ tels que $w_i = w_j$. Cela signifie qu'il existe un isomorphisme de corps $\alpha : L_i \simeq L_j$ qui est à la fois L-linéaire et K_v-linéaire. Notons $p_{i,j}$ la projection de A sur $L_i \times L_j$. On a donc $p_{i,j}(L) \subset \{(x, y) \in L_i \times L_j \mid \alpha(x) = y\}$. Il s'agit d'un sous-$K_v$-espace vectoriel, donc fermé de sorte que $p_{i,j}(A) \subset \{(x, y) \in L_i \times L_j \mid \alpha(x) = y\}$. Ceci contredit la surjectivité de $p_{i,j}$.

Montrons que toute place de L au-dessus de v est l'une des w_i. Soit w une telle place. L'injection de L dans L_w ainsi que le plongement $K_v \hookrightarrow L_w$ induisent un morphisme de K-algèbres $A = L \otimes_K K_v \to L_w$. Le noyau de ce morphisme est un idéal premier de A, il induit donc un morphisme $A \twoheadrightarrow L_i \hookrightarrow L_w$. En composant ce dernier avec l'inclusion de L dans A, on en déduit une suite de morphismes

$$L \hookrightarrow L_i \hookrightarrow L_w.$$

Comme $w \mid v$, la norme de L_w induit donc l'unique place de L_i compatible à la topologie de K_v, on en conclut que la topologie de L_i est induite par celle de L_w. Comme L_i est complet, il est fermé dans L_w. Comme L est dense dans L_w, on en

conclut que $L_i \simeq L_w$ comme corps topologiques et donc que $w = w_i$. On a donc prouvé les assertions (i) et (ii).

Le point (iii) s'en déduit, en effet on a déjà prouvé que L_w est de dimension finie sur K_v et le résultat concernant l'indice de ramification et le degré résiduel se déduit de la proposition 2.3.6.

Il reste à prouver (iv). Commençon par traiter le cas où l'extension L/K est séparable. Dans ce cas il existe donc un polynôme $P \in K[X]$ irréductible et séparable tel que $L \simeq K[X]/(P)$. On a donc $L \otimes_K K_v \simeq K_v[X]/(P)$. Comme P est également séparable dans $K_v[X]$, on en déduit que $A = L \otimes_K K_v$ est isomorphe à un produit de corps et ne contient donc pas d'éléments nilpotents non nuls. Or le noyau du morphisme f est l'intersection des idéaux premiers de A, c'est-à-dire l'ensemble des éléments nilpotents de A. On en conclut que f est injectif. Le reste suit. Il reste à traiter le cas où K est un corps global. Comme le cas des extensions séparables a déjà été traité, on peut supposer que K est une extension finie de $\mathbb{F}_p(T)$. D'après le lemme 2.3.10 ci-dessous, la clôture intégrale dans L de l'anneau de valuation $\mathcal{O}_v$ de v est un $\mathcal{O}_v$-module de type fini. On déduit des points (ii), (iii) et du corollaire 2.3.2 que

$$\sum_{w|v} [L_w : K_v] = \sum_{w|v} e_{\mathfrak{p}_q/\mathfrak{p}_v} f_{\mathfrak{p}_w/\mathfrak{p}_v} \leqslant [L : K].$$

Cependant cette inégalité est une égalité lorsque K est de caractéristique zéro ou une extension finie de $\mathbb{F}_p(T)$ (voir le théorème 1.2.4 et la proposition 1.2.14). □

Lemme 2.3.10. *Soit K une extension finie de $\mathbb{F}_p(T)$ et soit L une extension finie de K. Soit v une place de K et $\mathcal{O}_v \subset K$ sont anneau de valuation. Alors la clôture intégrale de $\mathcal{O}_v$ dans L est un $\mathcal{O}_v$-module de type fini.*

Démonstration. Soit v_0 l'uniquee place de $\mathbb{F}_p(T)$ au-dessous de v, c'est la classe d'équivalence de la restriction à $\mathbb{F}_p(T)$ d'une valeur absolue de classe v. Quitte à remplacer T par T^{-1}, le théorème 2.1.11 implique que l'on peut supposer que $\mathbb{F}_p[T]$ est contenu dans l'anneau de valuation $\mathcal{O}_{v_0}$ de v_0. Soit A la clôture intégrale de $\mathbb{F}_p[T]$ dans K et B la clôture intégrale de $\mathbb{F}_p[T]$ dans L, qui coïncide également avec la clôture intégrale de A dans L. Notons C la clôture intégrale de $\mathcal{O}_v$ dans L. Notons $\mathfrak{p}_v \subset A$ l'idéal maximal correspondant à v. Alors C coïncide avec le localisé de B en $A \smallsetminus \mathfrak{p}_v$. D'après le théorème 1.2.4, le $\mathbb{F}_p[T]$-module B est de type fini, c'est donc en particulier un A-module de type fini. Ainsi C est un $\mathcal{O}_v$-module de type fini. □

2.3.4 La formule du produit

Si K est un corps local et si v est une place de K, on note $|\cdot|_v$ l'unique valeur absolue de K correspondant à v.

Proposition 2.3.11. *Soit L/K une extension finie de corps globaux. Soit $x \in L$ et soit v une place de K. On a alors*

$$|N_{L/K}(x)|_v = \prod_{w|v} |N_{L_w/K_v}(x)| = \prod_{w|v} |x|_w.$$

Démonstration. Par définition $N_{L/K}x$ est le déterminant de l'automorphisme K-linéaire de L défini par $y \mapsto xy$. Après extension des scalaires, c'est aussi déterminant de l'automorphisme K_v-linéaire de $L \otimes_K K_v$ défini par $y \mapsto (x \otimes 1)y$. On déduit alors du théorème 2.3.9 (iv) l'isomorphisme $L \otimes_K K_v \simeq \prod_{w|v} L_w$ et donc

$$|N_{L/K}(x)|_v = \prod_{w|v} |N_{L_w/K_v}(x)|_v = \prod_{w|v} |x|_w. \qquad \square$$

Théorème 2.3.12 (Formule du produit)**.** *Soit K un corps global et soit $x \in K^\times$.*

(i) On a $|x|_v = 1$ pour presque toute place v (c'est-à-dire pour tout place sauf un nombre fini).

(ii) On a $\prod_v |x|_v = 1$.

Démonstration. Démontrons dans un premier temps le lemme suivant.

Lemme 2.3.13. *Soit $x \in K$. Alors $|x|_v \leqslant 1$ pour presque toute place v.*

Démonstration. Commençons par démontrer le cas où K est un corps de nombres. Soit $x \in K$. Comme $K \simeq \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}$, il existe un entier non nul m tel que $mx \in \mathcal{O}_K$. Soit v une place ultramétrique de K. Elle domine une place ultramétrique de $\mathbb{Q}$ correspondant à un nombre premier p. Comme $|\mathbb{Z}|_p \leqslant 1$ et comme les éléments de $\mathcal{O}_K$ sont entiers sur $\mathbb{Z}$, on a $|\mathcal{O}_K|_v \leqslant 1$. Ainsi $|m|_p = 1$ pour presque tout nombre premier p et il n'y a donc qu'un nombre fini de places v de K telle que $|m|_v \neq 1$. Comme il n'y a qu'un nombre fini de places archimédienne de K, on a bien $|x|_v \leqslant 1$ pour presque tout v.

Le cas des corps de fonctions est similaire si l'on remplace $\mathbb{Q}$ par $k(T)$ et $\mathbb{Z}$ par $k[T]$ où k est un corps fini. En effet il n'existe qu'un nombre fini de places v de K telles que $|k[T]|_v \leqslant 1$. $\square$

Le lemme implique immédiatement le point (i) du théorème. En effet, on peut appliquer le lemme à x et x^{-1}.

Démontrons le point (ii). Remarquons que si K/K_0 est une extension finie de corps globaux la proposition 2.3.11 et la formule du produit pour K_0 impliquent la formule du produit pour K. En effet, on a alors, pour $x \in L^\times$,

$$\prod_w |x|_w = \prod_v \prod_{w|v} |x|_w = \prod_v |N_{L/K} x|_v = 1$$

puisque $N_{L/K}(x) \in K^\times$. Si K est un corps de nombres, il suffit de prouver la formule pour $K = \mathbb{Q}$. Si $x \in \mathbb{Q}^\times$, on peut écrire $x = \pm \prod_p p^{\alpha_p}$. On a alors $|x|_\infty = \prod_p p^{\alpha_p}$ et $|x|_p = p^{-\alpha_p}$, on conclut immédiatement.

Si K est un corps de fonctions, il suffit de traiter le cas où $K = k(T)$ avec $k = \mathbb{F}_q$. Les places de $k(T)$ sont indexées par les polynômes irréductibles P de $\mathbb{F}_q[T]$ et par T^{-1}. Soit $x = \varepsilon \prod_P P^{\alpha_P} \in k(T)^\times$ avec $\varepsilon \in k^\times$. Comme $\mathbb{F}_q[T]/(P) \simeq \mathbb{F}_{q^{\deg P}}$, on a $|x|_P = q^{-\alpha_P \deg P}$. De plus $|x|_{T^{-1}} = q^{\deg x}$ de sorte que

$$|x|_{T^{-1}} \prod_P |x|_P = 1. \qquad \square$$

2.3.5 Places archimédiennes des corps de nombres

Soit K un corps de nombres. Il s'agit d'une extension finie de $\mathbb{Q}$. Notons d son degré. L'entier d est également le nombre de plongements de K dans $\mathbb{C}$. Rappelons (§1.2.3) qu'un tel plongement est dit *réel* si son image est incluse dans $\mathbb{R}$ et *complexe* dans le cas contraire. Le groupe de Galois $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ agit par composition sur l'ensemble de ces plongements et les points fixes sont exactement les plongements réels. Notons r_1 le nombre de plongements réels et r_2 le nombre d'orbites de plongements complexes. On a donc $d = r_1 + 2r_2$. Si j est un plongement $K \hookrightarrow \mathbb{C}$, on note $\overline{j}$ le composé de j avec la conjugaison complexe. Soit $j_1, \ldots, j_{r_1}$ les plongements réels K dans $\mathbb{C}$ et $j_{r_1+1}, \overline{j_{r_1+1}}, \ldots, j_{r_1+r_2}, \overline{j_{r_1+r_2}}$ les plongements complexes.

Si $j : K \hookrightarrow \mathbb{C}$, alors l'application $z \mapsto |j(z)| = (j(z)\overline{j(z)})^{\frac{1}{2}}$ est une valeur absolue archimédienne (c'est-à-dire non ultramétrique) sur K.

Théorème 2.3.14. *Les places archimédiennes de K sont exactement les classes d'équivalence des valeurs absolues suivantes*

$$x \mapsto |j_k(x)|_{\mathbb{C}}, \quad k = 1, \ldots, r_1 + r_2.$$

Démonstration. Soit j le plongement diagonal $K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ défini par $x \mapsto (j_1(x), \ldots, j_{r_1+r_2}(x))$. Il induit un morphisme de $(K, \mathbb{R})$-algèbres $K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. D'après le théorème 2.3.9, il suffit de prouver que ce morphisme est un isomorphisme. Comme $\mathbb{C}$ est un $\mathbb{R}$-module fidèlement plat, il suffit de le faire après

changement de base de $\mathbb{R}$ à $\mathbb{C}$. Considérons l'application

$$K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{j\otimes 1} \mathbb{C}^{r_1} \times (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C})^{r_2} \simeq \mathbb{C}^{r_1} \times \mathbb{C}^{2r_2} = \mathbb{C}^d.$$

Elle est donnée par $x \otimes 1 \mapsto (\sigma(x))_{\sigma:K\hookrightarrow\mathbb{C}}$. Ainsi il suffit de vérifier que pour une $\mathbb{Q}$-base $(e_1, \ldots, e_d)$ de K, les images des éléments $e_i \otimes 1$ forment une $\mathbb{C}$-base de $\mathbb{C}^d$, c'est-à-dire tels que la matrice $(\sigma(e_i))$ de taille $d \times d$ est inversible. C'est une conséquence directe du fait que les applications σ forment une famille $\mathbb{C}$-libre d'applications de K vers $\mathbb{C}$ (en utilisant par exemple l'indépendance linéaire des caractères de $K^\times$). □

2.3.6 Calcul locale de la différente

Soit L/K une extension finie séparable de corps. Soit A un anneau de Dedekind de corps des fractions K et soit B la clôture intégrale de A dans L. Soit $\mathfrak{p}$ un idéal maximal de A et soit $\mathfrak{q}$ un idéal maximal de B au-dessus de A. On note $K_\mathfrak{p}$ le complété de K pour la place définie par $\mathfrak{p}$ et $L_\mathfrak{q}$ le complété de L pour la place définie par $\mathfrak{q}$. D'après le théorème 2.3.9, l'extension $L_\mathfrak{q}/K_\mathfrak{p}$ est finie. De plus si $\mathcal{O}_\mathfrak{p}$ désigne l'anneau de valuation de $K_\mathfrak{p}$ et $\mathcal{O}_\mathfrak{q}$ l'anneau de valuation de $L_\mathfrak{q}$, alors $\mathcal{O}_\mathfrak{q}$ est la clôture intégrale de $\mathcal{O}_\mathfrak{p}$ dans $L_\mathfrak{q}$ et l'extension $L_\mathfrak{q}/K_\mathfrak{p}$ est séparable.

Lemme 2.3.15. *L'application naturelle $B \otimes_A \mathcal{O}_\mathfrak{p} \to \prod_{\mathfrak{q}|\mathfrak{p}} \mathcal{O}_\mathfrak{q}$ est un isomorphisme de $\mathcal{O}_\mathfrak{p}$-modules.*

Démonstration. D'après le théorème 2.3.9, cette application est un isomorphisme après tensorisation avec $K_\mathfrak{p}$ (c'est-à-dire application de $-\otimes_{\mathcal{O}_\mathfrak{p}} K_\mathfrak{p}$). Comme B est un A-module projectif de type fini (voir remarque 1.2.5), le terme de gauche $B \otimes_A \mathcal{O}_\mathfrak{p}$ est un $\mathcal{O}_\mathfrak{p}$-module projectif de type fini. Comme $\mathcal{O}_\mathfrak{p}$ est un anneau de valuation discrète (en particulier principal), c'est en fait un $\mathcal{O}_\mathfrak{p}$-module libre. De même, le terme de droite est un $\mathcal{O}_\mathfrak{p}$-module libre (voir la proposition 2.3.1). Ainsi le morphisme considéré est un morphisme entre $\mathcal{O}_\mathfrak{p}$-modules libres de type fini qui devient un isomorphisme après tensorisation avec $K_\mathfrak{p}$. Il s'agit donc d'un morphisme injectif entre $\mathcal{O}_\mathfrak{p}$-modules de même rang. Le théorème de structure des $\mathcal{O}_\mathfrak{p}$-modules de type fini (ou le lemme de Nakayama) implique qu'il suffit de vérifier que le morphisme est surjectif après tensorisation avec $k_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$. Comme $\mathfrak{p}$ est un idéal maximal de A, on a

$$(B \otimes_A \mathcal{O}_\mathfrak{p}) \otimes_{\mathcal{O}_\mathfrak{p}} k_\mathfrak{p} \simeq B \otimes_A (\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}) \simeq B \otimes_A (A/\mathfrak{p}) \simeq B/\mathfrak{p}B.$$

Les idéaux maximaux de $B/\mathfrak{p}B$ sont en bijection avec les idéaux maximaux de B contenant $\mathfrak{p}$, on déduit donc du lemme A.4.4 que l'application $B/\mathfrak{p}B \twoheadrightarrow \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}$ est surjective. Comme par ailleurs $\mathcal{O}_\mathfrak{q}/\mathfrak{q}\mathcal{O}_\mathfrak{q} \simeq B/\mathfrak{q}$ pour $\mathfrak{q} \mid \mathfrak{p}$, on en déduit le résultat. □

Proposition 2.3.16. *La différente $\mathcal{D}_{\mathcal{O}_\mathfrak{q}/\mathcal{O}_\mathfrak{p}}$ est l'idéal de $\mathcal{O}_\mathfrak{q}$ engendré par $\mathcal{D}_{B/A}$.*

Démonstration. On montre que $\mathcal{D}_{B/A}^{-1} \otimes_A \mathcal{O}_\mathfrak{p} = \{x \in L \otimes_K K_\mathfrak{p} \mid (\mathrm{Tr}_{L/K} \otimes \mathrm{Id}_{K_\mathfrak{p}})(x) \subset B \otimes_A \mathcal{O}_\mathfrak{p}\}$. Comme $\mathrm{Tr}_{L/K} \otimes \mathrm{Id}_\mathfrak{p} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathrm{Tr}_{L_\mathfrak{q}/K_\mathfrak{p}}$ sous l'isomorphisme $L \otimes_K K_\mathfrak{p}$, on en conclut que $\mathcal{D}_{L/K}^{-1} \otimes_A \mathcal{O}_\mathfrak{p} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} \mathcal{D}_{\mathcal{O}_\mathfrak{q}/\mathcal{O}_\mathfrak{p}}^{-1}$. D'où le résultat. □

Corollaire 2.3.17. *L'idéal de $\mathcal{O}_\mathfrak{p}$ engendré par le discriminant $\Delta_{B/A}$ est le produit des idéaux discriminants $\Delta_{\mathcal{O}_\mathfrak{q}/\mathcal{O}_\mathfrak{p}}$ pour $\mathfrak{q} \mid \mathfrak{p}$.*

Chapitre 3

Adèles et idèles

3.1 Adèles

3.1.1 Produits restreints de groupes topologiques

Soit Σ un ensemble et soit Σ_∞ une partie finie de Σ. Pour tout élément $v \in \Sigma$, on fixe un groupe localement compact G_v, et, si $v \notin \Sigma_\infty$ un sous-groupe ouvert et compact $K_v \subset G_v$.

Définition 3.1.1. *Le* produit restreint *de la famille $(G_v)_{v\in\Sigma}$ (relativement à la famille des $(K_v)_{v\notin\Sigma_\infty}$) est l'ensemble*

$$\prod_{v\in\Sigma}{}' G_v \coloneqq \{(g_v) \in \prod_{v\in\Sigma} \mid g_v \in K_v \text{ pp}(v)\}$$

où la notation pp(v) *signifie "pour tout sauf un nombre fini de v".*

Remarquons tout de suite que $G \coloneqq \prod'_{v\in\Sigma} G_v$ est un sous-groupe du groupe produit $\prod_{v\in\Sigma} G_v$.

Définissons une topologie sur $G = \prod'_{v\in\Sigma} G_v$. Soit $\mathcal{B}$ l'ensemble des parties de G de la forme

$$U_S \times \prod_{v\notin S} K_v$$

où S est une partie finie de Σ contenant Σ_∞ et U_S un voisinage ouvert de l'élément neutre de $\prod_{v\in S} G_v$ pour la topologie produit.

Lemme 3.1.2. *L'ensemble $\mathcal{B}$ vérifie les conditions du lemme B.3.1.*

Démonstration. Si U^1 et U^2 sont deux éléments de $\mathcal{B}$, on peut écrire, pour $i \in \{1,2\}$, $U^i = U_i \times \prod_{v\notin S_i} K_v$ où S_i est une partie finie de Σ contenant Σ_∞ et U_i est un ouvert de $\prod_{v\in S_i} G_v$ contenant l'élément neutre. Quitte à rétrécir U_i, on peut supposer que $U_i \subset \prod_{v\in\Sigma_\infty} G_v \times \prod_{v\in S_i\smallsetminus\Sigma_\infty} K_v$. Posons $S = S_1 \cup S_2$, $U_3 = (U_1 \times \prod_{v\in S_2\smallsetminus S_1} K_v) \cap (U_2 \times \prod_{v\in S_1\smallsetminus S_2} K_v)$ et $U^3 = U_3 \times \prod_{v\notin S} K_v$. On a alors $U^3 \in \mathcal{B}$ et $U^3 \subset U^1 \cap U^2$, ce qui prouve (i). La propriété (ii) se déduit facilement du fait que $\prod_{v\in S} G_v$ est un groupe topologique pour toute partie finie S de Σ. Vérifions la propriété (iii). Si $U_S \times \prod_{v\notin S} K_v \in \mathcal{B}$ et $g = (g_v) \in G$. Soit S' une partie finie de Σ contenant S et telle que $g_v \in K_v$ si $v \notin S'$. Soit $W_{S'}$ un ouvert de $\prod_{v\in S'} G_v$ tel que $gW_{S'}g^{-1} \subset U_S \times \prod_{v\in S'\smallsetminus S} K_v$. On a alors, en posant $W = W_{S'} \times \prod_{v\notin S'} K_v$, $gWg^{-1} \subset V$ et $W \in \mathcal{B}$. □

On déduit donc du lemme B.3.1 et du lemme 3.1.2 qu'il existe une unique topologie sur G pour laquelle G est un groupe topologique sur G et $\mathcal{B}$ est une base de voisinages de l'élément neutre. On munit G de cette topologie.

Lemme 3.1.3. *Le groupe G est un groupe topologique localement compact.*

Démonstration. L'inclusion de G dans $\prod_v G_v$ est continue. Comme les groupes G_v sont localement compacts, et en particulier séparés, le produit $\prod_v G_v$ est séparé, il en est donc de même de G. De plus si U est un voisinage compact de l'élément neutre dans le groupe localement compact $\prod_{v\in\Sigma\infty} G_v$, alors $g(U \times \prod_{v\notin\Sigma_\infty} K_v$ est un voisinage compact de g dans G pour tout $g \in G$. Ainsi G est localement compact. □

3.1.2 Adèles

Soit F un corps global et soit Σ l'ensemble de ses places. Soit Σ_∞ l'ensemble de ses places archimédiennes. Si $v \in \Sigma$, on note F_v le complété de F en v et, si $v \notin \Sigma_\infty$, $\mathcal{O}_v \subset F_v$ son anneau de valuation et $\mathfrak{p}_v \subset \mathcal{O}_v$ son idéal maximal. De plus, on note $|\cdot|_v$ la valeur absolue normalisée sur F associée à la place v.

Définition 3.1.4. *Le groupe des* adeles *est le produit restreint des groupes topologiques additifs $(F_v)_{v\in\Sigma}$ relativement à la famille des sous-groupes compacts ouverts $(\mathcal{O}_v)_{v\notin\Sigma_\infty}$. On le note*

$$\mathbb{A}_F := \prod_{v\in\Sigma}{}' F_v.$$

Le groupe $\mathbb{A}_F$ est donc un groupe abélien localement compact (par le lemme 3.1.3). On vérifie facilement que la multiplication est une application continue de $\mathbb{A}_F \times \mathbb{A}_F$ vers $\mathbb{A}_F$ de sorte qu'il possède en fait une structure d'anneau topologique.

Le plongement diagonal de F dans $\mathbb{A}_F$ est un morphisme d'anneaux défini par $\xi \mapsto (\xi)_{v\in\Sigma}$. On utilise ce plongement pour identifier F à un sous-anneau de $\mathbb{A}_F$.

Théorème 3.1.5. *Le sous-anneau $F \subset \mathbb{A}_F$ est discret et le groupe quotient $\mathbb{A}_F/F$ est compact.*

Démonstration. Commençons par prouver que F est une partie discrète de $\mathbb{A}_F$. Soit $v_0 \in \Sigma$ et soit $0 < r < 1$. Considérons le voisinage de 0 suivant

$$V \coloneqq \{(x_v)_v \in \mathbb{A}_F \mid |x_{v_0}|_{v_0} < r,\ |x_v|_v \leqslant 1 \text{ if } v \neq v_0\}.$$

Soit $x \in F \cap V$. On a alors $\prod_v |x_v| < r < 1$ de sorte que la formule du produit (théorème 2.3.12) implique $x = 0$. Ainsi $F \cap V = \{0\}$ et F est discret dans $\mathbb{A}_F$ par le lemme B.3.8.

Pour démontrer la compacité de $\mathbb{A}_F/F$, nous allons séparer les cas des corps de nombres et des corps de fonctions. Let $F_\infty \coloneqq \prod_{v|\infty} F_v = F \otimes_{\mathbb{Q}} \mathbb{R}$.

Nous allons utiliser le résultat suivant.

Lemme 3.1.6. *Soit A un anneau de Dedekind et soient $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ des idéaux premiers non nuls distincts de A. Pour $1 \leqslant i \leqslant r$ soit $x_i \in \mathcal{O}_{\mathfrak{p}_i}$ un élément de l'anneau de valuation du corps $F_{\mathfrak{p}_i}$, complété de F pour la place associée à $\mathfrak{p}_i$ et soit $n_i \geqslant 1$ un entier. Il existe alors $\xi \in A$ tel que $v_{\mathfrak{p}_i}(\xi - x_i) \geqslant n_i$ pour tout $1 \leqslant i \leqslant r$.*

Démonstration. Notons que pour tout $1 \leqslant i \leqslant r$, l'application $A/\mathfrak{p}_i^{n_i} \to \mathcal{O}_{\mathfrak{p}_i}/\mathfrak{p}_i^{n_i}\mathcal{O}_{\mathfrak{p}_i}$ est un isomorphisme d'après la proposition 2.2.8 et le lemme A.2.3. Il suffit donc de prouver que l'application diagonale $A \to \prod_{i=1}^r A/\mathfrak{p}_i^{n_i}$ est surjective, ce qui est une conséquence du lemme A.4.4. □

Supposons que F est une extension finie d'un corps global F_0. Supposons de plus qu'il existe un anneau de Dedekind A tel que $\mathrm{Frac}(A) = F_0$ et une place v_0 de F_0 tels que l'ensemble des places de F_0 soit v_0 et les places associées aux idéaux maximaux de A. Si $F_0 = \mathbb{Q}$, on peut prendre $A = \mathbb{Z}$ et $v_0 = \infty$ tandis que si $F_0 = \mathbb{F}_p(T)$, on peut prendre $A = \mathbb{F}_p[T]$ et $v_0 = |\cdot|_{T^{-1}}$. On note $F_{v_0} \coloneqq F \otimes_{F_0} F_{0,v_0}$.

Lemme 3.1.7. *On a $\mathbb{A}_F = F + F_0 \times \prod_{v\nmid v_0} \mathcal{O}_v$.*

Démonstration. Soit $x = (x_v)_v \in \mathbb{A}_F$. En utilisant le lemme 2.3.13, on voit qu'il exisye un élément non nul $m \in A$ tel que $mx_v \in \mathcal{O}_v$ pour tout $v \nmid v_0$. Choisissons $0 < \varepsilon_v < |m|_v^{-1}$ pour tout v tel que $|m|_v < 1$ (qui sont en nombres finis d'après le théorème 2.3.12). Le lemme 3.1.6 fournit l'existence de $\xi \in \mathcal{O}_F$ tel que $|mx_v - \xi| < \varepsilon_v$ pour v tel que $|m|_v < 1$. On a alors $|x_v - \frac{\xi}{m}|_v \leqslant 1$ pour tout $v \nmid v_0$ de sorte que $x = \frac{\xi}{m} + y$ avec $\frac{\xi}{m} \in F$ et $y \in F_{v_0} \times \prod_{v\nmid v_0} \mathcal{O}_v$. □

Supposons désormais que F est un corps de nombres.

Lemme 3.1.8. *On a* $F \cap F_\infty \times \prod_{v\nmid\infty} \mathcal{O}_v = \mathcal{O}_F$.

Démonstration. C'est clair : si $\xi \in F$ est tel que $|\xi|_\mathfrak{p} \leqslant 1$ pour tous les idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_F$, alors $\xi \in \mathcal{O}_F$. □

Les lemmes 3.1.7 et 3.1.8 impliquent que l'inclusion $F_\infty \times \prod_{v\nmid\infty} \mathcal{O}_v \subset \mathbb{A}_F$ induit un isomorphisme de groupes

$$(F_\infty \times \prod_{v\nmid\infty} \mathcal{O}_v)/\mathcal{O}_F \xrightarrow{\sim} \mathbb{A}_F/F.$$

Il existe une $\mathbb{Z}$-base $(e_1, \dots, e_d)$ de $\mathcal{O}_F$ qui est également une $\mathbb{Q}$-base de F. Ceci implique que $(e_1 \otimes 1, \dots, e_d \otimes 1)$ est une $\mathbb{R}$-base du $\mathbb{R}$-espace vectoriel $F_\infty = F \otimes_\mathbb{Q} \mathbb{R}$. Soit

$$Q \coloneqq \left\{ \sum_{i=1}^{d} t_i (e_i \otimes 1) \mid 0 \leqslant t_i \leqslant 1 \right\}.$$

L'inclusion $Q \subset F_\infty$ induit une application continue et surjective $Q \twoheadrightarrow F_\infty/\mathcal{O}_F$. Ainsi l'application $Q \times \prod_{v\nmid\infty} \mathcal{O}_v \to (F_\infty \times \prod_{v\nmid\infty} \mathcal{O}_v)/\mathcal{O}_F$ est surjective. On en déduit que l'application composée $Q \times \prod_{v\nmid\infty} \mathcal{O}_v \to \mathbb{A}_F \twoheadrightarrow \mathbb{A}_F/F$ est surjective et continue. Comme $Q \times \prod_{v\nmid\infty} \mathcal{O}_v$ est compact, il en est de même de $\mathbb{A}_F/F$.

Supposons désormais que F est un corps de fonctions, $F_0 = \mathbb{F}_p(T)$ et v_0 est la place associée à $|\cdot|_{T^{-1}}$. On peut améliorer le lemme 3.1.7.

Lemme 3.1.9. *On a* $\mathbb{A}_F = F + \prod_{v\in\Sigma} \mathcal{O}_v$.

Démonstration. Soit $x = (x_v)_v \in \mathbb{A}_F$. D'après le lemme 3.1.7, il existe $\xi \in F$ tel que $x_v - \xi \in \mathcal{O}_v$ si $v \nmid v_0$. Considérons $y = (y_v)_{v|v_0} = (x_v - \xi)_{v|v_0}$. Comme $F \otimes_{F_0} F_{0,v_0} \simeq B \otimes_A F_{0,v_0} \simeq \prod_{|v_0} F_v$ où $A = \mathbb{F}_p[T]$ et B est la clôture intégrale de A dans F. Si $(e_1, \dots, e_n)$ est une A-base de B, on peut donc écrire $y = \sum_{i=1}^n e_i \otimes y_i$ avec $y_i \in F_{0,v_0}$. Comme $F_{0,v_0} = \mathbb{F}_p((T^{-1}))$, on peut écrire $y_i = \zeta_i + z_i$ avec $\zeta_i \in A = \mathbb{F}_p[T]$ et $z_i \in \mathcal{O}_{F_{0,v_0}} = \mathbb{F}_p[\![T^{-1}]\!]$. On a donc $z = y - \sum_i \zeta_i e_i - \zeta_i \in \prod_v \mathcal{O}_v$. Ainsi

$$x = \xi + \sum_i \zeta_i e_i + z$$

avec $\xi + \sum_i \zeta_i e_i \in F$ et $z \in \prod_v \mathcal{O}_v$. □

Comme F est un sous-groupe discret de $\mathbb{A}_F$, c'est un sous-groupe fermé par le lemme B.3.8. L'intersection $F \cap \prod_v \mathcal{O}_v$ est donc un espace topologique discret et compact et est donc fini. C'est donc un sous-anneau fini de F, donc un sous-corps et on vérifie facilement que c'est le plus grand sous-corps fini de F. Notons le k. On conclut alors que $\mathbb{A}_F/F \simeq \prod_v \mathcal{O}_v/k$ est le quotient d'un groupe compact par un sous-groupe fini, c'est donc un groupe compact. □

3.1.3 Mesure de Haar

Soit $(G_v)_{v\in\Sigma}$ une famille de groupes localement compact et soit $(K_v)_{v\in\Sigma\smallsetminus\Sigma_\infty}$ une famille de sous-groupes ouverts. Supposons que S est une partie finie de Σ contenant Σ_∞ et que, pour tout $v\in\Sigma$, μ_v est une mesure de Haar à gauche sur G_v telle que $\mu_v(K_v)=1$ pour tout $v\notin S$.

Soit $G\coloneqq\prod'_{v\in\Sigma}G_v$.

Proposition 3.1.10. *Il existe une unique mesure de Haar (à gauche) μ sur G telle que, pour toute partie finie T de Σ contenant S et toute fonction $f_T\in\mathcal{C}_c(\prod_{v\in T}G_v,\mathbb{R})$, on ait*

$$\int_G(f_T\otimes 1^T)\mu=\int_{\prod_{v\in T}G_v}f_T\otimes_{v\in T}\mu_v$$

où $\mathbb{1}^T$ désigne la fonction indicatrice de $\prod_{v\notin T}K_v$ dans $\prod_{v\notin T}G_v$.

Démonstration. Soit I une forme linéaire positive sur $\mathcal{C}_c(G,\mathbb{R})$ correspondant à une mesure de Haar à gauche sur G (dont l'existence est assurée par le théorème B.5.2). Pour tout $f_T\in\mathcal{C}_c(\prod_{v\in T}G_v,\mathbb{R})$, on pose $I_T(f_T)\coloneqq I(f_T\otimes\mathbb{1}^T)$. Alors I_T est une forme linéaire positive $\prod_{v\in T}G_v$-invariante sur $\prod_{v\in T}G_v$ et coïncide avec la forme linéaire associée à la mesure de Haar $\otimes_{v\in T}\mu_v$ à un scalaire près. Ceci prouve l'existence et l'unicité. □

On applique cette construction au cas du groupe $G=\mathbb{A}_F$ avec $G_v=F_v$ et $K_v=\mathcal{O}_v$. Pour $v\in\Sigma$, on choisit une normalisation dx_v de la mesure de Haar de la façon suivante :

— $\int_{\mathcal{O}_v}dx_v=1$ si v est ultramétrique ;
— dx_v est la mesure de Lebesgue si $F_v=\mathbb{R}$ ($\int_0^1 dx=1$) ;
— $dx_v\coloneqq 2\,dx\,dy=dz\,d\overline{z}$ si $F_v=\mathbb{C}$.

On munit alors $\mathbb{A}_F$ de l'unique mesure de Haar fournie par la proposition 3.1.10 et la normalisation ci-dessous. On identifie F à un sous-groupe discret de $\mathbb{A}_F$ muni de la mesure de comptage. Le groupe quotient $\mathbb{A}_F/F$ est alors muni d'une mesure de Haar quotient satisfaisant les propriétés de la proposition B.5.4.

Théorème 3.1.11. *Si F est un corps de nombres, on a $\mathrm{Vol}(\mathbb{A}_F/F)=\sqrt{|\Delta_{\mathcal{O}_F/\mathbb{Z}}|}$. Si F est un corps de fonctions, on a $\mathrm{Vol}(\mathbb{A}_F/F)=\mathrm{Card}(k)^{-1}$ où k est le plus grans sous-corps fini de F.*

Démonstration. Supposons que F est un corps de nombres. D'après le corollaire B.5.7, il suffit de déterminer un domaine fondamental pour $\mathbb{A}_F/F$ et de calculer son

volume. D'après la démonstration du théorème 3.1.5, il est équivalent de déterminer un domain fondamental pour l'action de $\mathcal{O}_F$ sur $F_\infty \times \prod_{v\nmid\infty} \mathcal{O}_v$. Comme $\mathcal{O}_F$ agit librement sur F_∞, si Q est un domaine fondamental pour $F_\infty/\mathcal{O}_F$, alors $Q\times\prod_{v\nmid\infty} \mathcal{O}_v$ est un domaine fondamental pour $\mathbb{A}_F/F$. On a de plus

$$\mathrm{Vol}(Q \times \prod_{v\nmid\infty} \mathcal{O}_v) = \mathrm{Vol}(Q).$$

Ainsi il suffit de calculer $\mathrm{Vol}(Q)$. Rappelons que l'on peut choisir Q de la forme

$$Q \coloneqq \left\{ \sum_{i=1}^{d} t_i(e_i \otimes 1) \mid 0 \leqslant t_i \leqslant 1 \right\}$$

où $(e_1, \dots, e_d)$ est une $\mathbb{Z}$-base de $\mathcal{O}_F$. Soient $j_1, \dots, j_{r_1}$ les plongements réels de F et $j_{r_1+1}, \overline{j_{r_1+1}}, \cdots, j_{r_1+r_2}, \overline{j_{r_1+r_2}}$ des représentants des $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-orbites de plongements complexes (rappleons que $d = [F : \mathbb{Q}] = r_1 + 2r_2$). On peut identifier F_∞ avec $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ au moyen de l'application $e \otimes 1 \mapsto (j_1(e), \dots, j_{r_1+r_2}(e))$ et en identifiant $\mathbb{C}$ avec $\mathbb{R}^2$ au moyen de $z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$, on obtient un isomorphsime de $\mathbb{R}$-espace vectoriels $F_\infty \simeq \mathbb{R}^d$. L'image de Q est alors

$$\left\{ \sum_{i=1}^{d} t_i j(e_i) \mid 0 \leqslant t_i \leqslant 1 \right\}$$

où $j(e) = (j_1(e), \dots, j_{r_1}(e), \mathrm{Re}\, j_{r_1+1}(e), \mathrm{Im}\, j_{r_1+1}, \dots, \mathrm{Im}\, j_{r_1+r_2}(e))$. Comme le $\mathbb{R}$-isomorphisme $F_\infty \simeq \mathbb{R}^d$ échange la mesure de Haar sur F_∞ avec la mesure de Lebesgue sur $\mathbb{R}^d$ multipliée par 2^{r_2} (à cause de notre normalisation aux places complexes), on a

$$\begin{aligned}
\mathrm{Vol}(Q) &= 2^{r_2} \begin{vmatrix} j_1(e_1) & \cdots & \mathrm{Im}\, j_1(e_d) \\ \vdots & \ddots & \vdots \\ \mathrm{Re}\, j_{r_1+r_2}(e_1) & \cdots & \mathrm{Re}\, j_{r_1+r_2}(e_d) \\ \mathrm{Im}\, j_{r_1+r_2}(e_1) & \cdots & \mathrm{Im}\, j_{r_1+r_2}(e_d) \end{vmatrix} \\
&= 2^{r_2}2^{-r_2} \begin{vmatrix} j_1(e_1) & \cdots & j_1(e_d) \\ \vdots & \ddots & \vdots \\ j_{r_1+r_2}(e_1) & \cdots & j_{r_1+r_2}(e_d) \\ \overline{j_{r_1+r_2}}(e_1) & \cdots & \overline{j_{r_1+r_2}}(e_d) \end{vmatrix} = \det((j(e_i))_{\substack{j\in\mathrm{Hom}(F,\mathbb{C}) \\ 1\leqslant i\leqslant d}}) \\
&= \det((\mathrm{Tr}_{F/\mathbb{Q}}(e_ie_j))_{1\leqslant i,j\leqslant d})^{\frac{1}{2}} = |\Delta_{\mathcal{O}_F/\mathbb{Z}}|^{\frac{1}{2}}. \qquad \square
\end{aligned}$$

3.1.4 Le théorème d'approximation forte

Soit F un corps global. Si v_0 est une place de F, on note $\mathbb{A}_F^{v_0}$ le produit tensoriel restreint des groupes F_v pour $v \neq v_0$ relativement aux sous-groupes $\mathcal{O}_v$ pour $v \notin \Sigma_\infty \cup \{v_0\}$.

Théorème 3.1.12. *Soit v_0 une place de F. L'image de F par l'injection diagonale de F dans $\mathbb{A}_F^{v_0}$ est une partie dense. En d'autres termes, pour toute partie finie S de $\Sigma \smallsetminus \{v_0\}$, pour toute famille de réels $(\varepsilon_v > 0)_{v\in S}$, et pour tout $x = (x_v)_{v\in\Sigma} \in \mathbb{A}_F$, il existe $\xi \in F$ tel que $|x_v - \xi|_v \leqslant \varepsilon_v$ pour $v \in S$ et $|x_v - \xi|_v \leqslant 1$ pour $v \notin S \cup \{v_0\}$.*

Au cours de la preuve nous allons utiliser le résultat suivant.

Théorème 3.1.13 (Minkowski)**.** *Soit G un groupe abélien localement compact et soit Γ un sous-groupe discret dénombrable de G. On suppose qu'il existe un domaine fondamental D pour le quotient G/Γ. Alors si $E \subset G$ est un ensemble mesurable tel que $\mathrm{Vol}(E) > \mathrm{Vol}(G/\Gamma)$ (Γ étant muni de la mesure de comptage), alors il existe x et y dans E tels que $x - y \in \Gamma \smallsetminus \{0\}$.*

Démonstration. Supposons par l'absurde que ce ne soit pas le cas. Alors, pour tous $\xi_1, \xi_2 \in \Gamma$ avec $\xi_1 \neq \xi_2$, on a $(E + \xi_1) \cap (E + \xi_2) = \emptyset$. On a alors

$$\mathrm{Vol}(E) = \sum_{\xi\in\Gamma} \mathrm{Vol}(E \cap (D + \xi)) = \sum_{\xi\in\Gamma} \mathrm{Vol}((E + \xi) \cap D) \leqslant \mathrm{Vol}(D).$$

On aboutit donc à une contradiction. □

Lemme 3.1.14. *Soit S un ensemble fini de places de F tel que $v_0 \notin S$. Soit $(\varepsilon_v > 0)_{v\in S}$ une famille de réels positifs. Il exisye alors $\xi \in F^\times$ tel que $|x_i|_v \leqslant \varepsilon_v$ pour $v \in S$ et $|\xi|_v \leqslant 1$ pour $v \notin S \cup \{v_0\}$.*

Démonstration. Quitte à agrandir S, on peut supposer que S contient l'ensemble $\Sigma_\infty \smallsetminus \{v_0\}$ des places archimédiennes différentes de v_0. On considère l'ensemble mesurable suivant dans $\mathbb{A}_F$:

$$E = \left\{ x = (x_v)_v \in \mathbb{A}_F \mid |x_v|_x \leqslant \begin{cases} \frac{\varepsilon_v}{4} & \text{si } v \in S \\ 1 & \text{si } v \notin S \cup v_0 \\ A & \text{si } v = v_0 \end{cases} \right\}$$

où $A > 0$ est choisi tel que $A \prod_{v\in S} \varepsilon_v > 4^{\mathrm{Card}(S)} \mathrm{Vol}(\mathbb{A}_F/F)$. On a alors $\mathrm{Vol}(E) \geqslant 4^{-\mathrm{Card}(S)} A \prod_{v\in S} \varepsilon_v$ donc, d'après le théorème 3.1.13, il existe $\xi_1, \xi_2 \in E$ tels que $\xi_1 - \xi_2 \in F^\times$. Comme $|\xi_1 - \xi_2|_v \leqslant \varepsilon_v$ pour $v \in S$ et $|xi_1 - \xi_2|_v \leqslant 1$ pour $v \notin S \cup \{v_0\}$, on a le résultat voulu. □

Démonstration du théorème 3.1.12. On peut sans restriction supposer que $\Sigma_\infty \smallsetminus \{v_0\} \subset S$. Soit $(\varepsilon_v > 0)_{v\in S}$ une famille de réels strictement positifs. Soit D un domaine fondamental pour $\mathbb{A}_F/F$. On a vu au cours de la démonstration du théorème 3.1.11 que l'on peut choisir D tel qu'il existe un réel $M > 0$ vérifiant la propriété

suivante : si $x = (x_v) \in D$, alors $|x_v|_v \leqslant M$ si $v \in \Sigma_\infty$ et $|x_v|_v \leqslant 1$ si $v \notin \Sigma_\infty$. Le lemme 3.1.14 implique l'existence d'un élément $\xi \in F^\times$ tel que $|\xi|_v \leqslant \frac{\varepsilon_v}{M}$ si $v \in \Sigma_\infty \smallsetminus \{v_0\}$, $|\xi|_v \leqslant 1$ si $v \notin S \cup \{v_0\}$. Pour tout $x \in \mathbb{A}_F$, on peut décomposer $\xi^{-1}x \in \mathbb{A}_F$ sous la forme $\xi^{-1}x = \zeta + y$ avec $\zeta \in F$ et $y \in D$. On alors $|\xi y|_v \leqslant \varepsilon_v$ pour $v \in S$ et $|\xi y|_v \leqslant 1$ pour $v \notin S \cup \{v_0\}$ et $\xi\zeta \in F$ est l'élément recherché. □

3.2 Idèles

3.2.1 Définition et premières propriétés

Soit F un corps global. Le *groupe des idèles* I_F de F est le produit restreint des groupes localement compacts $(F_v^\times)_{v\in\Sigma}$ relativement à la famille de groupes ouverts compacts $(\mathcal{O}_v^\times)_{v\notin\Sigma_\infty}$.

Rappelons que si R est un anneau topologique, la topologie naturelle sur $R^\times$ est la topologie induite par l'inclusion $i : R^\times \hookrightarrow R^2$ définie par $x \mapsto (x, x^{-1})$. Pour cette topologie, $R^\times$ est un groupe topologique.

Proposition 3.2.1. *1. Le groupe topologiqie I_F est isomorphe au groupe $\mathbb{A}_F^\times$ muni de sa topologie naturelle.*

2. L'inclusion diagonale de $F^\times$ dans I_F a une image discrète.

Démonstration. Remarquons que si $x = (x_v)_{v\in\Sigma} \in I_F$, alors $(x_v)_{v\in\Sigma} \in \mathbb{A}_F$ et $(x_v^{-1})_{v\in\Sigma} \in \mathbb{A}_F$ de sorte que $(x_v)_{v\in\Sigma} \in \mathbb{A}_F^\times$. Réciproquement si $x = (x_v)_{v\in\Sigma} \in \mathbb{A}_F^\times$, alors il existe $y = (y_v)_{v\in\Sigma}$ tel que $xy = 1$. Ainsi $|x_v| \leqslant 1$ for presque tout v et $|y_v| = |x_v|^{-1} \leqslant 1$ pour presque tout v, ce qui implique que $(x_v)_{v\in\Sigma} \in I_F$. Une base de voisinages de 1 dans $\mathbb{A}_F^\times$ pour la topologie naturelle est donnée par

$$i^{-1}(U_S \times \prod_{v\notin S} \mathcal{O}_v) \times (V_S \prod_{v\notin S} \mathcal{O}_v) = \{(x_v)_{v\in\Sigma} \in I_F \mid (x_v)_{v\in S} \in U_S \cap V_S^{-1},\ x_v \in \mathcal{O}_v^\times \text{ for } v \notin S\}.$$

C'est une base de voisingaes de 1 pour la topologie de I_F.

Pour démontrer que $F^\times$ est discret dans I_F, il suffit de remarquer que l'inlusion $I_F \hookrightarrow \mathbb{A}_F$ est continues, de sorte que l'image inverse de F est discrète par le théorème 3.1.5. □

Remarque 3.2.2. L'inclusion $I_F \subset \mathbb{A}_F$ est continue. Cependant ce n'est pas un homéomorphism sur son image. En effet, la topologie de I_F est strictement plus fine que la topologie induite par l'inclusion de $\mathbb{A}_F^\times$ dans $\mathbb{A}_F$.

Soit $x = (x_v)_{v\in\Sigma} \in I_F$ un idèle. On définit sa *norme d'idèle* comme le nombre réel

$$|x| \coloneqq \prod_{v\in\Sigma} |x_v|_v$$

où $|\cdot|_v$ est la valeur absolue normalisée sur (rappelons que si $F_v = \mathbb{C}$, ce n'est pas vraiment une valeur absolue...). Ce produit est bien défini car $|x_v|_v = 1$ pour presque tout v (théorème 2.3.12).

La norme d'idèle défini un morphisme continu de groupes topologiques $I_F \to \mathbb{R}_{>0}$ dont le noyau est noté I_F^1.

Lemme 3.2.3. *On a un isomorphisme de groupes topologiques $I_F \simeq I_F^1 \times |I_F|$. En particulier,*

a) si F est un corps de nombres, on a $I_F \simeq I_F^1 \times \mathbb{R}_{>0}$;

b) et si F est un corps de fonctions, on a $I_F \simeq I_F^1 \times \mathbb{Z}$.

Démonstration. Il suffit de construire une section continus $s : |I_F| \to I_F$ au morphisme $|\cdot|$.

a) Si F est un corps de nombres, choisissons v_0 une place archimédienne et posons, pour $t \in \mathbb{R}_{>0}$, $s(t) = (x_v)_v$ où $x_{v_0} \coloneqq t^{1/[F_{v_0}:\mathbb{R}]}$ et $x_v \coloneqq 1$ pour $v \neq v_0$. Alors s convient.

b) Soit a le pgcd des degrés résiduels $f_v = [k_v : \mathbb{F}_p]$, où k_v désigne le corps résiduel k_v. Il existe une famille $(m_v)_v \in \mathbb{Z}^\Sigma$ telle que $m_v = 0$ pour presque tout v et $\sum_v m_v f_v = a$. On a alors $|I_F| \subset p^{a\mathbb{Z}} \subset \mathbb{R}_{>0}$. Soit $\varpi = (\varphi_v) \in I_F$ l'élément définit par $\varpi_v = \pi_v^{m_v}$ pour tout $v \in \Sigma$ où π_v désigne une uniformisante de F_v. On définit un morphisme de groupes $s : p^{a\mathbb{Z}} \to I_F$ par la formule $s(p^{-an}) \coloneqq \varpi^n$ et on vérifie que s est bien la section recherchée. □

Théorème 3.2.4. *On a $F^\times \subset I_F^1$ et le groupe topologique quotient $I_F^1/F^\times$ est compact.*

Démonstration. L'inclusion $F^\times \subset I_F^1$ est une conséquence directe de la formule du produit (théorème 2.3.12. Démontrons la compacité du quotient. Pour $t > 0$, on définit l'ensemble

$$I_F^t \coloneqq \{x \in I_F \mid |x| = t\}.$$

Lemme 3.2.5. *Il existe un nombre réel $C > 0$ tel que, pour tout $x = (x_v)_v \in I_F$ tel que $|x| > C$, il existe $\xi \in F^\times$ vérifiant $|\xi|_v \leqslant |x_v|_v$ pour tout $v \in \Sigma$.*

Démonstration. Soit $A_x \coloneqq \{y = (y_v)_v \in \mathbb{A}_F \mid |y_v|_v \leqslant \delta_v |x_v|_v\}$ où $\delta_v = 1$ excepté lorsque v est une place archimédienne où on pose $\delta_v = 1/4$. Alors $\mathrm{Vol}(A_x) = \alpha \prod_v |x_v|_v$ pour un certain $\alpha > 0$ indépendant de x (dépendant uniquement de F,

et plus précisément de r_1 et r_2). Soit $C > 0$ tel que $C\alpha > \mathrm{Vol}(\mathbb{A}_F/F)$. Alors si $|x| > C$, il existe, d'après le théorème 3.1.13 x_1 et x_2 dans A_x tels que $x_1 - x_2 \in F^\times$. On a alors $|\xi|_v \leqslant |x_v|_v$ pour toute $v \in \Sigma$. □

Lemme 3.2.6. *Il existe un nombre réel $C > 0$ tel que, pour tout $t > C$ et tout $x = (x_v)_v \in I_F^t$, il exisye $\xi \in F^\times$ tel que $1 \leqslant |\xi x_v|_v \leqslant t$ pour tout $v \in \Sigma$.*

Démonstration. Soit $C > 0$ comme dans le lemme 3.2.5. Pour $x = (x_v)_v \in I_F^t$, on a $|x| > C$ de sorte qu'il existe $\xi \in F^\times$ vérifiant $|\xi^{-1}|_v \leqslant |x_v|_v$ pour toute $v \in \Sigma$. Ceci nous donne $|\xi x_v|_v \geqslant 1$ pour toute $v \in \Sigma$. Enfin, si $v \in \Sigma$, on a

$$|\xi x_v|_v = \frac{\xi x}{\prod_{w \neq v} |\xi x_w|_w} \leqslant |\xi x| = |x| = t. \qquad \square$$

Lemme 3.2.7. *Soit $t > 1$. Il n'existe qu'un nombre fini de places ultramétrique v de F vérifiant $q_v \coloneqq \mathrm{Card}(k_v) \leqslant t$.*

Démonstration. Exercice. □

Nous pouvons à présent finir la démonstration du théorème 3.2.4. Soit $C > 0$ comme dans le lemme 3.2.6 et soit $t > \max\{C, 1\}$ tel que $t \in |I_F|$. Le lemme 3.2.7 implique l'existence d'un ensemble fini de places S de F contenant Σ_∞ et tel que $q_v > t$ si $v \notin S$. Soit $x \in I_F^t$. D'après le lemme 3.2.6, il existe $\xi \in F^\times$ tel que $1 \leqslant |\xi x_v|_v \leqslant t$ pour toute $v \in \Sigma$. Comme $|F_v|_v \cap]1, t[\subset |F_v| \cap]1, q_v[= \emptyset$, on a $|\xi x_v|_v = 1$ pour $v \notin S$. Ainsi

$$\xi x \in \prod_{v \in S} \{y_v \in F_v^\times \mid 1|y_v|_v \leqslant t\} \times \prod_{v \notin \Sigma} \mathcal{O}_v^\times$$

et cette dernière partie est compacte. On a donc prouvé qu'il existe une partie compacte de I_F^t qui se surjecte sur $I_F^t/F^\times$. Par translation par l'inverse d'un élément de I_F^t, on obtient une partie compacte de I_F^1 qui se surjecte sur $I_F^1/F^\times$. □

3.2.2 Idèles et idéaux

Le cas des corps de nombres

Soit F un corps de nombres et soit $x = (x_v)_v \in I_F$. On peut associer à x un idéal fractionnaire non nul $\mathfrak{a}(x)$ de $\mathcal{O}_F$ de la façon suivante. Il s'agit de l'idéal

$$\mathfrak{a}(x) \coloneqq \prod_{v \in \Sigma \smallsetminus \Sigma_\infty} \mathfrak{p}_v^{v(x_v)}$$

où $v(x_v) \in \mathbb{Z}$ désigne la valuation v-adic de x_v, ou encore $|x_v| = q_v^{-v(x_v)}$.

Exemple 3.2.8. Si $v \in \Sigma \setminus \Sigma_\infty$ et π_v est une uniformisante de F_v, si $x^{(v)} \coloneqq (x_w)_w$ avec $x_v = \pi_v$ et $x_w = 1$ lorsque $w \neq v$, alors $\mathfrak{a}(x^{(v)})$ est l'idéal maximal $\mathfrak{p}_v$ de $\mathcal{O}_F$.

Remarquons que $\mathfrak{a}(x) = \mathcal{O}_F$ si et seulement si $|x_v|_v = 1$ pour tout $v\Sigma \setminus \Sigma_\infty$. Ainsi on obtient un morphisme de groupes

$$\mathfrak{a} : I_F \to I(\mathcal{O}_F).$$

Ce morphisme est surjecrif comme le montre l'exemple 3.2.8 et son noyau est le sous-groupe ouvert $F_\infty^\times \times \prod_{v\nmid\infty} \mathcal{O}_v^\times$. Autrement dit, on a une suite exacte de groupes topologiques (où $I(\mathcal{O}_F)$ est muni de la topologie discrète)

$$1 \longrightarrow F_\infty^\times \times \prod_{v\nmid\infty} \mathcal{O}_v^\times \longrightarrow I_F \longrightarrow I(\mathcal{O}_F) \longrightarrow 1.$$

Soit $P(\mathcal{O}_F) \subset I(\mathcal{O}_F)$ le sous-groupe des idéaux fractionnaires principaux non nuls. Remarquons que si $\xi \in F$, on a $\mathfrak{a}(\xi) = \xi\mathcal{O}_F$. Ainsi $\mathfrak{a}(F^\times) = \mathcal{P}_{\mathcal{O}_F}$. On obtient donc un isomorphisme de groupes

$$\overline{\mathfrak{a}} : I_F/(F^\times F_\infty^\times \times \prod_{v\nmid\infty} \mathcal{O}_v^\times) \xrightarrow{\sim} \mathrm{Cl}(\mathcal{O}_F) = I(\mathcal{O}_F)/\mathcal{P}_{\mathcal{O}_F}. \tag{3.1}$$

Corollaire 3.2.9. *Le groupe* $\mathrm{Cl}(\mathcal{O}_F)$ *est fini.*

Démonstration. Soient $G \coloneqq I_F/F^\times F_\infty^\times \times \prod_{v\nmid\infty} \mathcal{O}_v^\times$ et $G^1 \coloneqq I_F^1/F^\times$. Comme $|F_\infty^\times| = \mathbb{R}_>0$, l'application naturelle continue $G^1 \to G$ est surjective. Comme $F_\infty^\times \times \prod_{v\nmid\infty} \mathcal{O}_v^\times$ est un sous-groupe ouvert de I_F, le noyau de $I_F \to G$ est un sous-groupe ouvert de I_F, donc G est discret en tant qu'espace topologique quotient, en particulier séparé. Comme G^1 est compact par le théorème 3.2.4, on en déduit également que le groupe G est compact. Finalement G est compact et discret, donc fini. □

Le cas des corps de fonctions

Soit p un nombre premier et soit F une extension finie de $\mathbb{F}_p(T)$. Soit k la clôture algébrique de $\mathbb{F}_p$ dans F. Il s'agit d'un corps fini qui est également le plus grand sous-corps fini de F. On l'appelle *corps des constantes* ou *corps de définition* de F.

Un *diviseur* de F est une application à support fini

$$d : \left\{ \begin{array}{ccc} \Sigma & \longrightarrow & \mathbb{Z} \\ v & \longmapsto & d(v) \end{array} \right.$$

On note souvent $\sum d(v)v$ une telle application. Le *degree* d'un diviseur d est l'entier $\sum_v f_v d(v)$ où $f_v \coloneqq [k_v : k]$ désigne la dimension du corps résiduel k_v de F_v en tant k-espace vectoriel. L'ensemble $\mathrm{Div}(F)$ des diviseurs de F possède une structure naturelle de groupe abélien, il s'agit par définition du groupe abélien libre engendré par l'ensemble des places de F. Le degré définit un morphisme de groupes $\mathrm{Div}(F) \to 0$ dont le noyau est noté $\mathrm{Div}^0(F)$.

On définit également un morphisme de groupes $\mathrm{div} : I_F \to \mathrm{Div}(F)$ par la formule

$$\mathrm{div}((x_v)_v) \coloneqq \sum_v d(v)v$$

où $d(v)$ est l'entier vérifiant $|x_v|_v = q_v^{-d(v)}$, q_v désignant le cardinal du corps résiduel k_v en v et $|\cdot|_v$ désugne la valeur absolue normalisée. L'application div est clairement surjective. On a de plus la formule $|x| = \mathrm{Card}(k)^{-\deg(\mathrm{div}(x))}$ qui montre que $\mathrm{div}(x) \in \mathrm{Div}^0(F)$ si et seulement si $x \in I_F^1$. Ainsi $\mathrm{div}(I_F^1) = \mathrm{Div}^0(F)$.

La formule du produit (théorème 2.3.12) implique $\mathrm{div}(F^\times) \subset \mathrm{Div}^0(F)$. On définit le *groupe de Picard* de F comme

$$\mathrm{Pic}(F) \coloneqq \mathrm{Div}(F)/\mathrm{div}(F^\times), \quad \mathrm{Pic}^0(F) \coloneqq \mathrm{Div}^0(F)/F^\times.$$

Corollaire 3.2.10. *Le groupe* $\mathrm{Pic}^0(F)$ *est fini.*

Démonstration. La démonstration est analogque à la démonstration du corollaire 3.2.9. □

Remarque 3.2.11. 1) On a une suite exact de groupes

$$1 \to k^\times \to F^\times \to \mathrm{Div}^0(F) \to \mathrm{Pic}^0(F) \to 1.$$

Il faut essentiellement vérifier qu'un élément $\xi \in F^\times$ tel que $\mathrm{div}(\xi) = 0$ est dans k. Un tel élément est dans le groupe $F^\times \cap \prod_v \mathcal{O}_v^\times$ qui est à la fois discret et compact, et donc fini. Ainsi ξ est une racine de l'unité et donc algébrique sur $\mathbb{F}_p$ et appartient donc à k.

2) Il existe en fait une courbe projective lisse et géométriquement connexe C définie sur k telle que F est le corpsdes fractions de C. Une telle courbe est unique à isomorphisme près. Le groupe $\mathrm{Pic}(F)$ est alors naturellement isomorphe au groupe des classes d'isomorphisme de fibrés inversibles sur C et $\mathrm{Pic}^0(C)$ au sous-groupe des fibrés inversibles de degré 0.

3.2.3 Mesures de Haar

Comme I_F est le produit restreint des groupes localement compacts $F_v^\times$ relativement aux sous-groupes ouverts compacts $\mathcal{O}_v^\times$, il est possible de construire une

mesure de Haar sur I_F au moyen d'une famille de mesures de Haar $d^\times x_v$ sur les $F_v^\times$ sous la conditions $\int_{\mathcal{O}_v^\times} d^\times x_v = 1$ pour presque toute v (voir la section 3.1.3).

Soit donc v une place de F et soit dx_v une mesure de Haar $(F_v, +)$. Comme $F_v^\times$ est ouvert dans F_v, la restriction de dx_v à $F_v^\times$ est une mesure de Radon sur $F_v^\times$. De plus, par définition de la valeur absolue normalisée sur F_v (définition 2.2.32) la mesure $|x_v|_v^{-1}\, dx_v$ est une mesure de Haar sur $(F_v^\times, \times)$. Calculons donc le volume de $\mathcal{O}_v^\times$ pour cette mesure lorsque v est ultramétrique. Si π_v désigne une uniformisante de F_v, on a $\mathcal{O}_v^\times = \mathcal{O}_v \smallsetminus \pi_v \mathcal{O}_v$ de sorte que

$$\int_{\mathcal{O}_v^\times} |x_v|_v^{-1}\, dx_v = \int_{\mathcal{O}_v^\times} |x_v|_v^{-1}\, dx_v = \int_{\mathcal{O}_v} dx_v - \int_{\pi_v \mathcal{O}_v} dx_v = \mathrm{Vol}(\mathcal{O}_v)(1 - q_v^{-1}).$$

Ainsi, il est naturel de renormaliser la mesure de Haar measure sur $F_v^\times$ aux places ultramétriques. Soit dx_v la mesure de Haar normalisée sur $(F_v, +)$ et posons, pour v ultramétrique,

$$d^\times x_v \coloneqq \frac{1}{1 - q_v^{-1}} |x_v|_v^{-1}\, dx_v.$$

Si $v \mid \infty$, on définit $d^\times x_v$ comme $|x_v|_v^{-1}\, dx_v$. Comme ces mesures ont presque toutes un volume égal à 1 sur $\mathcal{O}_v^\times$, on peut définir une mesure de Haar sur I_F en prenant leur produit :

$$d^\times x \coloneqq \prod_v{}' d^\times x_v.$$

La suite exacte de groupes topologiques

$$1 \longrightarrow I_F^1 \longrightarrow I_F \longrightarrow |I_F| \longrightarrow 1$$

nous permet de choisir une mesure de Haar sur le groupe localement compact I_F^1. On munit en effet le groupe $|I_F| \simeq \mathbb{R}_{>0}$ de la mesure de Haar $\frac{dt}{t}$, où dt désigne la mesure de Lebesgue si F est un corps de nombres et a number field and $|I_F| \simeq \mathbb{Z}$ de la mesure de comptage si F est un corps de fonctions. Dans les deux cas nous notons $\frac{dt}{t}$ cette mesure de Haar sur $|I_F|$. L'unicité de la mesure de Haar à un scalaire près (théorème B.5.2) ainsi que le théorème B.5.4 impliquent qu'il existe une unique mesure de Haar $d^1 g$ sur I_F^1 telle que pour toute $f \in C_c(I_F)$, on a

$$\int_{I_F} f(x)\, d^\times x = \int_{|I_f|} \int_{I_F^1} f(t x_1)\, d^1 x_1 \frac{dt}{t}.$$

3.2.4 Le volume de $I_F^1/F^\times$

Le cas des corps de nombres et le théorème des unités de Dirichlet

On commence naturellement par déterminer un domaine fondamental pour le groupe quotient $I_F^1/F^\times$.

Soit h_F le cardinal du groupe des classes $\mathrm{Cl}(\mathcal{O}_F)$. On déduit de l'isomorphisme (3.1) un isomorphismes de groupes $I_F^1/F^\times(F_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times) \simeq \mathrm{Cl}(\mathcal{O}_F)$ où F_∞^1 désigne l'ensemble des éléments de $F_\infty^\times$ de norme 1, c'est-à-dire

$$F_\infty^1 = \{(x_v)_{v|\infty} \in F_\infty^\times \mid \prod_{v|\infty} |x_v|_v = 1\}.$$

Soit donc $a_1, \ldots, a_{h_F}$ des représentants des éléments de $\mathrm{Cl}(\mathcal{O}_F)$ dans I_F^1. On a

$$I_F^1 = \coprod_{i=1}^{h} a_i (F_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times) F^\times.$$

On est donc réduit à la recherche d'un domaine fondamentale pour

$$(F_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times)F^\times/F^\times \simeq (F_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times)/\mathcal{O}_F^\times$$

puisque $F^\times \cap ((F_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times) = \mathcal{O}_F^\times$.

Lemme 3.2.12. *Soient A et B deux ensembles munis d'une action d'un groupe Γ. Si D est un domaine fondamental strict poue l'action de Γ sur A, alors $D \times B$ est un domaine fondamental pour l'action de Γ sur le produit $A \times B$.*

Démonstration. C'est immédiat. □

On est donc réduit à déterminer un domaine fondamental strict (et mesurable) D_∞ pour l'action de $\mathcal{O}_F^\times$ sur F_∞^1.

Soit $L : F_\infty^\times \to \mathbb{R}^{r_1+r_2}$ le morphisme de groupes topologiques défini par

$$L(x) \coloneqq (\log|x_v|_v)_v, \quad x = (x_v)_{v|\infty}.$$

C'est un morphisme surjectif et la formule du produit (théorème 2.3.12) implique que $L(\mathcal{O}_F^\times)$ est inclus dans l'hyperplan H de $\mathbb{R}^{r_1+r_2}$ d'équation $\sum_v X_v = 0$. De plus le noyau de L est un sous-groupe compact isomorphe à $\{\pm 1\}^{r_1} \times (\mathbb{S}^1)^{r_2}$.

Proposition 3.2.13. *Le sous-groupe $L(\mathcal{O}_F^\times)$ est un réseau de H, c'est-à-dire que $L(\mathcal{O}_F^\times)$ est un sous-groupe discret de H et $H/L(\mathcal{O}_F^\times)$ est compact.*

Démonstration. Comme le morphisme $L : F_\infty^\times \to \mathbb{R}^{r_1+r_2}$ possède une section continue, le morphisme L est ouvert. Il en est donc de même du morphisme $L|_{F_\infty^1} : F_\infty^1 \to H$. Comme le noyau de L est un sous-groupe compact, le lemme B.3.7 implique que le morphisme surjectif de groupes $L : F_\infty^1 \to H$ est à la fois ouvert et fermé. Comme $\mathcal{O}_F^\times$ est un sous-groupe fermé de F_∞^1, on en conclut que $L(\mathcal{O}_F^\times)$

est un sous-groupe fermé de H. Comme de plus $L(\mathcal{O}_F^\times)$ est dénombrable ($\mathcal{O}_F$ est en bijection avec $\mathbb{Z}^{[F:\mathbb{Q}]}$, la structure des sous-groupes fermés de $\mathbb{R}^n$ implique que $L(\mathcal{O}_F)$ est un sous-groupe discret de H. En particulier le quotient $H/L(\mathcal{O}_F^\times)$ est séparé. Nous allons montrer que le quotient $F_\infty^1/\mathcal{O}_F^\times$ est compact. Ainsi $H/L(\mathcal{O}_F^\times)$ sera isomorphe à un quotient séparé d'un groupe compact et sera donc compact. Montrons donc que $F_\infty^1/\mathcal{O}_F^\times$ est compact. L'inclusion $F_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_F^\times \hookrightarrow I_F^1$ est ouverte, on en conclut que $F_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_F^\times \hookrightarrow I_F^1/F^\times$ est un sous-groupe ouvert de $I_F^1/F^\times$, donc fermé et donc compact d'après le théorème 3.2.4. De plus le quotient de $F_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_F^\times \hookrightarrow I_F^1/F^\times$ par l'image du sous-groupe compact $\{1\} \times \prod_{v\nmid\infty} \mathcal{O}_v^\times$ est séparée et isomorphe à $F_\infty^1/\mathcal{O}_F^\times$ qui est donc compact. □

On en déduit le célèbre :

Théorème 3.2.14 (Théorème des unités de Dirichlet)**.** *Le groupe $\mathcal{O}_F^\times$ est de type fini est isomorphe à $\mu_F \times \mathbb{Z}^{r_1+r_2-1}$ où μ_F est le groupe fini des racines de l'unités contenues dans F.*

Démonstration. Comme $L(\mathcal{O}_F^\times)$ est un réseau de H d'après la proposition 3.2.13, il s'agit d'un $\mathbb{Z}$-module libre de rang $r_1 + r_2 - 1$. Le noyau de $L|_{\mathcal{O}_F^\times}$ est l'ensemble des éléments $\xi \in F^\times$ tels que $|\xi|_v = 1$ pour toute $v \in \Sigma$. Il s'agit d'une partie compacte et discrète de I_F, donc finie. Ses éléments sont donc de torsion dans $F^\times$, ce sont donc des racines de l'unités dans F. □

Soient $\varepsilon_1, \dots, \varepsilon_{r_1+r_2-1}$ des éléments de $\mathcal{O}_F^\times$ tels que les $L(\varepsilon_i)$ forment une $\mathbb{Z}$-base de $L(\mathcal{O}_F^\times)$. Fixons une place $v_0 \in \Sigma_\infty$ et considérons $L' : F_\infty^1 \to \mathbb{R}^{r_1+r_2-1}$ l'application composée de L et de la projection de $\mathbb{R}^{r_1+r_2}$ sur $\mathbb{R}^{\Sigma_\infty \smallsetminus \{v_0\}}$ consistant à oublier la place v_0. Alors L' est surjective et $L'(\mathcal{O}_F^\times)$ est un réseau de $\mathbb{R}^{\Sigma_\infty \smallsetminus \{v_0\}}$. Soit

$$Q \coloneqq \sum_{v \in \Sigma_\infty \smallsetminus \{v_0\}} [0,1[L'(\varepsilon_i)$$

de sorte que

$$\mathbb{R}^{\Sigma_\infty \smallsetminus \{v_0\}} = \bigcap_{\gamma \in L'(\mathcal{O}_F^\times)} (Q + \gamma).$$

Soit w_F le cardinal du groupe fini μ_F. Posons

$$D_\infty \coloneqq \{x = (x_v)_{v\in\Sigma_\infty} \in F_\infty^1 \mid L'(x) \in Q \text{ and } \operatorname{Arg}(x_{v_0}) \in [0, \tfrac{2\pi}{w}[\}.$$

Proposition 3.2.15. *L'ensemble $\coprod_{i=1}^h a_i(D_\infty \times \prod_{v\nmid\infty} \mathcal{O}_v^\times)$ est un domaine fondamentale strict pour l'action de $F^\times$ sur I_F^1.*

Démonstration. Il suffit de prouver que l'ensemble D_∞ est un domaine fondamentale strict pour l'action de $\mathcal{O}_F^\times$ sur F_∞^1. Posons $D'_\infty = \{x = (x_v)_{v\in\Sigma_\infty} \in F_\infty^1 \mid L'(x) \in Q\}$. On a bien $F_\infty^1 = \bigcup_{\gamma\in\mathcal{O}_F^\times} \gamma D'_\infty$. Par ailleurs si $\gamma_1 D_\infty \cap \gamma_2 D_\infty \neq \emptyset$, alors $\gamma_1 D'_\infty \cap \gamma_2 D'_\infty \neq \emptyset$, $L'(\gamma_1) = L'(\gamma_2)$ et $\gamma_2 \in \gamma_1\mu_F$. Soit $x \in D'_\infty$ tel que $\gamma_2\gamma_1^{-1} \in D'_\infty$. Comme $\mathrm{Arg}(x_{v_0})$ et $\mathrm{Arg}(\gamma_2\gamma_1^{-1}x_{v_0})$ sont tous deux dans $[0, \frac{2\pi}{w_F}[$ et $\gamma_2\gamma_1^{-1} \in \mu_F$, on doit avoir $\gamma_2 = \gamma_1$. Enfin on a clairement $D'_\infty = \bigcup_{\gamma\in\mu_F} \gamma D_\infty$. □

Le *régulateur* de F est le nombre réel positif

$$R_F := |\det((\log(|\varepsilon_i|_v))_{1\leqslant i\leqslant r_1+r_2-1,\ v\neq v_0})|.$$

Il s'agit du volume du parallélogramme engendré par les vecteurs $L'(\varepsilon_i)$ dans $\mathbb{R}^{r_1+r_2-1}$, il ne dépend donc pas du choix des éléments $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$. Par ailleurs la formule du produit montre que ce nombre ne dépend pas non plus du choix de la place v_0.

Théorème 3.2.16. *On a*

$$\mathrm{Vol}(I_F^1/F^\times) = \frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{w_F}.$$

Démonstration. On a $I_F^1 = \coprod_{i=1}^{h_F} a_i(F_\infty^1 \prod_{v\nmid\infty} \mathcal{O}_v^\times)F^\times$ de sorte que $\mathrm{Vol}(I_F^1/F^\times) = h_F \mathrm{Vol}(F_\infty^1/\mathcal{O}_F^\times)$ (rappelons que $\mathrm{Vol}(\mathcal{O}_v^\times) = 1$ pour toute place ultramétrique v). On munit $F_\infty^\times$ de la mesure produit $d^\times x_\infty \bigotimes_{v|\infty} d^\times x_v$ et F_∞^1 de l'unique mesure de Haar $d^1 x_\infty$ telle que le quotient de $d^\times x_\infty$ par $d^1 x_\infty$ soit $\frac{dt}{t}$ sur $\mathbb{R}_{>0}$. Rappelons que l'on a défini $D'_\infty := \{x \in F_\infty^1 \mid L'(x) \in Q\}$ dans la preuve de la proposition 3.2.15 et que l'on a $D'_\infty = \coprod_{\zeta\in\mu_F} \zeta D_\infty$ de sorte que $\mathrm{Vol}(D'_\infty) = w_F \mathrm{Vol}(D_\infty)$. Il suffit donc de prouver que $\mathrm{Vol}(F_\infty^1/\mathcal{O}_F^\times) = 2^{r_1}(2\pi)^{r_2} R_F$.

Soit

$$E_\infty := \{x \in F_\infty \mid x = (\underbrace{t, \ldots, t}_{r_1}, \underbrace{t^{\frac{1}{2}}, \ldots, t^{\frac{1}{2}}}_{r_2})d \mid t \in [1, e],\ d \in D'_\infty\}.$$

On a alors

$$\mathrm{Vol}(E_\infty) = \int_{E_\infty} d^\times x = \int_1^{e^{r_1+r_2}} \mathrm{Vol}(D'_\infty)\frac{dt}{t} = \mathrm{Vol}(D'_\infty)(r_1 + r_2).$$

On utilise la décomposition $F_\infty^\times \simeq (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$ pour calculer le volume de E_∞ en coordonnées polaires. Considérons l'application quotient $\rho : F_\infty^\times \twoheadrightarrow (\mathbb{R}_{>0})^{r_1+r_2}$ définie par $\rho(x) = (|x_v|_v)_v$. On obtient

$$\begin{aligned}\int_{E_\infty} d^\times x_1 \cdots d^\times x_{r_1+r_2} &= \int_{\rho(E_\infty)} \frac{d\rho_1}{\rho_1} \cdots \frac{d\rho_{r_1+r_2}}{\rho_{r_1+r_2}} \int_{\mathrm{Ker}\,\rho} d^\times y \\ &= 2^{r_1}(2\pi)^{r_2} \int_{\rho(E_\infty)} \frac{d\rho_1}{\rho_1} \cdots \frac{d\rho_{r_1+r_2}}{\rho_{r_1+r_2}}.\end{aligned}$$

En effet si v est une place complexe, on a $d^\times x_v = \frac{d\rho_v}{\rho_v}\, d\theta$. Avec le changement de variables $X_i = \log \rho_i$, l'intégrale $\int_{\rho(E_\infty)} \frac{d\rho_1}{\rho_1} \cdots \frac{d\rho_{r_1+r_2}}{\rho_{r_1+r_2}}$ est le volume de l'ensemble

$$P = \sum_{i=1}^{r_1+r_2-1} [0,1[L(\varepsilon_i) + [0,1[(1,\dots,1)$$

dans $\mathbb{R}^{r_1+r_2}$. On a donc

$$\begin{aligned}\mathrm{Vol}(P) &= \begin{vmatrix} \log|\varepsilon_1|_1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ \log|\varepsilon_1|_{r_1+r_2} & \cdots & 1 \end{vmatrix} \\ &= \begin{vmatrix} \log|\varepsilon_1|_1 & \cdots & \log|\varepsilon_{r_1+r_2-1}|_1 & 1 \\ \vdots & \ddots & \vdots & \vdots \\ \log|\varepsilon_1|_{r_1+r_2-1} & \cdots & \log|\varepsilon_{r_1+r_2-1}|_{r_1+r_2-1} & 1 \\ 0 & \cdots & 0 & r_1+r_2 \end{vmatrix} = (r_1+r_2)R_F. \quad \square\end{aligned}$$

Le cas des corps de fonctions

Soit F un corps global de caractéristique p. Soit $k \subset F$ le corps (fini) des constantes de F. Notons h_F le cardinal du groupe $\mathrm{Pic}^0(F)$ (fini d'après le corollaire 3.2.10). Soient $a_1, \dots, a_{h_F}$ des représentants de $\mathrm{Pic}^0(F)$ dans I_F^1. On a alors

$$\mathrm{Pic}^0(F) = \coprod_{i=1}^{h_F} a_i F^\times \prod_v \mathcal{O}_v^\times$$

et $F^\times \prod_v \mathcal{O}_v^\times / F^\times \simeq \prod_v \mathcal{O}_v^\times / k^\times$, on a donc

$$\mathrm{Vol}(I_F^1/F^\times) = \frac{h_F}{\mathrm{Card}(k^\times)}.$$

Chapitre 4

Fonctions Zêta

4.1 Dualité dans les groupes abéliens localement compacts

4.1.1 Le dual d'un groupe abélien localement compact

On note $\mathbb{S}^1 \coloneqq \{z \in \mathbb{C}^\times \mid |z| = 1\}$ le groupe abélien compact des nombres complexes de module 1. Si G est un groupe abélien localement compact, on appelle *caractère* un morphismes de groupes continu $\chi : G \to \mathbb{C}^\times$. Un caractère χ de G est dit *unitaire* si $\chi(G) \subset \mathbb{S}^1$. On définit le *dual* de G comme l'ensemble des caractères unitaires de G. L'ensemble $\widehat{G}$ est muni d'une structure de groupe pour la loi de multiplication donnée par $(\chi_1 \cdot \chi_2)(g) \coloneqq \chi_1(g)\chi_2(g)$ pour tout $g \in G$.

Si K est une partie compacte de G et V un voisinage de l'unité dans $\mathbb{S}^1$, on note $W(K, V)$ l'ensemble des éléments $\chi \in \widehat{G}$ tels que $\chi(K) \subset V$. On vérifie facilement que l'ensemble des $W(K, V)$ vérifie les propriétés du lemme B.3.1. L'ensemble des parties de la forme $W(K, V)$ forment donc un système de voisinages de l'unité pour une unique topologie de $\widehat{G}$, pour laquelle $\widehat{G}$ est un groupe topologique, appelée la *topologie compacte ouverte* (ou parfois topologique de la convergence compacte). Dans la suite de ce cours on muniera toujours $\widehat{G}$ de cette structure de groupe topologique.

Théorème 4.1.1. *(i) Si G est compact, le groupe topologique $\widehat{G}$ est discret.*

(ii) Si G est discret, le groupe topologiquep $\widehat{G}$ est compact.

(iii) Dans le cas général, le groupe topologique $\widehat{G}$ est localement compact.

Nous utiliserons plusieurs fois le lemme suivant.

Lemme 4.1.2 (Lemme des petits sous-groupes)**.** *Dans $\mathbb{C}^\times$ le seul sous-groupe contenu dans la boule ouverte $B(1,\sqrt{3})$ est le sous-groupe trivial $\{1\}$.*

Démonstration. Soit H un sous-groupe de $\mathbb{C}^\times$ contenu dans $B(1,\sqrt{3})$. Alors H est borné, ce qui implique que ses éléments sont de valeur absolue 1 et donc que $H \subset \mathbb{S}^1 \cap B(1,\sqrt{3})$. Comme $\mathbb{S}^1 \cap B(1,\sqrt{3})$ n'est pas dense dans $\mathbb{S}^1$, la classification des sous-groupes de $\mathbb{S}^1$ montre que H est un sous-groupe fini de $\mathbb{S}^1$. Tous les éléments de H sont donc des racines de l'unité. Supposons par l'abusr qu'il existe $z = e^{2\pi i\theta} \in H \smallsetminus \{1\}$. Alors $\theta \in 2\pi i\frac{a}{b}$ avec $a, b \in \mathbb{Z}$, $a \wedge b = 1$ et $1 \leqslant a < b$. Si $\frac{a}{b} \notin [\frac{1}{3}, \frac{2}{3}]$, alors quitte à remplacer z par z^{-1}, on peut supposer que $\frac{a}{b} \in]0, \frac{1}{3}[$. Alors $z^k \notin B(1,\sqrt{3})$ si k est le plus petit entier $\geqslant \frac{b}{a}$. On obtient une contradiction. □

Démonstration du théorème 4.1.1. Démontrons la propriété (i). Supposons donc G compact. Alors $W(G, B(1,\sqrt{3}))$ est un voisinage du caractère unité dans $\widehat{G}$. De plus, si $\chi W(G, B(1,\sqrt{3}))$, alors $\chi(G)$ est un sous-groupe de $\mathbb{C}^\times$ contenu dans $B(1,\sqrt{3})$. On déduit alors du lemme 4.1.2 que χ est le caractère trivial. Ceci impique bien que $\widehat{G}$ est discret.

Démontrons à présent (ii). Supposons donc G discret. Les parties compactes de G sont les ensembles finis et la topologie de $\widehat{G}$ est donc la topologie de la convergence simple c'est-à-dire la topologie induite par la topologie produit sur $(\mathbb{S}^1)^G$. On vérifie facilement que $\widehat{G}$ est un fermé de $(\mathbb{S}^1)^G$ qui est compact d'après le théorème de Tychonoff. On en conclut que $\widehat{G}$ est compact également.

Nous ne donnons pas de démonstration de la propriété (iii). Nous la démontrerons directement dans des cas particuliers chaque fois que nous en aurons besoin. Pour le cas général, voir [CG47, III.7] ou [RV99, Prop. 3.2]. □

Soit G un groupe abélien localement compact. Il existe un morphisme de groupes continu $G \to \widehat{\widehat{G}}$ défini par $g \mapsto (\hat{g} \mapsto \hat{g}(g))$ et appelé *morphisme de bidualité*. Nous ne démontrerons pas le résultat suivant dans le cas général, mais nous le vérifierons dans tous les cas particuliers où il sera utile.

Théorème 4.1.3 (Dualité de Pontriagin)**.** *Le morphisme de bidualité est un isomorphisme de groupes topologiques.*

Démonstration. Voir par exemple le théorème 5 dans [CG47, VI.16] ou [RV99, Thm. 3.20]. □

Corollaire 4.1.4. *Soit G un groupe abélien localement compact. Alors G est discret si et seulement si $\widehat{G}$ est compact et G est compact si et seulement si $\widehat{G}$ est discret.*

Corollaire 4.1.5. *Soit $g \in G$. On a $g = 1$ si et seulement si $\chi(g) = 1$ pour tout $\chi \in \widehat{G}$.*

Soit G un groupe localement compact et soit H un sous-groupe fermé de G. Soit $H^\perp$ le sous-groupe défini par $\{\chi \in \widehat{G} \mid \chi|_H = 1\}$. C'est un sous-groupe fermé de $\widehat{G}$. On a de plus un isomorphisme de groupes topologiques $\widehat{G/H} \simeq H^\perp$ induit par la précomposition d'un caractère avec l'application quotient $G \twoheadrightarrow G/H$.

4.1.2 Dualité dans les corps locaux

Soit F un corps local ultramétrique . Soit $\mathcal{O}$ son anneau de valuation et $\mathfrak{p}$ l'idéal maximal de $\mathcal{O}$.

Proposition 4.1.6. *Soit χ un caractère $F \to \mathbb{C}^\times$, alors χ est une fonction localement constante sur F. De plus χ est unitare. Soit χ un caractère $F^\times \to \mathbb{C}^\times$, alors χ est une fonction localement constante sur $F^\times$.*

Démonstration. On remarque que F et $F^\times$ possèdent des sous-groupes ouverts arbitrairement petits, plus précisément ils possèdent une base de voisinage de l'unité constituée de sous-groupes. On déduit alors du lemme 4.1.2 que les caractères de F et $F^\times$ sont des fonctions localement constantes.

Soit χ un caractère de F. Comme $\mathfrak{p}^n = \pi^n\mathcal{O}$ est un sous-groupe compact de F, le sous-groupe $\chi(\mathfrak{p}^n)$ est un sous-groupe compact de $\mathbb{C}^\times$ et donc $\chi(\mathfrak{p}^n) \subset \mathbb{S}^1$. Comme F est l'union des sous-groupes $\mathfrak{p}^n$ pour $n \in \mathbb{Z}$, on en conclut que $\chi(F) \subset \mathbb{S}^1$. □

Donnons à présent quelques exemples de caractères de F.

Exemple 4.1.7. Commençons par le cas où $F = \mathbb{Q}_p$ pour un nombre premier p. On a $\mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}[1/p]$ et $\mathbb{Z}_p \cap \mathbb{Z}[1/p] = \mathbb{Z}$. Ainsi si $x \in \mathbb{Q}_p$, on peut écrire $x = u + x'$ avec $u \in \mathbb{Z}_p$ et $x' \in \mathbb{Z}[1/p]$. Et cette décomposition est unique à un élément de $\mathbb{Z}$ près. On peut alors poser $\psi_{\mathbb{Q}_p}(x) \coloneqq e^{2\pi i x'}$, qui ne dépend pas des choix de u et x'. On vérifie que $\psi_{\mathbb{Q}_p}$ est un morphisme $\mathbb{Q}_p$ dans $\mathbb{C}^\times$. Son noyau est le sous-groupes $\mathbb{Z}_p$. Il s'agit donc d'une fonction localement constante de $\mathbb{Q}_p$ dans $\mathbb{C}^\times$ et donc continue. Plus généralement, si F est une extension finie de $\mathbb{Q}_p$, alors $\psi_F \coloneqq \psi_{\mathbb{Q}_p} \circ \mathrm{Tr}_{F/\mathbb{Q}_p}$ est un caractère non trivial de F.

Exemple 4.1.8. Supposons à présent que F est un corps local de caractéristique p pour p premier. Alors F est isomorphe au corps $k(\!(T)\!)$ où k est un corps fini de caractéristique p. On peut définir un caractère non trivial de $k(\!(T)\!)$ en posant

$$\psi_{k((T))}\left(\sum_{n>>-\infty} a_n T^n\right) = e^{\frac{2\pi i}{p}\mathrm{Tr}_{k/\mathbb{F}_p}(a_{-1})}.$$

Si ψ est un caractère du corps local F, on définit son *conducteur* comme le plus grand idéal $\mathfrak{f}_\psi$ de F contenu dans $\mathrm{Ker}(\psi)$. C'est-à-dire que

$$x \in \mathfrak{f}_\psi \Leftrightarrow \forall y \in \mathcal{O}, \quad \psi(xy) = 1.$$

Exemple 4.1.9. Le conducteur de $\psi_{\mathbb{Q}_p}$ est $\mathbb{Z}_p$. Le conducteur de $\psi_{k((T))}$ est $k[[T]]$.

Lemme 4.1.10. *Soit E/F une extension finie séparable de corps locaux ultramétrique. Soit ψ un caractère non trivial de F. On a alors*

$$\mathfrak{f}_{\psi\circ\mathrm{Tr}_{E/F}} = \mathfrak{f}_\psi \mathcal{D}_{E/F}^{-1}.$$

Démonstration. On a en effet

$$\begin{aligned} x \in \mathfrak{f}_{\psi\circ\mathrm{Tr}_{E/F}} &\Leftrightarrow \forall y \in \mathcal{O}_E, \quad \psi(\mathrm{Tr}_{E/F}(yx)) = 1 \\ &\Leftrightarrow \forall z \in \mathcal{O}_F, \forall y \in \mathcal{O}_E, \quad \psi(\mathrm{Tr}_{E/F}(zyx)) = 1 \\ &\Leftrightarrow \forall z \in \mathcal{O}_F, \forall y \in \mathcal{O}_E, \quad \psi(z\,\mathrm{Tr}_{E/F}(yx)) = 1 \\ &\Leftrightarrow \forall y \in \mathcal{O}_E, \quad \mathrm{Tr}_{E/F}(yx) \in \mathfrak{f}_\psi \\ &\Leftrightarrow x \in \mathfrak{f}_\psi \mathcal{D}_{E/F}^{-1}. \end{aligned}$$

□

Théorème 4.1.11. *Soit F un corps local. Soit ψ un caractère unitaire non trivial de F. Pour $x \in F$, on note ψ_x le caractère de F défini par $y \mapsto \psi(xy)$. Alors l'application $x \mapsto \psi_x$ est un isomorphisme de groupes topologiques.*

Démonstration. Posons $\Psi(x) \coloneqq \psi_x$. L'application Ψ est clairement un morphisme de groupes. Le morphisme Ψ est injectif. En effet si $x \neq 0$, soit $z \in F$ tel que $\psi(z) \neq 1$. Alors $\psi_x(zx^{-1}) \neq 1$ et donc ψ_x est non trivial.

Commençons par traiter le cas où F est ultramétrique. Si $n \in \mathbb{Z}$, on note W_n l'ensemble des caractères φ de F tels que $\varphi(\pi^n\mathcal{O}) = \{1\}$. L'ensemble des W_n constitue une base de voisinage de l'unité. En effet, puisque $\pi^n\mathcal{O}$ est un sous-groupe de F, le lemme 4.1.2 implique que $W_n = W(\pi^n\mathcal{O}, B(1,\sqrt{3}))$. De plus, puisque $F = \bigcup_{n\in\mathbb{Z}} \pi^n\mathcal{O}$ est que les $\pi^n\mathcal{O}$ sont ouverts, pour tout compact K de F, on a $K \subset \pi^n\mathcal{O}$ pour un certain $n \in \mathbb{Z}$ et donc $W_n \subset W(K,V)$ pour tout voisinage V de l'unité dans $\mathbb{C}^\times$. Comme $\Psi^{-1}(W_n) \supset \pi^{-n}\mathfrak{f}_\psi$, on en conclut que Ψ est continue. Par ailleurs l'image de $\pi^{-n}\mathfrak{f}_\psi$ par Ψ est exactement l'ensemble des caractères φ dans l'image de Ψ tels que $\varphi(\pi^n\mathcal{O}) = \{1\}$, c'est-à-dire $\Psi(F) \cap W_n$. On en déduit que Ψ induit un homéomorphisme de F sur son image.

Il reste donc à prouver que Ψ est surjectif. On suit [BH06, Prop. 1.7]. Soit $\varphi \in \widehat{F}$. Supposons φ non trivial. Notons $\mathfrak{f}_\psi = (\pi^d)$ le conducteur de ψ et $\mathfrak{f}_\varphi = (\pi^m)$ le conducteur de φ. Les caractère φ et $\psi_{u\pi^{d-m}}$ sont tous deux de conducteur (π^m) pour $u \in \mathcal{O}^\times$. Montrons qu'il existe $u \in \mathcal{O}^\times$ tel que $\varphi = \psi_{u\pi^{d-m}}$. Si u et u'

sont deux éléments de $\mathcal{O}^\times$ et si $n \geqslant 1$ est entier, les caractères $\psi_{u\pi^{d-m}}$ et $\psi_{u'\psi^{d-m}}$ coïncident sur (π^{m-n}) si et seulement si $u - u' \in (\pi^n)$. Comme les groupes abéliens $(\pi^{m-n})/(\pi^m)$ et $(\pi^{m-n})/(\pi^{m-1})$ sont de cardinaux respectifs q^n et q^{n-1}, le groupe $(\pi^{m-n})/(\pi^m)$ possède exactement $q^n - q^{n-1}$ caractères non triviaux sur (π^{m-1}). Comme $\mathcal{O}^\times/(1+(\pi^n))$ est un groupe fini de cardinal $q^n - q^{n-1}$, il existe un élément $u_n \in \mathcal{O}^\times$, uniquement déterminé modulo π^n tel que $\varphi|_{(\pi^{m-n})} = \psi_{u_n\pi^{d-m}}|_{(\pi^{m-n})}$. Par unicité, on a $u_{n+1} - u_n \in (\pi^n)$ pour tout entier $n \geqslant 1$. La suite (u_n) converge donc dans $\mathcal{O}^\times$ vers un élément u tel que $u - u_n \in (\pi^n)$ pour tout $n \geqslant 1$. On a donc $\varphi|_{(\pi^{m-n})} = \psi_{u\pi^{d-m}}|_{(\pi^{m-n})}$ pour tout $n \geqslant 1$, c'est-à-dire $\varphi = \psi_{u\pi^{d-m}}$ puisque $F = \bigcup_{n\geqslant 1}(\pi^{m-n})$.

Il reste à traiter les cas de $\mathbb{R}$ et $\mathbb{C}$ qui sont laissés en exercice. □

4.1.3 Dualité dans les adèles

Soit F un corps global et soit $\mathbb{A} = \mathbb{A}_F$. Si $\psi : \mathbb{A} \to \mathbb{C}^\times$ est un caractère, on note ψ_v le caractère de F_v obtenu par précomposition avec l'inclusion de F_v dans $\mathbb{A}$. La continuité de ψ ainsi que le lemme 4.1.2 impliquent que $\psi_v(\mathcal{O}_v) = 1$ pour presque toutes les places v de F. Réciproquement, si $(\psi_v)_v$ est une famille où ψ_v est un caractère de F_v telle que $\psi_v(\mathcal{O}_v) = 1$ pour presque toute v, alors on peut définir un caractère de $\mathbb{A}$ par la formule

$$(x_v)_v \longmapsto \prod_v \psi_v(x_v).$$

On note $\bigotimes_v \psi_v$ le caractère obtenu de cette façon. On obtient ainsi une bijection naturelle entre les caractères de $\mathbb{A}$ et les familles de caractères $(\psi_v)_v$ telles que $\psi_v(\mathcal{O}_v) = 1$ pour presque toute v.

Proposition 4.1.12. *Il existe un caractère unitaire non trivial $\psi : \mathbb{A} \to \mathbb{S}^1$ tel que $\psi(F) = 1$ et $\mathfrak{f}_{\psi_v} = \mathcal{O}_v$ pour presque toute v.*

Démonstration. Définissons ψ explicitement. Dans un premier temps, on le construit lorsque $F = \mathbb{Q}$. Soit $\psi_\mathbb{Q}$ le caractère de $\mathbb{A}_\mathbb{Q}$ défini par la formule $\psi_\mathbb{Q} = \bigotimes_v \psi_v$ où $\psi_v = \psi_{\mathbb{Q}_p}$ si $v = p$ et ψ_∞ est le caractère de $\mathbb{R}$ défini par $x \mapsto e^{-2\pi i x}$. On a $\mathfrak{f}_{\psi_{\mathbb{Q}_p}} = \mathbb{Z}_p$ pour tout p, de sorte que la condition sur les conducteurs est vérifiée. De plus si $\xi \in \mathbb{Q}$, on peut écrire ξ comme une somme finie $\sum_p \xi_p + m$ avec $m \in \mathbb{Z}$ et $\xi_p \in \mathbb{Z}[1/p]$. Par définition de $\psi_\mathbb{Q}$ on a $\psi_\mathbb{Q}(m) = 1$ et, pour un premier p, on a

$$\psi_\mathbb{Q}(\xi_p) = \psi_{\mathbb{Q}_p}(\xi_i)\psi_\infty(\xi_p) = e^{2\pi i\xi_p}e^{-2\pi i\xi_p} = 1$$

de sorte que $\psi_\mathbb{Q}(\mathbb{Q}) = 1$.

Si F est un corps de nombres, on pose $\psi_F = \psi_{\mathbb{Q}} \circ \mathrm{Tr}_{F/\mathbb{Q}}$. Le caractère ψ_F correspond à une famille de caractères ψ_v tels que $\mathfrak{f}_{\psi_v} = \mathcal{O}_v$ pour presque toute v puisque l'extension $F/\mathbb{Q}$ est non ramifiée en presque toute place.

Le cas des corps de fonctions est laissé en exercice. □

Remarque 4.1.13. Soit ψ un caractère unitaire non trivial de $\mathbb{A}_F$ tel que $\psi(F) = 1$. Le théorème d'approximation forte 3.1.12 implique que ψ_v est non trivial pour toute place v. En effet si $\psi_v = 1$, comme $F + F_v$ est dense dans $\mathbb{A}_F$, alors $\psi = 1$ par continuité.

Théorème 4.1.14. *Soit $\psi : \mathbb{A}_F \to \mathbb{S}^1$ un caractère unitaire de $\mathbb{A}_F$ tel que $\psi(F) = \{1\}$ et $\mathfrak{f}_{\psi_v} = \mathcal{O}_v$ pour presque toute v. Alors l'application $x \mapsto \psi_x$, with $\psi_x(y) = \psi(xy)$ est un isomorphisme de groupes topologiques de $\mathbb{A}_F$ sur $\widehat{\mathbb{A}}_F$.*

Démonstration. Soit $x = (x_v)_v \in \mathbb{A}_F$. Pour $y = (y_v)_v \in \mathbb{A}_F$, on a

$$\psi_x(y) = \prod_v \psi_v(x_v y_y).$$

Alors $\psi_v(x_v \mathcal{O}_v) = 1$ pour presque toute v de sorte que ψ_x est un caractère continu de $\mathbb{A}_F$. On vérifie facillement que l'application $x \mapsto \psi_x$ est injective et un homéomorphisme sur son image. Montrons qu'elle est surjective. Si $\varphi \in \widehat{\mathbb{A}}_F$, le caractère φ correspond à une famille (φ_v) de caractères unitaires des F_v telle que $\varphi(\mathcal{O}_v) = 1$ pour presque toute v. Comme $\psi_v \neq 1$ pour tout v d'après la remarque 4.1.13, il existe $x_v \in F_v$ tel que $\varphi_v = \psi_{v,x_v}$. Par ailleurs $\mathfrak{f}_{\psi_v} = \mathcal{O}_v$ pour presque toute v, on doit donc avoir $x_v \mathcal{O}_v \in \mathcal{O}_v$ pour presque toute v, c'est-à-dire $x_v \in \mathcal{O}_v$. Ainsi $(x_v) \in \mathbb{A}_F$. Ceci implique que $\varphi = \psi_x$ pour $x = (x_v)_v$. □

Corollaire 4.1.15. *Soit ψ un caractère unitaire non trivial de $\mathbb{A}_F$ tel que $\mathfrak{f}_{\psi_v} = \mathcal{O}_v$ pour presque toute v. Alors l'application $x \mapsto \psi_x$ induit un isomorphisme de F sur $\widehat{\mathbb{A}_F/F}$.*

Démonstration. Le groupe dual $\widehat{\mathbb{A}_F/F}$ s'identifie à $F^\perp \in \mathbb{A}_F$. En utilisant l'isomorphisme $\mathbb{A}_F \simeq \widehat{\mathbb{A}_F}$ prouvé au théorème 4.1.14, on considère $F^\perp$ comme un sous-groupe discret de $\mathbb{A}_F$ d'après le théorème 4.1.1. Comme $\psi(F) = 1$, on a $F \subset F^\perp$. De plus, il est facile de vérifier que $F^\perp$ est un sous-F-espace vectoriel de $\mathbb{A}_F$. Le quotient $F^\perp/F$ est alors un sous-groupe discret du groupe compact $\mathbb{A}_F/F$ (théorème 3.1.5) et est donc fini. Mais $F^\perp/F$ est également un F-espace vectoriel et F est infini. On doit donc avoir $F^\perp = F$. □

Corollaire 4.1.16. *Soit ψ un caractère unitaire non trivial de $\mathbb{A}_F$ tel que $\psi(F) = 1$. Alors $\mathfrak{f}_{\psi_v} = \mathcal{O}_f$ pour presque toute v.*

Démonstration. D'après le corollaire 4.1.15, ψ est de la forme $\varphi(\xi-)$ pour caractère φ vérifiant les propriétés demandées et $\xi \in F$. Comme $\xi \in \mathcal{O}_v^\times$ pour presque toute v, on en déduit le résultat. □

4.1.4 Transformée de Fourier

Soit G un groupe abélien localement compact et soit dg une mesure de Haar sur G. Pour $f \in L^1(G)$, la *transformée de Fourier* de f est la fonction $\hat{f}$ sur $\widehat{G}$ définie par

$$\forall \hat{g} \in \widehat{G}, \quad \hat{f}(\hat{g}) \coloneqq \int_G f(g)\hat{g}(g)^{-1}\, dg.$$

Théorème 4.1.17 (Inversion de Fourier)**.** *Il existe une unique mesure de Haar $d\hat{g}$ sur $\widehat{G}$ telle que, pour tout $f \in L^1(G)$ vérifiant $\hat{f} \in L^1(G)$ on a*

$$\forall g \in G, \quad f(g) = \int_{\widehat{G}} \hat{f}(\hat{g})\hat{g}(g)\, d\hat{g}.$$

La mesure $d\hat{g}$ est appelée la *mesure duale* de dg.

Remarque 4.1.18. Le théorème d'inversion 4.1.17 peut se réécrore $\hat{\hat{f}} = \check{f}$ où $\check{f}$ est défini par $\check{f}(g) \coloneqq f(g^{-1})$.

Supposons que G est isomorphe à son dual $\widehat{G}$ et fixons un isomorphisme entre ces deux groupes topologiques. Par exemple, si $G = F$ où F est un corps local, il revient au même de fixer un caractère unitaire non trivial de F. Dans ce cas, on peut on peut considérer la transformée de Fourier $\hat{f}$ d'une fonction f comme une fonction sur G et la mesure duale $d\hat{g}$ comme une mesure de Haar sur G. Si $c \in \mathbb{R}_{>0}$, la mesure duale de $c\, dg$ est donnée par $c^{-1}\, d\hat{g}$. Ainsi il existe une unique mesure de Haar dg sur G qui est autoduale, c'est-à-dire $d\hat{g} = dg$. On l'appelle la *mesure autoduale*. Il faut bien noter que cette mesure autoduale ne dépend pas uniquement de G mais aussi de l'isomorphisme choisi entre G et $\widehat{G}$.

4.1.5 Transformée de Fourier sur un corps local

Soit F un corps local. On suppose dans un premier temps que F est ultramétrique ultramétrique. Soit $\mathcal{O}_F$ son anneau de valuation, $\mathfrak{p}_F$ l'idéal maximal de $\mathcal{O}_F$, π_F une uniformisante de F et q_F le cardinal du corps résiduel $\mathcal{O}_F/\mathfrak{p}_F$. Soit ψ un caractère non trivial de F. Le choix de ψ fournit un isomorphisme $F \simeq \widehat{F}$. Soit $\mathfrak{f}_\psi$ le conducteur de ψ et soit $d \in \mathbb{Z}$ tel que $\mathfrak{f}_\psi = \mathfrak{p}_F^d = (\pi_F^d)$. On note dx l'unique mesure de Haar sur F telle que $\mathrm{Vol}(\mathcal{O}_F) = \int_{\mathcal{O}_F} dx = q_F^{\frac{d}{2}}$. Nous verrons un peu plus

loin qu'avec ce choix dx est la mesure autoduale de F (relativement à notre choix de ψ). La transformée de Fourier d'une fonciton f sur F est alors la fonction $\hat{f}$ définie sur G par

$$\hat{f}(y) = \int_G f(x)\psi(-xy)\,dx.$$

Nous allons être plus particulièrement intéressés par certaines fonctions spéciales de F. Soit $\mathcal{S}(F)$ le $\mathbb{C}$-espace vectoriel des fonctions localement constantes à support compact sur F. Cet espace est appelé *l'espace de Schwartz-Bruhat*.

Théorème 4.1.19. *Si $f \in \mathcal{S}(F)$, alors $\hat{f} \in \mathcal{S}(F)$ et on a $\hat{\hat{f}} = \check{f}$.*

Remarque 4.1.20. Le théorème 4.1.19 montre que notre choix de mesure dg est bien autodual pour le caractère ψ.

Démonstration. Une fonction $f \in \mathcal{S}(F)$ est une combinaison $\mathbb{C}$-linéaire finie de fonctions de la forme $\mathbb{1}_{a+\mathfrak{p}_F^n}$ pour $a \in F$ et $n \in \mathbb{Z}$. Il est donc suffisant de vérifier le théorème lorsque $f = \mathbb{1}_{a+\mathfrak{p}_F^n}$. Nous allons utiliser plusieurs fois le résultat suivant.

Lemme 4.1.21. *Soit G un groupe abélien compact, soit dg une mesure de Haar sur G et soit ψ un caractère de G. On a alors*

$$\int_G \psi(g)\,dg = \begin{cases} 0 & \text{si } \psi \neq \mathbb{1}_G \\ \mathrm{Vol}(G) & \text{si } \psi = \mathbb{1}_G. \end{cases}$$

Démonstration. Si $\psi = \mathbb{1}_G$, le résultat est évident. Supposons donc qu'il existe $h \in G$ tel que $\psi(h) \neq 1$. On a alors, par invariance de dg, $\psi(h)\int_G \psi(g)\,dg = \int_G \psi(g)\,dg$ et donc $\int_G \psi(g)\,dg = 0$. □

Revenons à la démonstration du théorème 4.1.19. On a

$$\begin{aligned}\widehat{f_{a,n}}(y) &= \int_F \mathbb{1}_{a+\pi^n\mathcal{O}_F}(x)\psi(-xy)\,dx = \int_{\pi^n\mathcal{O}_F} \psi(-(a+z)y)\,dy \\ &= \psi(-ay)\int_{\pi^n\mathcal{O}_F} \psi(zy)\,dz.\end{aligned}$$

Le lemme 4.1.21 immplique que

$$\int_{\pi^n\mathcal{O}_F} \psi(zy)\,dz = \begin{cases} 0 & \text{si } y\pi^n\mathcal{O}_F \not\subset \mathfrak{f}_\psi \\ \mathrm{Vol}(\pi^n\mathcal{O}_F) & \text{si } y\pi^n\mathcal{O}_F \not\subset \mathfrak{f}_\psi. \end{cases}$$

On a donc

$$\widehat{f_{a,n}}(y) = \mathrm{Vol}(\pi^n\mathcal{O}_F)\psi(-ay)\mathbb{1}_{\pi^{-n}\mathfrak{f}_\psi}(y) = q_F^{-n}\,\mathrm{Vol}(\mathcal{O}_F)\psi(-ay)\mathbb{1}_{\pi^{-n+d}\mathcal{O}_F}(y). \quad (4.1)$$

En utilisant à nouveau l'égalité (4.1), on obtient

$$\begin{aligned}\widehat{\widehat{f_{a,n}}}(x) &= q_F^{-n}\operatorname{Vol}(\mathcal{O}_F)\int_F \psi(-az)\mathbb{1}_{\pi^{-n+d}\mathcal{O}_F}(z)\psi(-xz)\,dz\\ &= q_F^{-n}\operatorname{Vol}(\mathcal{O}_F)\int_F \mathbb{1}_{\pi^{-n+d}\mathcal{O}_F}(z)\psi(-(a+x)z)\,dz\\ &= q_F^{-n}\operatorname{Vol}(\mathcal{O}_F)q_F^{n-d}\operatorname{Vol}(\mathcal{O}_F)\psi(0\cdot x)\mathbb{1}_{\pi^{n-d}\mathfrak{f}_\psi}(a+x)\\ &= q_F^{-d}\operatorname{Vol}(\mathcal{O}_F)^2\mathbb{1}_{-a+\pi^n\mathcal{O}_F}(x) = q_F^{-d}\operatorname{Vol}(\mathcal{O}_F)^2\mathbb{1}_{a+\pi^n\mathcal{O}_F}(-x).\end{aligned}$$

L'équation (4.1) et la proposition 4.1.6 montrent que $\widehat{f_{a,n}} \in \mathcal{S}(F)$ et le choix de la mesure de Haar dg implique $q_F^{-d}\operatorname{Vol}(\mathcal{O}_F) = 1$, de sorte que $\widehat{\widehat{f_{a,n}}} = \check{f}_{a,n}$. □

Exemple 4.1.22. Si F est une extension finie de $\mathbb{Q}_p$ et $\psi = \psi_{\mathbb{Q}_p} \circ \operatorname{Tr}_{F/\mathbb{Q}_p}$, alors $\mathfrak{f}_\psi = \mathcal{D}_{F/\mathbb{Q}_p}^{-1}$. Pour ce choix de caractère, la mesure autoduale de F est $q_F^{-\frac{m}{2}}\,dx$ où dx est la mesure de Haar normalisée (c'est-à-dire $\int_{\mathcal{O}_F} dx = 1$) et $\mathcal{D}_{F/\mathbb{Q}_p} = \mathfrak{p}_F^m$, avec $m \in \mathbb{N}$.

Exercice 4.1.1. On considère ici le cas où $F = \mathbb{R}$. On définit un caractère unitaire non trivial unitary de $\mathbb{R}$ en posant $\psi_{\mathbb{R}}(x) \coloneqq e^{-2\pi i x}$. Vérifier que la mesure de Haar autoduale pour ce caractère est le mesure de Lebesgue dx (c'est-à-dire telle que $\int_0^1 dx = 1$). De plus soit $\mathcal{S}(\mathbb{R})$ l'espace de Schwartz des fonctions indéfiniment dérivables $f : \mathbb{R} \to \mathbb{C}$ telles que pour tout $(m,n) \in \mathbb{N}^2$

$$\lim_{|x|\to+\infty} |x|^m |f^{(n)}(x)| = 0.$$

Véfifier que $f \in \mathcal{S}(\mathbb{R})$ implique $\hat{f} \in \mathcal{S}(\mathbb{R})$ et $\hat{\hat{f}} = \check{f}$.

Exercice 4.1.2. On considère à présent le cas où $F = \mathbb{C}$. On définit un caractère unitaire non trivial de $\mathbb{C}$ en posant $\psi_{\mathbb{C}}(z) \coloneqq \psi_{\mathbb{R}}(\operatorname{Tr}_{\mathbb{C}/\mathbb{R}}(z)) = e^{-4\pi i \operatorname{Re}(z)}$. Vérifier que la mesure de Haar autoduale sur $\mathbb{C}$ est la mesure $2\,dx\,dy$ (telle que la mesure de $[0,1]^2$ vaut 2). Soit $\mathcal{S}(\mathbb{C})$ l'espace de Schwartz space des fonctions indéfiniment différentiables $f : \mathbb{C} \simeq \mathbb{R}^2 \to \mathbb{C}$ telles que pour tout $(p,q,n) \in \mathbb{N}^3$

$$\lim_{|z|\to+\infty} |z|^n \left|\frac{\partial^{p+q} f}{\partial x^p \partial y^q}(z)\right| = 0.$$

Véfiier que $f \in \mathcal{S}(\mathbb{C})$ implique $\hat{f} \in \mathcal{S}(\mathbb{C})$ et que $\hat{\hat{f}} = \check{f}$.

4.1.6 Transformée de Fourier sur les adèles

Soit ψ un caractère unitaire non trivial de $\mathbb{A}_F$ tel que $\psi(F) = 1$. Le corollaire 4.1.16 implique alors que $\mathfrak{f}_{\psi_v} = \mathcal{O}_v$ pour presque toute v. Soit $\mathbb{A}_f$ l'anneau des

adèles finis, c'est-à-dire le produit restreint des F_v pour v place ultramétrique relativement aux sous-groupes $\mathcal{O}_v$. On définit l'espace des fonctions de *Schwartz-Bruhat* sur $\mathbb{A}_F$ comme

$$\mathcal{S}(\mathbb{A}_F) \coloneqq \mathcal{S}(F_\infty) \otimes_{\mathbb{C}} \mathcal{S}(\mathbb{A}_f)$$

où $\mathcal{S}(F_\infty) \coloneqq \bigotimes_{v|\infty} \mathcal{S}(F_v)$ et $\mathcal{S}(\mathbb{A}_f)$ est l'espace des fonctions localement constantes à support compact sur $\mathcal{A}_f$. Tout élément de $\mathcal{S}(\mathbb{A}_F)$ est une somme finie de fonctions de la forme $\bigotimes_{v\in S} f_v \otimes \chi^S$ où $\chi^S = \mathbb{1}_{\prod_{v\notin S} \mathcal{O}_v}$ pour S un ensemble fini de places contenant Σ_∞ et $f_v \in \mathcal{S}(F_v)$.

Noter que $\mathfrak{f}_{\psi_v} = \mathcal{O}_v$ pour presque tout v. Dans ce cas, la mesure autoduale de F_v relativement à ψ_v vérifie $\int_{\mathcal{O}_v} dx_v = 1$. Soit dx la mesure sur $\mathbb{A}_F$ définie comme le produit des mesures autoduales mesure sur les F_v relativement aux ψ_v. Cette mesure est bien définie d'après le proposition 3.1.10.

Proposition 4.1.23. *Si $f \in \mathcal{S}(\mathbb{A}_F)$, alors $\hat{f} \in \mathcal{S}(\mathbb{A}_F)$ et $\hat{\hat{f}} = \check{f}$.*

En particulier la mesure de Haar sur $\mathbb{A}_F$ définie comme le produit des mesures autoduales sur les F_v relativement aux ψ_v est bien la mesure autoduale sur $\mathbb{A}_F$ relativement à ψ.

Démonstration. Par linéarité, il suffit de vérifier le résultat pour une fonction f de la forme $\bigotimes_{v\in S} f_v \otimes \chi^S$. Sans perte de généralité, on peut agrandir S de sorte que S contienne toutes les places v pour lesquelles $\mathfrak{f}_{\psi_v} \neq \mathcal{O}_v$. D'après la proposition 3.1.10, on a alors

$$\hat{f}(y) = \int_{\mathbb{A}_F} f(x)\psi(-xy)\,dx = \prod_{v\in S} \int_{F_v} f_v(x)\psi_v(-x_v y_v)\,dx_v = \prod_{v\in S} \hat{f}_v(y_v).$$

On en déduit que $\hat{f} = \bigotimes_{v\in S} \hat{f}_v \otimes \chi^S \in \mathcal{S}(\mathbb{A}_F)$ et la formule d'inversion se déduit du théorème 4.1.19. □

D'après le corollaire 4.1.15, tout autre caractère unitaire ψ de $\mathbb{A}_F$ vérifiant $\psi(F)$ est de la forme $\psi(\xi-)$ pour un certain $\xi \in F$. La formule du produit (théorème 2.3.12 implique alors que la mesure autoduale sur $\mathbb{A}_F$ relativement à $\psi(\xi-)$ est aussi dx. En effet, en posant $\psi' = \psi(\xi-)$, on vérifie facilement que la mesure autoduale sur F_v relativement à ψ'_v est $|\xi_v|_v^{\frac{1}{2}}\,dx_v$. Ainsi la mesure autoduale sur $\mathbb{A}_F$ ne dépend pas du choix du caractère character ψ (à condition que $\psi(F) = \{1\}$). Le quotient de cette mesure autoduale sur $\mathbb{A}_F$ par la mesure de comptage sur F est une measure de Haar sur $\mathbb{A}_F/F$ appelée *mesure de Tamagawa* sur $\mathbb{A}_F$.

Proposition 4.1.24. *Pour la mesure de Tamagawa, le volume de $\mathbb{A}_F/F$ vaut* 1.

Démonstration. Prouvons le cas des corps de nombres. Soit $dx = \bigotimes_v dx_v$la mesure sur $\mathbb{A}_F$ telle que dx_v est la mesure normalisée sur pour tout v. D'après le théorème 3.1.11, on a $\int_{\mathbb{A}_F/F} dx = |\Delta_F|^{\frac{1}{2}}$ pour la mesure quotient de dx par la mesure de comptage sur F. Soit ψ un caractère unitaire non trivial de $\mathbb{A}_F$. Comme la mesure autoduale sur $\mathbb{A}_F$ ne dépend du choix de ce caractère, on peut le choisir de la forme $\psi_{\mathbb{Q}} \circ \mathrm{Tr}_{F/\mathbb{Q}}$. Alors $\mathfrak{f}_{\psi_v} = \mathcal{D}^{-1}_{F_v/\mathbb{Q}_p}$ pour toute place v ultramétrique (avec $p = v|_{\mathbb{Q}}$) alors que dx_v est déjà autoduale si $v \mid \infty$ (d'après les exercices 4.1.1 et 4.1.2). Ainsi la mesure autoduale sur $\mathbb{A}_F$ est $c\,dx$ où $c = \prod_{v\nmid\infty} c_v$ avec $c_v = |\pi_v|_v^{\frac{d_v}{2}}$ tel que $\mathcal{D}_{F_v/\mathbb{Q}_p} = (\pi_v^{d_v})$. La formule du produit (théorème 2.3.12 implique alors que

$$\prod_v c_v = \prod_{v\nmid\infty} |\pi_v|_v^{\frac{d_v}{2}} = \prod_p \prod_{v|p} |N_{F_v/\mathbb{Q}_p}(\pi_v)^{d_v}|_p^{\frac{1}{2}} = \prod_p |\Delta_F|_p^{\frac{1}{2}} = |\Delta_F|_\infty^{-\frac{1}{2}}.$$

Ce qui nous donne le résultat. □

Exercice 4.1.3. Démontrer la proposition 4.1.24 lorsque F est un corps de fonctions.

4.2 Fonctions zêta locales

4.2.1 Caractères multiplicatifs

Soit F un corps local ultramétrique. On rappelle qu'un caractère de $F^\times$ est un morphisme de groupes continu $\omega : F^\times \to \mathbb{C}^\times$. Un caractère est dit *non ramifié* si $\omega(\mathcal{O}_F^\times) = 1$. Dans ce cas, il est déterminé par sa valeurs sur une uniformisante π_F de F et donc de la forme $|\cdot|_F^s$ pour un nombre complexe $s \in \mathbb{C}$. Plus généralement, un carcatère ω de $F^\times$ peut s'écrire sous la forme $\omega_0|\cdot|_F^s$ où ω_0 est unitaire et $s \in \mathbb{C}$. Noter qu'une telle écriture n'est pas unique. On dit que deux caractères $|\cdot|_1$ et $|\cdot|_2$ sont *equivalents* s'il existe $s \in \mathbb{C}$ tel que $|\cdot|_2|\cdot|_1^{-1} = |\cdot|^s$. La classe d'équivalence d'un caractère est en bijection avec $\mathbb{C}/\mathbb{Z}\frac{2\pi i}{\log(q_F)} \simeq \mathbb{C}^\times$ et peut être munie d'une structure de surface de Riemann. Cela nous permet de parler de l'holomorphie ou de la méromorphie d'une fonction à valeurs complexes définie sur l'ensemble des caractères.

Si ω est un caractère de $F^\times$, on pose $\sigma(\omega) \coloneqq \mathrm{Re}(s)$ où $\omega = \omega_0|\cdot|^s$ avec ω_0 unitaire. Cette définition ne dépend pas de la décomposition choisie. En effet, si$\omega_0|\cdot|^s = \omega_0'|\cdot|^{s'}$, alors $s - s' \in i\mathbb{R}$.

À partir de maintenant, on fixe ψ un caractère non trivial de F et on note dx la mesure autoduale de F relativement au choix de ψ. On fixe également $d^\times x$ une mesure de Haar sur $F^\times$ (le choix de $d^\times x$ n'influe sur ce qui suit).

Si $f \in \mathcal{S}(F)$ et si ω est un caractère de $F^\times$, l'*intégrale zêta* associée à f et ω est

$$Z(f,\omega) \coloneqq \int_{F^\times} f(x)\omega(x)\, d^\times x$$

lorsque l'intégrale converge.

Lemme 4.2.1. *L'intégrale $Z(f,\omega)$ converge absolument pour $\sigma(\omega) > 0$.*

Démonstration. On peut écrire $f = f(0)\mathbb{1}_{\mathcal{O}_F} + g$ où g est localement constante à support compact dans $F^\times$. L'intégrale $\int_{F^\times} g(x)\omega(x)\, d^\times x$ converge absolument pour tout ω. De plus, si $\sigma \coloneqq \sigma(\omega) > 0$, on a

$$\begin{aligned}\int_{F^\times} |\mathbb{1}_{\mathcal{O}_F}(x)\omega(x)|\, d^\times x = \int_{\mathcal{O}_F} |x|^\sigma\, d^\times x &= \sum_{n=0}^{+\infty} \int_{\pi_F^n \mathcal{O}_F} |x|^\sigma\, d^\times x \\ &= \sum_{n=0}^{\infty} q_F^{-n\sigma} \operatorname{Vol}(\mathcal{O}_F^\times) = \operatorname{Vol}(\mathcal{O}_F^\times)\frac{1}{1-q_F^{-\sigma}}.\end{aligned}$$

□

Remarque 4.2.2. La preuve du lemme 4.2.1 montre que, pour tout $s \in \mathbb{C}$ tel que $\operatorname{Re} s > 0$, on a

$$Z(\mathbb{1}_{\mathcal{O}_F}, |\cdot|_F^s) = \operatorname{Vol}(\mathcal{O}_F^\times)\frac{1}{1-q_F^{-s}}.$$

4.2.2 L'équation fonctionnelle locale

Soit $f \in \mathcal{S}(F)$. La remarque 4.2.2 implique que, pour $\operatorname{Re} s > 0$,

$$Z(f, |\cdot|^s) = f(0)\operatorname{Vol}(\mathcal{O}_F^\times)\frac{1}{1-q_F^{-s}} + Z(g, |\cdot|^s)$$

où $g = f - f(0)\mathbb{1}_{\mathcal{O}_F}$. Comme g est une fonction à support compact sur $F^\times$, l'intégrale $Z(g,|\cdot|^s)$ converge absolument pour toute valeur de $s \in \mathbb{C}$ et l'application $s \mapsto Z(g,|\cdot|^s)$ est holomorphe sur $\mathbb{C}$. Ceci montre que l'application $s \mapsto Z(f,|\cdot|^s)$ se prolonge (de façon unique par le théorème du prolongement analytique) en une fonction méromorphe sur $\mathbb{C}$.

Considérons à présent le cas de caractères ramifiés. Soit ω_0 un caractère unitaire de $F^\times$ et supposons que ω_0 est ramifié, ce qui est encore équivalent à demander que ω_0 ne soit pas de la forme $|\cdot|^{it}$ pour $t \in \mathbb{R}$. On définit le *conducteur* de ω_0 comme le plus grand idéal $\mathfrak{f}_{\omega_0}$ de $\mathcal{O}_F$ tel que ω_0 est trivial sur $1 + \mathfrak{f}_{\omega_0}$. La proposition 4.1.6 montre que le conducteur est un idéal ouvert de $\mathcal{O}_F$. Il est donc de la forme $\mathfrak{f}_{\omega_0} = (\pi_F^m)$ pour un certain. Notons que, puisque ω_0 est ramifié, la restriction de ω_0 à $\mathcal{O}_F^\times$ est non triviale. Le lemme 4.1.21 implique que

$$\int_{\mathcal{O}_F^\times} \omega_0(x)\, d^\times x = 0.$$

Par invariance de la mesure de Haar, on en déduit que, pour tout $n \in \mathbb{Z}$, on a $\int_{\pi^n \mathcal{O}_F^\times} \omega_0(x)\, d^\times x = 0$. Soit $f \in \mathcal{S}(F)$ et soit $n \geqslant 1$ tel que f est constante sur $\pi^n \mathcal{O}_F$. Pour $s \in \mathbb{C}$ tel que $\operatorname{Re} s > 0$, on a

$$\begin{aligned}\int_{\pi^n \mathcal{O}_F \smallsetminus \{0\}} f(x)\omega_0(x)|x|^s\, d^\times x &= \sum_{k \geqslant n} \int_{\pi^k \mathcal{O}_F^\times} f(x)\omega_0(x)|x|^s\, d^\times x \\ &= \sum_{k \geqslant n} |\pi|^{ks} \int_{\pi^k \mathcal{O}_F^\times} f(0)\omega_0(x)\, d^\times x = 0.\end{aligned}$$

On a donc prouvé

$$Z(f, \omega_0|\cdot|^s) = \int_{F \smallsetminus \pi^n \mathcal{O}_F} f(x)\omega_0(x)|x|^s\, d^\times x$$

pour tout $s \in \mathbb{C}$ tel que $\operatorname{Re} s > 0$. L'intégrale de droite est absolument convergente pour tout $s \in \mathbb{C}$ et fournit une fonction holomorphe sur $\mathbb{C}$. Ainsi on a prouvé que la fonction $s \mapsto Z(f, \omega_0|\cdot|^s)$ s'étend en une fonction holomorphe sur $\mathbb{C}$ (autrement dit une fonction entière).

Pour conclure, nous avons prouvé que la fonction $\omega \mapsto Z(f, \omega)$ possède un unique prolongement méromorphe en ω. Ce prolongement méromorphe est holomorphe sur les classes d'équivalence de caractères ramifiés. Nous allons à présent vérifier que ce prolongement méromorphe satisfait une équation fonctionnelle.

Si ω est un caractère de $F^\times$, on définit $\widetilde{\omega} := |\cdot|\omega^{-1}$. En écrivant $\omega = \omega_0|\cdot|^s$ où ω_0 est unitaire, on a $\widetilde{\omega} = \omega_0^{-1}|\cdot|^{1-s} = \overline{\omega_0}|\cdot|^{1-s}$.

Proposition 4.2.3. *Soit ω un caractère de $F^\times$ tel que $0 < \sigma(\omega) < 1$. Soient f et g deux éléments de $\mathcal{S}(F)$. On a alors*

$$Z(f, \omega)Z(\hat{g}, \widetilde{\omega}) = Z(g, \omega)Z(\hat{f}, \widetilde{\omega}).$$

Démonstration. Prouvons que la quantité $Z(f, \omega)Z(\hat{g}, \widetilde{\omega})$ ne change pas lorsque

l'on échange les rôles de f et g.

$$\begin{aligned}
Z(f,\omega)Z(\hat{g},\widetilde{\omega}) &= \int\int_{F^\times\times F^\times} f(x)\hat{g}(y)|y|\omega(xy^{-1})\,d^\times x\,d^\times y \\
&= \int\int_{F^\times\times F^\times} f(yz)\hat{g}(y)|y|\omega(z)\,d^\times y\,d^\times z \\
&= \int_{F^\times}\omega(z)\left(\int_{F^\times} f(yz)\hat{g}(y)|y|\,d^\times y\right)d^\times z \\
&= \int_{F^\times}\omega(z)\int_{F^\times} f(yz)|y|\int_F g(u)\psi(-uy)\,du\,d^\times y\,d^\times z \\
&= \int_{F^\times}\omega(z)\int_{F^\times}\int_F f(v)|vz^{-1}|g(u)\psi(-uvz^{-1})\,du\,d^\times v\,d^\times z \\
&= \int_{F^\times}\omega(z)|z^{-1}|\int_F\int_F f(v)g(u)\psi(-uvz^{-1})\,du|v|\,d^\times v\,d^\times z \\
&= C\int_{F^\times}\omega(z)|z^{-1}|\int_F\int_F f(v)g(u)\psi(-uvz^{-1})\,du\,dv\,d^\times z
\end{aligned}$$

Comme $|v|\,d^\times v$ est, à un facteur scalaire non nul $C>0$, la mesure de Haar dv sur F, on voit bien que la quatité est symétrique en f et g. □

Finalement, nous avons prouvé le résultat suivant.

Théorème 4.2.4 (Tate)**.** *Pour toute $f\in\mathcal{S}(F)$, la fonction $\omega\mapsto Z(f,\omega)$ possède un prolongement méromorphe sur l'espace de tous les caractères de $F^\times$. De plus, il existe une fonction méromophe inversible $\omega\mapsto\gamma(\psi,\omega)$ telle que*

$$Z(f,\omega)=\gamma(\psi,\omega)Z(\hat{f},\widetilde{\omega})$$

pour tout ω.

Démonstration. Il suffit de prouver que pour tout caractère unitaire ω_0 de $F^\times$, il existe une fonction $g\in\mathcal{S}(F)$ telle que that $Z(\hat{g},\omega_0^{-1}|\cdot|^{1-s})$ and $Z(g,\omega_0|\cdot|^s)$ sont méromorphe en $s\in\mathbb{C}$ et non nulles. En effet, on choisit alors $\gamma(\psi,\omega_0|\cdot|^s)=\frac{Z(g,\omega_0|\cdot|^s)}{Z(\hat{g},\omega_0^{-1}|\cdot|^{1-s})}$. Notons qu'il suffit de trouver g telle que la fonction $s\mapsto Z(\hat{g},\omega_0^{-1}|\cdot|^{1-s})$ est non nulle. En effet si $Z(g,\omega_0|\cdot|^s)$ était nulle, on aurait

$$\begin{aligned}
Z(\hat{g},\omega_0^{-1}|\cdot|^{1-s})Z(\hat{g},\omega_0|\cdot|^s) &= Z(g,\omega_0^{-1}|\cdot|^{1-s})Z(\hat{\hat{g}},\omega_0|\cdot|^z) \\
&= \omega_0(-1)Z(g,\omega_0|\cdot|^{1-s})Z(\omega_0|\cdot|^{1-s})=0
\end{aligned}$$

et il en serait de même de $s\mapsto Z(\hat{g},\omega_0^{-1}|\cdot|^{1-s})$.

Pour trouver g, considérons séparément le cas où ω_0 est non ramifié et le cas où ω_0 est ramifié.

Supposons ω_0 non ramifié. On peut alors supposer que $\omega_0 = 1$. On peut choisir g telle que $\hat{g} = \mathbb{1}_{\mathcal{O}_F}$. En effet, on a déjà calculé (remarque 4.2.2) que

$$Z(\mathbb{1}_{\mathcal{O}_F}, |\cdot|^{1-s}) = \mathrm{Vol}(\mathcal{O}_F^\times)\frac{1}{1-q_F^{s-1}}$$

qui est bien non nulle.

Supposons que ω_0 est ramifié et choisissons g telle que $\hat{g} = \mathbb{1}_{1+\mathfrak{p}_F^m}$ où $\mathfrak{p}_F^m$ est le conducteur de ω_0 (et donc de ω_0^{-1}). On a alors

$$Z(\hat{g}, \omega_0^{-1}|\cdot|^{1-s}) = \mathrm{Vol}(1+\mathfrak{p}_F^m) \neq 0. \qquad \square$$

Si ω désigne un caractère de $F^\times$, on définit sa *fonction L locale* par la formule

$$L(\omega) \coloneqq \begin{cases} \frac{1}{1-q_F^{-s}} & \text{si } \omega = |\cdot|^s \text{ is unramified} \\ 1 & \text{si } \omega \text{ is ramified.} \end{cases}$$

Les calculs précédents montrent que, pour toute fonction $f \in \mathcal{S}(F)$, la fonction $\omega \mapsto L(\omega)^{-1}Z(f,\omega)$ est holomorphe en ω. Autrement dit, pour tout caractère unitaire ω_0 de $F^\times$, la fonction $s \mapsto L(\omega_0|\cdot|^s)^{-1}Z(f,\omega_0|\cdot|^s)$ est holomorphe en s.

On définit alors le *facteur epsilon* de ω par la formule

$$\varepsilon(\psi,\omega) \coloneqq \gamma(\psi,\omega)\frac{L(\widetilde{\omega})}{L(\omega)}.$$

L'équation fonctionnelle locale (théorème 4.2.4) se réécrit

$$\forall f \in \mathcal{S}(F), \quad \forall \omega, \quad \frac{Z(f,\omega)}{L(\omega)} = \varepsilon(\psi,\omega)\frac{Z(\hat{f},\widetilde{\omega})}{L(\widetilde{\omega})}.$$

De plus, la fonction $\omega \mapsto \varepsilon(\psi,\omega)$ est holomorphe et inversible.

Proposition 4.2.5. *Soit ω un carcatère de $F^\times$, on a alors : formulas.*

(i) $\gamma(\psi,\omega)\gamma(\psi,\widetilde{\omega}) = \omega(-1)$ *;*

(ii) $\gamma(\psi,\overline{\omega}) = \omega(-1)\overline{\gamma(\psi,\omega)}$ *;*

(iii) si $\sigma(\omega) = \frac{1}{2}$*, alors* $|\gamma(\psi,\omega)| = 1$.

Démonstration. (...) $\square$

Remarque 4.2.6. Les facteurs γ et ε peuvent être explicités complètement. Soit (π_F^d) le conducteur de ψ. On a alors

$$\varepsilon(\psi, |\cdot|^s) = q_F^{d(\frac{1}{2}-s)}$$

et, si ω_0 est un caractère unitaire ramifié de $F^\times$, de conducteur $\mathfrak{p}_F^m$, vérifiant de plus $\omega_0(\pi) = 1$, alors

$$\varepsilon(\psi, \omega_0|\cdot|^s) = q_F^{(d-m)(\frac{1}{2}-s)} q_F^{-\frac{m}{2}} G(\psi, \omega_0)$$

où $G(\psi, \omega_0)$ est la "somme de Gauss"

$$G(\psi, \omega_0) = \sum_{a \in (\mathcal{O}_F/\mathfrak{p}_F^m)^\times} \omega_0(a)\psi(\pi_F^{d-m}a).$$

La proposition 4.2.5 montre alors que $|G(\psi, \omega_0)| = q_F^{\frac{n}{2}}$. Si $n = 1$, on retrouve le résultat classique concernant les sommes de Gauss sums du corps fini k_F.

4.2.3 Le cas des corps locaux archimédiens

L'énoncé du théorème 4.2.4 reste valable si l'on remplace F par $\mathbb{R}$ ou $\mathbb{C}$ à condition de faire les modifications ci-dessous. Nous laissons les calculs et démonstrations en exercice.

Si $F = \mathbb{R}$, posons

$$L(|\cdot|^s) \coloneqq \pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2}), \quad L(\mathrm{sgn}|\cdot|^s) \coloneqq L(|\cdot|^{s+1}).$$

On a alors

$$\varepsilon(\psi_\mathbb{R}, |\cdot|^s) = 1, \quad \varepsilon(\psi_\mathbb{R}, \mathrm{sgn}|\cdot|^s) = -i$$

(rappelons que $\psi_\mathbb{R}$ est le caractère $x \mapsto e^{-2\pi i x}$.

Si $F = \mathbb{C}$ et $n \in \mathbb{Z}$, on définit θ_n par $z \mapsto (z\overline{z}^{-1})^{\frac{n}{2}}$. Il s'agit d'un carcatère unitaire de $\mathbb{C}^\times$ et tout caractère de $\mathbb{C}^\times$ est équivalent à θ_n pour un unique $n \in \mathbb{Z}$. On pose

$$L(\theta_n|\cdot|_\mathbb{C}^s) \coloneqq (2\pi)^{1-s+\frac{|n|}{2}}\Gamma\left(s + \frac{|n|}{2}\right).$$

On a alors

$$\varepsilon(\psi_\mathbb{C}, \theta_n|\cdot|_\mathbb{C}^s) = i^{-|n|}.$$

Rappelons que $\psi_\mathbb{C}$ est le caractère $\psi_\mathbb{R} \circ \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}$ de $\mathbb{C}$ et que $|\cdot|_\mathbb{C} = |\cdot|_\mathbb{R} \circ N_{\mathbb{C}/\mathbb{R}} = |\cdot|^2$.

4.3 Fonctions zêta globales

4.3.1 La formule d'inversion dans le cas compact

Soit G un groupe abélien compact. Son dual $\widehat{G}$ est donc discret d'après le théorème 4.1.1. On munit G de la mesure de Haar dg de volume 1. Nous allons

voir que la mesure duale correspondante sur $\widehat{G}$ est la mesure de comptage. Nous supposons de plus que si $g \in G$, il existe $\chi \in \widehat{G}$ tel que $\chi(g) \neq 1$. C'est une conséquence du théorème 4.1.3, mais nous allons démontrer directement le résultat qui suit sans faire appel à ce résultat plus fort.

Remarque 4.3.1. On peut vérifier que le groupe $\mathbb{A}_F/F$ vérifie la propriété précédente en utilisant le corollaire 4.1.15.

Théorème 4.3.2. *Soit $f \in L^1(G)$ telle que $\widehat{f}$ est une fonction sommable sur $\widehat{G}$. Alors pour presque tout $g \in G$, on a*

$$f(g) = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(g).$$

Démonstration. La sous-algèbre de l'ensemble des fonctions continues de G dans $\mathbb{C}$ formée des combinaisons linéaires d'éléments de $\widehat{G}$ vérifie les hypothèses du théorème de Stone et est donc dense dans $\mathcal{C}(G, \mathbb{C})$ pour la norme de la borne supérieure. On montre alors que la fonction $f - \sum_\xi \widehat{f}(\chi)\chi$ est orthogonale à cette sous-algèbre pour le produit scalaire

$$\langle u, v \rangle = \int_G \overline{u(g)} v(g)\, dg.$$

On en conclut que cette fonction est orthogonale à $\mathcal{C}(G, \mathbb{C})$ dans $L^1(G)$, qui est dense dans $L^1(G)$, et on obtient le résultat. □

4.3.2 Formule de Poisson

Lemme 4.3.3. *Soit $f \in \mathcal{S}(\mathbb{A}_F)$. Alors la série de fonctions*

$$x \longmapsto \sum_{\xi \in F} f(x + \xi)$$

est normalement convergente sur tout compact de $\mathbb{A}_F$.

Démonstration. Comme f est une combinaison linéaire finie de fonctions de la forme $f_\infty \otimes \mathbb{1}_U$ où U est un ouvert compact de $\mathbb{A}_f$ et $f_\infty \in \mathcal{S}(F_\infty)$, il suffit de prouver le lemme pour les fonctions de ce type. Soit K une partie compacte de $\mathbb{A}_F$. Quitte à agrandir K, on peut supposer que K est de la forme $K_\infty \times \prod_{v \in S} \pi_v^{m_v} \mathcal{O}_{F_v} \times \prod_{v \notin S} \mathcal{O}_{F_v}$ où $S \subset \Sigma \smallsetminus \Sigma_\infty$ est fini, $m_v \in \mathbb{Z}$ pour $v \in S$ et $U \subset \prod_{v \in S} \pi_v^{m_v} \mathcal{O}_{F_v} \times \prod_{v \notin S} \mathcal{O}_{F_v}$. Soit Λ l'image dans F_∞ de $F \cap \prod_{v \in S} \pi_v^{m_v} \mathcal{O}_{F_v} \times \prod_{v \notin S} \mathcal{O}_{F_v}$. Alors Λ est un réseau de

$F_\infty \simeq \mathbb{R}^{[F:\mathbb{Q}]}$. Pour $\xi \in F$, si la fonction $x \mapsto f_\xi(x) \coloneqq f(x+\xi)$ est non nulle, alors $\xi \in \Lambda$. On en conclut que

$$\sum_{\xi\in F} \sup_K |f_\xi| \leqslant \sum_{\xi\in\Lambda} \sup_{K_\infty} |f_{\infty,\xi}|.$$

Comme $f_v \in \mathcal{S}(F_v)$ pour tout $v \in \Sigma_\infty$, on a $f_\infty(x) = O(\|x\|^{-[F:\mathbb{Q}]+1})$ pour $x \in F_\infty$ (où $\|\cdot\|$ désigne une norme sur le $\mathbb{R}$-espace vectoriel F_∞). On en conclut que la série de fonctions $\sum_{\xi\in F} f_\xi$ converge normalement sur K. □

Théorème 4.3.4 (Poisson formula)**.** *Pour $f \in \mathcal{S}(\mathbb{A}_F)$, on a*

(i) $\sum_{\xi\in F} f(\xi) = \sum_{\xi\in F} \hat{f}(\xi)$;

(ii) et pour tout $a \in I_F$, $|a| \sum_{\xi\in F} f(a\xi) = \sum_{\xi\in F} \hat{f}(a^{-1}\xi)$.

Démonstration. La formule (ii) se déduit facilement de la formule (i) appliquée à la fonction $x \mapsto f(ax)$. Prouvons donc (i). D'après le lemme 4.3.3, la série $\sum_\xi f(x+\xi)$ est normalement convergente pour x variant dans une partie compacte de $\mathbb{A}_F$, la fonction $x \mapsto g(x) \coloneqq \sum_{\xi\in F} f(x+\xi)$ est continue sur $\mathbb{A}_F/F$. Comme $\mathbb{A}_F/F$ est compact (théorème 3.1.5), la fonction g est intégrable. Calculons ses coefficients de Fourier (c'est-à-dire la fonction $\hat{g}$ sur l'espace discret $\widehat{\mathbb{A}_F/F}$). Le corollaire 4.1.15 nous permet d'identifier $\widehat{\mathbb{A}_F/F}$ à F. Plus précisément on fixe ψ un caractère unitaire non trivial de $\mathbb{A}_F$ trivial sur F. On associe alors $\xi \in F$ le caractère $\psi_\xi : x \mapsto \psi(\xi x)$ de $\mathbb{A}_F/F$. Soit $D \subset \mathbb{A}_F$ un domaine fondamental compact de $\mathbb{A}_F/F$ (qui existe d'après la démonstration du théorème 3.1.11). Pour $\xi \in F$, on a, en utilisant la proposition B.5.4,

$$\begin{aligned}\hat{g}(\xi) &= \int_{\mathbb{A}_F/F} g(x)\psi(-\xi x)\,dx = \int_{\mathbb{A}_F/F} \sum_{u\in F} f(x+u)\psi(-\xi x)\,dx \\ &= \int_{\mathbb{A}_F} f(x)\psi(-\xi x)\,dx = \hat{f}(\xi).\end{aligned}$$

On a $\hat{f} \in \mathcal{S}(\mathbb{A}_F)$ d'après la proposition 4.1.23. La série $\sum_{\xi\in F} \hat{g}(\xi)$ est donc absolument convergente et la formule d'inversion de Fourier implique

$$\forall x \in \mathbb{A}_F/F, \quad g(x) = \sum_{\xi\in F} \hat{f}(\xi)\psi(\xi x).$$

On obtient la formule (i) en évaluant cette égalité en $x = 0$. □

4.3.3 Intégrales sur I_F

Rappelons que si $z \in \mathbb{C}$ vérifie $|z-1| < 1$, alors on pose

$$\log(z) = \sum_{n\geqslant 1} \frac{(-1)^{n-1}}{n}(z-1)^n.$$

Soit $(x_v)_{v\in\Sigma}$ une famille de nombres complexes non nuls indexée par un ensemble Σ. On dit que le produit $\prod_{v\in\Sigma} x_v$ est *absolument convergent* si la famille $(|x_v - 1|)_{v\in\Sigma}$ est sommable. Dans ce cas, le produit infini $\prod_{v\in\Sigma} x_v$ existe comme un élément de $\mathbb{C}^\times$. En effet, il existe une partie finie $S \subset \Sigma$ telle que $|x_v - 1| < 1$ pour $v \notin S$. Comme $|\log(x_v)| \sim |x_v - 1|$ quand v varie parmi les complémentaires des parties finies de $\Sigma \setminus S$, la série $\sum_{v\notin S} \log(x_v)$ converge absoluement. On pose alors

$$\prod_{v\in\Sigma} x_v \coloneqq \left(\prod_{v\in S} x_v\right) \exp\left(\sum_{v\notin S} \log(x_v)\right).$$

Dans ce cas la famille $(\prod_{v\in S} x_v)_{S\subset\Sigma}$ indexée par les parties finies $S \subset \Sigma$ converge vers $\prod_{v\in\Sigma} x_v$ pour le filtre des complémentaires des parties finies. Autrement dit pour tout $\varepsilon > 0$, il existe une partie finie $S_0 \subset \Sigma$ telle que, pour toute partie finie $S \supset S_0$, on a $|\prod_{v\in S} x_v - \prod_{v\in\Sigma} x_v| \leqslant \varepsilon$.

On considère désormais une famille de groupes localement compacts G_v indexée par $v \in \Sigma$, une partie finie $\Sigma_\infty \subset \Sigma$ et, pour tout $v \notin \Sigma_\infty$ un sous-groupe compact ouvert $H_v \subset G_v$. Pour tout $v \in \Sigma$, on fixe une mesure de Haar (à gauche) dg_v sur G_v telle que que $\int_{H_v} dg_v = 1$ pour presque tout $v \notin \Sigma_\infty$. Soit $dg = \bigotimes_{v\in\Sigma} dg_v$ la mesure produit sur $G \coloneqq \prod'_v G_v$.

Lemme 4.3.5. *Pour $v \in \Sigma$ et soit f_v une fonction continue et intégrable sur G_v. Supposons que $f_v|_{H_v} = \mathbb{1}_{H_v}$ pour presque tout $v \notin \Sigma_\infty$ et définissons $f((g_v)) \coloneqq \prod_v f_v(g_v)$ sur G. Si le produit $\prod_v \int_{G_v} |f_v(g_v)|\, d^\times g_v$ est absolument convergent, alors la fonction f est intégrable sur G et*

$$\int_G f(g)\, d^\times g = \prod_v \int_{G_v} f_v(g_v)\, d^\times g_v.$$

Démonstration. On démontre le résultat en utilisant le théorème de convergence dominée. Soit S_0 l'ensemble fini des v tels que $v \in \Sigma_\infty$ ou $f_v|_{H_v} \neq \mathbb{1}_{H_v}$. Pour toute partie finie S de Σ contenant S_0, posons

$$G_S = \prod_{v\in S} G_v \times \prod_{v\notin S} H_v.$$

Alors G est l'union des ouverts G_S. Pour un tel S notons dg_S la mesure de Haar $\bigotimes_{v\in S} dg_v$ sur G_S. Si on prouve qu'il existe un réel $C > 0$ tel que $\int_{G_S} |f(g)|\, dg_S \leqslant C$ pour tout $S \supset S_0$, alors le théorème de convergence dominée implique que f est intégrable et que

$$\int_G f(g)\, dg = \lim_{S_0\subset S\subset\Sigma} \int_{G_S} f(g_S) \otimes_{v\in S} dg_S.$$

Or l'inclusion $S \supset S_0$ et la proposition 3.1.10 impliquent que

$$\int_{G_S} |f(g)| = \prod_{v \in S} \int_{G_v} |f_v(g_v)| \, dg_v.$$

En particulier la famille des $\prod_{v\in S} \int_{G_v} |f_v(g_v)| \, dg_v$ est bornée. On en conclut l'existence de $C > 0$. De plus la famille des $\left(\int_{G_v} |f_v(g_v)| \, dg_v - 1\right)_v$ est sommable si et seulement si la famille des $\left(\int_{G_v \smallsetminus H_v} |f_v(g_v)| \, dg_v\right)_{v \notin \Sigma_\infty}$ est sommable. En particulier la famille $\left(\left|\int_{G_v \smallsetminus H_v} f_v(g_v) \, dg_v\right|\right)_{v \notin \Sigma_\infty}$ est sommable, ce qui implique que le produit $\prod_v \int_{F_v^\times} f_v(g_v) \, dg_v$ est absolument convergent. On en déduit donc

$$\int_G f(g) \, dg = \lim_S \prod_{v \in S} \int_{G_v} f_v(g_v) \, dg_v = \prod_v \int_{G_v} f_v(g_v) \, dg_v. \qquad \square$$

Nous appliquerons en particulier ce résultat au cas où $G = I_F$, $G_v = F_v^\times$ et $H_v = \mathcal{O}_{F_v}^\times$.

4.3.4 Caractères de Hecke, fonctions zêta globales

Un *caractère de Hecke* est un caractère du groupe localement compact $I_F/F^\times$, c'est-à-dire un morphisme de groupes continu $\chi : I_F/F^\times \to \mathbb{C}^\times$. Si χ est un caractère de Hecke, pour toute place v de F, la précomposition de χ avec l'inclusion $F_v^\times \hookrightarrow I_F$ est un caractère χ_v de $F_v^\times$. On déduit de la continuité de χ que χ_v est non ramifié pour presque toute place v. Réciproquement si $(\chi_v)_{v\in\Sigma}$ est une famille de caractères de $F_v^\times$ telle que presque tous les χ_v sont non ramifiée, on définit un caractère χ de I_F par la formule

$$\chi((x_v)_v) \coloneqq \prod_{v \in \Sigma_F} \chi_v(x_v).$$

Cependant ce caractère n'est pas toujours un caractère de Hecke, il faut de plus supposer que $\chi(F^\times) = \{1\}$.

Proposition 4.3.6. *Soit χ un caractère de Hecke. Alors il existe un nombre réel $\sigma_\chi \in \mathbb{R}$ tel que*

$$\forall x \in I_F, \quad |\chi(x)| = |x|^{\sigma_\chi}.$$

Démonstration. C'est une conséquence de la compacité de $I_F^1/F^\times$ (théorème 3.2.4). En effet, on en déduit $\chi(I_F^1/F^\times) \subset S^1$ de sorte que $|\chi|$ se factorise à travers l'application norme. $\square$

En conséquence, si χ est un caractère de Hecke de composantes locales χ_v, $v \in \Sigma$, le nombre réel σ_{χ_v} est indépendant du choix de v.

Fixons une mesure de Haar $d^\times x$ on I_F de la forme $\bigotimes_v d^\times x_v$ où $d^\times x_v$ est une mesure de Haar sur $F_v^\times$ telle que $\int_{\mathcal{O}_{F_v}^\times} d^\times x_v = 1$ pour presque toute v. Si $f \in \mathcal{S}(\mathbb{A}_F)$ et χ est un caractère de Hecke character, on définit l'*intégrale zêta globale* $Z(f,\chi)$ associée à f et χ par la formule

$$Z(f,\chi) \coloneqq \int_{I_F} f(x)\chi(x)\, d^\times x$$

(lorsqu'elle est convergente).

Proposition 4.3.7. *Si $\sigma_\chi > 1$, l'intégrale $Z(f,\chi)$ est absolument convergente.*

Démonstration. Supposons donc $\sigma_\chi > 1$. On peut supposer que f est de la forme $\bigotimes_v f_v$ où $f_v \in \mathcal{S}(F_v)$ et $f_v = \mathbb{1}_{\mathcal{O}_v}$ pour $v \notin S$ où S est un ensemble fini de places de F contenant Σ_∞. Quitte à agrandir S, on peut même supposer que χ_v est non ramifié et que $\int_{\mathcal{O}_{F_v}^\times} d^\times x_v = 1$ pour $v \notin S$. Pour chaque v, on déduit du lemme 4.2.1 que l'intégrale zêta locale $\int_{F_v^\times} f_v(x)\chi_v(x)\, d^\times x_v$ est absolument convergente, puisque $\sigma_{\chi_v} = \sigma_\chi > 1 > 0$. Il est donc suffisant de vérifier la convergence absolue du produit product

$$\prod_{v\notin S} \int_{F_v^\times} |f_v(x_v)\chi_v(x_v)|\, d^\times x_v = \prod_{v\notin S} \int_{\mathcal{O}_v} |\chi_v(x_v)|\, d^\times x_v.$$

Or χ_v est non ramifié dès que $v \notin S$. On a donc $|\chi_v| = |\cdot|_v^{\sigma_\chi}$ et $\int_{\mathcal{O}_v} |\chi_v(x_v)|\, d^\times x_v = \frac{1}{1-q_v^{-\sigma_\sigma}}$ (voir remarque 4.2.2). Le résultat se déduit donc du lemme suivant. □

Lemme 4.3.8. *Le produit $\prod_{v\notin S} \frac{1}{1-q_v^{-\sigma}}$ est absolument convergent pour $\sigma > 1$.*

Démonstration. Supposons dans un premier temps $F = \mathbb{Q}$, on a alors $\frac{1}{1-p^{-\sigma}} - 1 = \frac{p^{-\sigma}}{1-p^{-\sigma}} \leqslant 2p^{-\sigma}$ et il est bien connu que $\sum_p p^{-\sigma} < +\infty$ dès que $\sigma > 1$. Si F est un corps de nombres, on a, pour tout idéal maximal $\mathfrak{p}$ de $\mathcal{O}_F$, $\frac{1}{1-N\mathfrak{p}^{-\sigma}} - 1 \leqslant 2N\mathfrak{p}^{-\sigma}$. De plus $\mathrm{Card}\,\{\mathfrak{p} \mid p\} \leqslant [F:\mathbb{Q}]$ pour tout nombre premier p. Ainsi on a

$$\sum_{\mathfrak{p}} N\mathfrak{p}^{-\sigma} \leqslant [F:\mathbb{Q}] \sum_p p^{-\sigma} < +\infty$$

si $\sigma > 1$.

Le cas des corps de fonctions est laissé en exercice. □

4.3.5 L'équation fonctionnelle globale

On déduit facilement de la convergence absolue des intégrales zêta globales pour $\sigma_\chi > 1$ que la fonction $\chi \mapsto Z(f,\chi)$ est holomorphe sur l'ensemble des caractères de Hecke χ vérifiant $\sigma_\chi > 1$. Plus précisément, si χ_0 désigne un caractère de Hecke unitaire, la fonction $s \mapsto Z(f, \chi_0|\cdot|^s)$ est bien définie et est holomorphe sur l'ouvert $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\}$.

Remarque 4.3.9. Si F est un corps de fonctions, et si $|I_F| = q^{\mathbb{Z}}$, la fonction $s \mapsto Z(f,s)$ est invariant par addition d'éléments du groupe $\frac{2\pi i}{\log q}$.

Nous aurons besoin du lemme suivant.

Lemme 4.3.10. *Soit $f \in \mathcal{S}(\mathbb{A}_F)$ et soit K une partie compacte de I_F. Alors la série $\sum_{\xi \in F^\times} f(y\xi)$ est normalement convergente pour $y \in K$.*

Théorème 4.3.11. *Soit $f \in \mathcal{S}(\mathbb{A}_F)$.*

(1) La fonction $\chi \mapsto Z(f,\chi)$ possède une unique extension méromophe à l'ensemble des caractères de Hecke characters et vérifie l'équation fonctionnelle suivante

$$Z(f,\chi) = Z(\hat{f}, \widetilde{\chi})$$

où $\widetilde{\chi} := |\cdot|\chi^{-1}$ et la transformée de Fourier $\hat{f}$ est relative à la mesure autoduale sur $\mathbb{A}_F$.

(2) Si χ_0 est un caractère de Hecke tel que $\chi_0(I_F^1) \neq \{1\}$, alors la fonction méromorphe $s \mapsto Z(f, \chi_0|\cdot|^s)$ est holomorphe (elle ne possède aucun pôle).

(3) Supposons que F est un corps de nombres. Alors la fonction $s \mapsto Z(f, |\cdot|^s)$ est holomorphe sur $\mathbb{C} \smallsetminus \{0,1\}$. De plus, tous ses pôles sont simples et sont inclus dans l'ensemble $\{0,1\}$. Si la fonction possède un pôle simple en 0 (resp. 1), le résidu y est $-\kappa f(0)$ (resp. $\kappa \hat{f}(0)$), où κ désigne le nombre $\int_{I_F^1/F^\times} d^\times x$.

(4) Supposons que F est un corps de fonctions et soit $q \in \mathbb{Z}_{\geqslant 1}$ tel que $|I_F| = q^{\mathbb{Z}}$. Alors la fonction $s \mapsto Z(f, |\cdot|^s)$ est holomorphe sur $\mathbb{C} \smallsetminus (\frac{2\pi i}{\log q}\mathbb{Z} \cup 1 + \frac{2\pi i}{\log q})$. De plus, tous ses pôles sont simples et sont inclus dans l'ensemble $\{0,1\}$. Si la fonction possède un pôle simple en 0 (resp. 1), le résidu y est $-\kappa f(0)$ (resp. $\kappa \hat{f}(0)$), où κ désigne le nombre $\int_{I_F^1/F^\times} d^\times x$.

Démonstration. Dans la démonstration nous supposons que F est un corps de nombres. Dans le cas d'un corps de fonctions, la démosntration est

Fixons χ_0 un caractère de Hecke *unitaire* (en particulier $\sigma_{\chi_0} = 0$) et montrons que la fonction $s \mapsto Z(f, \chi_0|\cdot|^s)$ a les propriétés recherchées. On $Z(f, \chi_0^s) = I(s) +$

$II(s)$ où

$$I(s) = \int_{|x|<1} f(x)\chi_0(x)|x|^s \, d^\times x, \quad II(s) = \int_{|x|\geqslant 1} f(x)\chi_0(x)|x|^s \, d^\times x.$$

D'après la proposition 4.3.7, l'intégrale définissant la fonction $s \mapsto II(s)$ est absolument convergente sur tout compact du domaine $\{\mathrm{Re}(s) > 1\}$ et la fonction $s \mapsto II(s)$ est holomorphe sur ce domaine. Si $\mathrm{Re}(s) \leqslant 1$, on a $|f(x)||x^s| \leqslant |f(x)||x|^2$ pour $|x| \geqslant 1$, de sorte que l'intégrale $\int_{|x|\geqslant 1}|f(x)||x^s| \, d^\times x$ est dominée sur le domaine $\{\mathrm{Re}(s) \leqslant 1\}$ et donc la fonction $s \mapsto II(s)$ est définie et holomorphe sur $\mathbb{C}$.

Notons $v : |I_F| \to I_F$ la section de la norme d'idèle considérée dans la preuve du lemme 3.2.3. On a alors, pour $\mathrm{Re}(s) > 1$,

$$I(s) = \int_0^1 \int_{I_F^1} f(xv(t))\chi_0(xv(t))t^s \, d^1x \frac{dt}{t}.$$

Remarquons que, quitte à remplacer s par $s - i\alpha$ pour un certain $\alpha \in \mathbb{R}$, on peut toujours supposer que $\chi_0(v(t)) = 1$ pour tout $t \in |I_F|$. On a donc

$$I(s) = \int_0^1 t^s \int_{I_F^1} f(xv(t))\chi_0(x) \, d^1x \frac{dt}{t}.$$

Soit D un domaine fondamental compact pour le quotient $I_F^1/F^\times$ (dont l'existence a été démontrée dans la section 3.2.4). On a alors

$$\int_{I_F^1} f(xv(t))\chi_0(x) \, d^1x = \sum_{\xi\in F^\times} \int_D f(\xi xv(t))\chi_0(x) \, d^1x = \int_D \sum_{\xi\in F^\times} f(\xi xv(t))\chi_0(x) \, d^1x.$$

En effet la série $\sum_{\xi\in\mathbb{F}^\times} f(\xi y)$ converge normalement sur tout compact de I_F. On peut donc écrire

$$I(s) + \int_0^1 t^s \int_D f(0)\chi_0(x) \, d^1x \frac{dt}{t} = \int_0^1 \int_D \sum_{\xi\in F} f(\xi v(t)x)\chi_0(x) \, d^1x \frac{dt}{t}.$$

En utilisant le lemme 4.1.21, on peut écrire

$$\int_0^1 t^s \int_D f(0)\chi_0(x) \, d^1x \frac{dt}{t} = \kappa f(0)\delta\tfrac{1}{s}$$

où $\delta = \begin{cases} 1 & \text{si } \chi_0(I_F^1) = \{1\} \\ 0 & \text{sinon.} \end{cases}$. Ainsi

$$I(s) + \kappa f(0)\delta\frac{1}{s} = \int_0^1 t^s \int_D \sum_{\xi\in F} f(\xi v(t)x)\chi_0(x) \, d^1x \frac{dt}{t}.$$

En utilisant la formule de Poisson (théorème 4.3.4), on a

$$\begin{aligned} I(s) + \kappa f(0)\delta\frac{1}{s} &= \int_0^1 t^{s-1} \int_D t \sum_{\xi\in F} f(\xi v(t)x)\chi_0(x)\, d^1x \frac{dt}{t} \\ &= \int_0^1 t^{s-1} \int_D \sum_{\xi\in F} \hat{f}(\xi v(t)x)\chi_0(x)\, d^1x \frac{dt}{t} \\ &= \int_1^{+\infty} t^{1-s} \int_{D^{-1}} \sum_{\xi\in F} \hat{f}(\xi v(t)x)\chi_0^{-1}(x)\, d^1x \frac{dt}{t} \\ &= \int_{|x|\geqslant 1} \hat{f}(x)\chi_0^{-1}(x)|x|^{1-s}\, d^\times x + \hat{f}(0)\kappa\delta\frac{1}{s-1} \end{aligned}$$

En particulier la fonction $s \mapsto I(s) + \kappa f(0)\delta\frac{1}{s} - \kappa\hat{f}(0)\delta\frac{1}{s-1}$ se prolonge en une fonction holomorphe sur $\mathbb{C}$. On en déduit que la fonction $s \mapsto Z(f, \chi_0|\cdot|^s)$ possède un prolongement méromorphe à $\mathbb{C}$. On en déduit aussi immédiatement que si $\chi_0(I_F^1) \neq \{1\}$, on a $\delta = 0$ et que le prolongement est holomorphe. Enfin, pour tout $s \notin \mathbb{C}$, on a l'égalité

$$\begin{aligned} Z(f, \chi_0|\cdot|^s) = \int_{|x|\geqslant 1} \hat{f}(x)\chi_0^{-1}(x)|x|^{1-s}\, d^\times x + \int_{|x|\geqslant 1} f(x)\chi_0(x)|x|^s\, d^\times x \\ - \kappa\delta\left(\frac{\hat{f}(0)}{1-s} + \frac{f(0)}{s}\right) \end{aligned}$$

qui implique l'équation fonctionnelle et l'assertion concernant les pôles et résidus. □

4.3.6 Fonctions L globales

Soit $\chi : I_F/F^\times \to \mathbb{C}^\times$ un caractère de Hecke. Notons S_χ l'ensemble des places v de F telles que $v \mid \infty$ ou χ_v est ramifié en v (c'est-à-dire $\chi_v(\mathcal{O}_{F_v}^\times \neq \{1\})$. Notons I_F^S le produit restreint des groupes $F_v^\times$ pour $v \notin S$ relativement aux sous-groupes $\mathcal{O}_{F_v}^\times$. Le groupe I_F^S s'identifie naturellement à un sous-groupe de I_F. Notons $I(F)^S$ le quotient de I_F^S par le sous-groupe compact $\prod_{v\notin S}\mathcal{O}_{F_v}^\times$. D'après la section 3.2.2, le groupe I_F^S s'identifie naturellement au groupe $I(\mathcal{O}_F)^S$ des idéaux fractionnaires de $\mathcal{O}_F$ premiers aux $\mathfrak{p}_v$ pour $v \in S \smallsetminus \Sigma_\infty$ dans le cas des corps de nombres et au groupe $\mathrm{Div}^S(F)$ des diviseurs de F dont le support ne rencontre pas S dans le cas des corps de fonctions. Comme χ est non ramifié hors de S, le caractère $\chi|_{I_F^S}$ se factorise à travers $I(F)^S$ et fournit donc un caractère de $I(F)^S$, que l'on note encore χ.

On note $I(F)_+^S$ le sous-monoïde de $I(F)^S$ engendré par les uniformisante π_v pour $v \notin S$. Il s'identifie alors au monoïde des idéaux $\mathfrak{a} \subset \mathcal{O}_F$ premiers aux $\mathfrak{p}_v$,

$v \in S \smallsetminus \Sigma_\infty$, dans le cas des corps de nombres et au sous-monoïde $\mathrm{Div}_+^S(F)$ de $\mathrm{Div}^S(F)$ constitué des diviseurs *positifs*, c'est-à-dire à coefficients positifs.

On note $L(\chi)$ le nombre, lorsqu'il existe,

$$L(\chi) \coloneqq \sum_{\mathfrak{a} \in I(F)_+^S} \chi(\mathfrak{a}).$$

On adopte très souvent la notation suivante lorsque χ est unitaire. On note

$$L(\chi, s) \coloneqq L(\chi|\cdot|^s).$$

En particulier si F est un corps de nombres, on a

$$L(\chi, s) = \sum_{\mathfrak{a} \in I(\mathcal{O}_F)_+^S} \chi(\mathfrak{a}) N(\mathfrak{a})^{-s}.$$

Et si F est un corps de fonctions et $q \in \mathbb{Z}_{\geqslant 1}$ est tel que $|I_F| = q^{\mathbb{Z}}$, on a

$$L(\chi, s) = \sum_{\mathfrak{a} \in \mathrm{Div}_+^S(F)} \chi(\mathfrak{a}) q^{-s \deg(\mathfrak{a})}.$$

Lorsque χ est unitaire, ces sommes sont absolument convergentes dès $\mathrm{Re}(s) > 1$. On a alors

$$L(\chi, s) = \prod_{v \nmid \infty} L(\chi_v |\cdot|_v^s)$$

(en effet $L(\chi_v|\cdot|_v^s) = 1$ si χ_v est ramifié).

Remarque 4.3.12. Soit S l'ensemble des places finies de F telles que χ_v est ramifié. Si $v \in S$, alors $L(\chi_v|\cdot|_v^s) = 1$. Cependant, si $v \notin S$, alors $\chi_v(\varpi_v)$ ne dépend pas du choix de l'uniformisante ϖ_v of F_v et on note ce nombre $\chi_v(\mathfrak{p}_v)$. On a alors $L(\chi_v|\cdot|_v^s) = \frac{1}{1-\chi_v(\mathfrak{p}_v)N(\mathfrak{p}_v)^{-s}}$. On peut donc réécrire, pour $\mathrm{Re}\, s > 1$,

$$L(\chi, s) = \prod_{v \nmid \infty} \left(\tfrac{1}{1-\chi_v(\mathfrak{p}_v)N(\mathfrak{p}_v)^{-s}} \right).$$

On définit la *fonction L complétée* d'un caractère de Hecke χ par la formule

$$\Lambda(\chi) \coloneqq L(\chi) \prod_{v \mid \infty} L(\chi_v).$$

En d'autres termes, pour χ unitaire et $s \in \mathbb{C}$,

$$\Lambda(\chi, s) = L(\chi, s) \prod_{v \mid \infty} L(\chi_v |\cdot|_v^s).$$

On fixe à présent ψ a caractère unitaire non trivial de $\mathbb{A}_F/F$. On définit alors le *facteur* ε de χ par la formule

$$\varepsilon(\chi) = \prod_v \varepsilon(\psi_v, \chi_v)$$

avec, comme toujours, la variante, pour χ unitaire et $s \in \mathbb{C}$,

$$\varepsilon(\chi, s) = \prod_v \varepsilon(\psi_v, \chi_v|\cdot|_v^s).$$

Ce produit est bien défini car il s'agit d'un produit fini : $\varepsilon(\psi_v, \chi_v) = 1$ si χ_v est non ramifié et si le conducteur de ψ_v est $\mathcal{O}_v$ (remarque 4.2.6). Nous verrons également un peu plus loin que, comme la notation le suggère, ce produit ne dépend pas du choix de ψ.

Dans la suite on munit $\mathbb{A}_F$ de la mesure de Tamagawa (mesure autoduale pour ψ mais indépendante de ψ) et on utilise ψ pour identifier $\mathbb{A}_F$ à son dual (dans la transformée de Fourier).

Théorème 4.3.13 (Hecke, Tate)**.** *Soit χ un caractère de Hecke unitaire. La fonction $s \mapsto \Lambda(\chi, s)$ s'étend de façon unique en une fonction méromorphe sur $\mathbb{C}$ et vérifie l'équation fonctionnelle suivante*

$$\Lambda(\chi^{-1}, 1-s) = \varepsilon(\chi, s)\Lambda(\chi, s).$$

De plus si $\chi(I_F^1) \neq \{1\}$ (de façon équivalente, si le caractère χ n'est pas de la forme $|\cdot|^{it}$ pour un certain $t \in \mathbb{R}$), alors la fonction $s \mapsto \Lambda(\chi, s)$ est holomorphe sur $\mathbb{C}$.

Démonstration. Les théorèmes 4.2.4 et 4.3.11 impliquent formellemnt l'égalité

$$\prod_{v \in \Sigma} \gamma(\psi_v, \chi_v|\cdot|_v^s) = 1$$

qui fournit immédiatement l'égalité recherchée. Cependant ce raisonnement purement formel est délicat à utiliser car les produits $\prod_v L(\chi_v|\cdot|_v^s)$ et $\prod_v L(\chi_v^{-1}|\cdot|_v^{1-s})$ ne convergent pas absolument pour les mêmes valeurs de s. Il faut donc procéder un peu plus délicatement.

Soit S un ensemble fini de places de F contenant les places archimédiennes, les places où χ_v est ramifié, les places où le conducteur de ψ_v est différent de $\mathcal{O}_{F_v}$ et les places où $\int_{\mathcal{O}_{F_v}^\times} d^\times x_v = 1$. Choisissons $f \in \mathcal{S}(\mathbb{A}_F)$ telle que $Z(f, \chi|\cdot|^s) \neq 0$ et de la forme $f = \bigotimes_{v \in S} f_v \otimes \chi^S$. Les formules explicites des sections 4.2.2 et 4.2.3 montrent que c'est possible. On a alors, pour $v \notin S$

$$Z(f_v, \chi_v|\cdot|_v^s) = L(\chi_v|\cdot|_v^s).$$

Ainsi, pour $\operatorname{Re} s > 1$, le quotient $\frac{Z(f,\chi|\cdot|^s}{\Lambda(\chi,s)}$ est égal à un produit fini de fonctions se prolongeant en des fonctions holomorphes sur $\mathbb{C}$:

$$\frac{Z(f,\chi|\cdot|^s)}{\Lambda(\chi,s)} = \prod_{v\in S} \frac{Z(f_v,\chi_v|\cdot|_v^s)}{L(\chi_v|\cdot|_v^s)}.$$

En particulier, on déduit du théorème 4.3.11 que $\Lambda(\chi,s)$ se prolonge à $\mathbb{C}$ en une fonction méromorphe. Si $v \notin S$, on a $\hat{f}_v = f_v$ (d'après les calculs dans la démonstration du théorème 4.1.19). Ainsi

$$\frac{Z(\hat{f},\chi^{-1}|\cdot|^{1-s})}{\Lambda(\chi^{-1},1-s)} = \prod_{v\in S} \frac{Z(\hat{f}_v,\chi_v^{-1}|\cdot|_v^{1-s})}{L(\chi_v^{-1}|\cdot|_v^{1-s})}.$$

On déduit donc des théorèmes 4.2.4 et 4.3.11 que

$$\Lambda(\chi^{-1},1-s) = \varepsilon(\chi,s)\Lambda(\chi,s).$$

Concernant l'holomorphie si $\chi(I_F^1) \neq \{1\}$, il suffit de choisir une fonction f de telle sorte que $Z(f,\chi|\cdot|^s) = \Lambda(\chi,s)$ et d'utiliser le théorème 4.3.11. □

Exemple 4.3.14. Si l'on choisit pour χ le caractère trivial, la fonction $L(\chi,s)$ est également appelée *fonction zêta de Dedekind* du corps F et est notée $\zeta_F(s)$. Lorsque F est un corps de nombres, on a donc, pour $\operatorname{Re} s > 1$,

$$\zeta_F(s) = \sum_{\mathfrak{a}\subset\mathcal{O}_F} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1-N(\mathfrak{p})^{-s}}$$

la somme étant prise sur les idéaux non triviaux de $\mathcal{O}_F$ et le produit sur les idéaux maximaux de $\mathcal{O}_F$. On a alors

$$\Lambda(s) \coloneqq \Lambda(1,s) = (\pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2}))^{r_1}((2\pi)^{1-s}\Gamma(s))^{r_2}\zeta_F(s).$$

Si F est un corps de fonctions de corps des constantes $\mathbb{F}_q$, on a

$$\zeta_F(s) = \sum_{D\in \operatorname{Div}(F)_+} \frac{1}{q^{s\deg(D)}}.$$

Corollaire 4.3.15. *Supposons que F est un corps de nombres. La fonction zêta de Dedekind de F est holomorphe hors de 1 et on a*

$$\zeta_F(s) \sim_{s\to 1} \frac{2^{r_1}(2\pi)^{r_2}h_F R_F}{w_F|\Delta_{F/\mathbb{Q}}|^{\frac{1}{2}}}(s-1)^{-1}.$$

La fonction ζ_F possède un zéro d'ordre r_1+r_2-1 en 0. On a de plus l'équation fonctionnelle

$$\Lambda(1-s) = |\Delta_{F/\mathbb{Q}}|^{s-\frac{1}{2}}\Lambda(s).$$

Remarque 4.3.16. Ce n'est pas totalement un hasard que l'ordre du zéro de la fonction ζ_F en 0 soit le rang du groupe $\mathcal{O}_F^\times$.

Remarque 4.3.17. Les formules de la remarque 4.2.6 et de la section 4.2.3 montrent que, si χ est un caractère de Hecke unitaire, on a

$$\varepsilon(\chi, s) = W(\chi)A^{s-\frac{1}{2}}$$

où $W(\chi)$ est un nombre algébrique tel que $|W(\chi)| = 1$ appelé le « *root number* » et A est un nombre réel positif.

Chapitre 5

Théorie du corps de classe

5.1 Extensions abéliennes de corps p-adiques

Soit p un nombre premier et soit F une extension finie de $\mathbb{Q}_p$. On note $\mathcal{O}_F$ son anneau de valuation, $\mathfrak{p}_F$ l'idéal maximal de $\mathcal{O}_F$ et $k_F \coloneqq \mathcal{O}_F/\mathfrak{p}_F$ le corps résiduel. Soit q_F le cardinal de k_F. On fixe également π_F une uniformisante de F. Posons $U_F \coloneqq \mathcal{O}_F^\times$ et, pour $i \geqslant 0$,

$$U_F^i \coloneqq \begin{cases} U_F & \text{if } i = 0 \\ 1 + \mathfrak{p}_F^i & \text{if } i \geqslant 1. \end{cases}$$

On note également $|\cdot|_F$ la valeur absolue normalisée de F, qui vérifie $|\pi_F| = q_F^{-1}$.

5.1.1 Extensions non ramifiées

Si E/F est une extension non ramifiée de degré d, la restriction à $\mathcal{O}_E$ et la réduction modulo π_E induisent un isomorphisme de groupes $\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(k_E/k_F) \simeq \mathbb{Z}/d\mathbb{Z}$ (proposition 2.3.3). Ce groupe est engendré par l'automorphisme de Frobenius $(\mathfrak{p}_F, E/F)$. Il s'agit de l'unique automorphisme σ de E tel que

$$\forall x \in \mathcal{O}_E, \quad \sigma(x) \equiv x^{q_F} \bmod \mathfrak{p}_E.$$

Il s'agit d'un générateur d'ordre d du groupe de Galois cyclique $\mathrm{Gal}(E/F)$.

Proposition 5.1.1. *Soit E/F une extension finie non ramifiée de degré d. On a alors $N_{E/F}(U_F) = U_F$. On en déduit que $N_{E/F}(E^\times) = \pi_F^{d\mathbb{Z}} U_F$.*

Démonstration. Comme l'extension E/F est galoisienne, on a $N_{E/F}(x) = \prod_{\sigma\in\mathrm{Gal}(E/F)} \sigma(x)$. On en déduit que $N_{E/F}(U_E) \subset U_F$ et que, si $i \geqslant 1$, $\sigma(U_F^i) = U_F^i$ pour tout $\sigma \in \mathrm{Gal}(E/F)$ de sorte que $N_{E/F}(U_E^i) \subset U_E^i \cap U_F = (1+\pi_F^i\mathcal{O}_E)\cap\mathcal{O}_F = 1+\pi_F^i\mathcal{O}_F = U_F^i$ (nous avons utilisé ici le fait que π_F est également une uniformisante de E puisque E/F est non ramifiée). Nous avons donc deux diagrammes commutatifs, $i \geqslant 1$,

$$\begin{array}{ccc} U_E/U_E^1 & \xrightarrow{N_{E/F}} & U_F/U_F^1 \\ \downarrow\wr & & \downarrow\wr \\ k_E^\times & \xrightarrow{N_{k_E/k_F}} & k_F^\times \end{array} \qquad \begin{array}{ccc} U_E^i/U_E^{i+1} & \xrightarrow{N_{E/F}} & U_F^i/U_F^{i+1} \\ \downarrow\wr & & \downarrow\wr \\ k_E & \xrightarrow{\mathrm{Tr}_{k_E/k_F}} & k_F \end{array}$$

En effet, si $x \in \mathcal{O}_E$, on a, pour $i \geqslant 1$,

$$N_{E/F}(1+\pi_F^i x) = \prod_{\sigma\in\mathrm{Gal}(E/F)} (1+\pi_F^i\sigma(x)) \equiv 1 + \pi_F^i \sum_{\sigma\in\mathrm{Gal}(E/F)} \sigma(x) \bmod \mathfrak{p}_F^{i+1}.$$

Comme k_E/k_F est une extension séparable, l'application $\mathrm{Tr}_{k_E/k_F} : k_E \to k_F$ est surjective et il en est de même de $N_{E/F} : U_E^i/U_E^{i+1} \to U_F^i/U_F^{i+1}$ pour tout $i \geqslant 1$. De même, si $x \in k_E^\times$, on a

$$N_{k_E/k_F}(x) = x^{1+q_F+\cdots+q_F^{d-1}}$$

de sorte que N_{k_E/k_F} est surjective (exercice) et donc aussi $N_{E/F} : U_E/U_E^1 \to U_F/U_F^1$. On déduit de ce résultat que l'application $N_{E/F} : U_E/U_E^i \to U_F/U_F^i$ est surjective pour tout i. Si $x \in U_F$, on peut trouver, pour tout $n \geqslant 1$, un élément $y_n \in U_E$ tel que $x - N_{E/F}(y_n) \in \pi_F^n\mathcal{O}_F$. On en déduit l'existence de $y \in \mathcal{O}_E$ tel que $x = N_{E/F}(y)$. □

Corollaire 5.1.2. *Si E/F est une extension finie non ramifiée, le quotient $F^\times/N_{E/F}(E^\times)$ est un groupe cyclique d'ordre $[E : F]$ engendré par une uniformisante de F.*

Il existe donc un unique isomorphisme $F^\times/N_{E/F}(E^\times) \simeq \mathrm{Gal}(E/F)$ tel que $\pi_F \mapsto (\mathfrak{p}_F, E/F)$.

5.1.2 Énoncés locaux

Si G est un groupe, on note G' son groupe dérivé, c'est-à-dire le sous-groupe de G engendré par tous les commutateurs $[g,h] = ghg^{-1}h^{-1}$ où $g, h \in G$. Il s'agit d'un sous-groupe distingué de G et le quotient est le plus grand quotient abélien de G. On l'appelle l'*abélianisé* G^{ab} de G.

Théorème 5.1.3 (Loi de réciprocité locale)**.** *Pour toute extension galoisienne finie E/F, le sous-groupe $N_{E/F}(E^\times)$ est ouvert dans $F^\times$ et il existe un isomorphisme de groupes*

$$r_{E/F} : F^\times/N_{E/F}(E^\times) \xrightarrow{\sim} \mathrm{Gal}(E/F)^{\mathrm{ab}}$$

tel que les propriétés suivantes sont satisfaites.

(i) Si E/F est non ramifiée, alors $r_{E/F}(\pi_F) = (\mathfrak{p}_F, E/F)$.

(ii) Si E'/F' est une extension galoisienne finie telle que $F \subset F'$ et $E \subset E'$, alors le diagramme suivant commute

$$\begin{array}{ccc} F'^\times/N_{E'/F'}(E'^\times) & \xrightarrow{N_{F'/F}} & F^\times/N_{E/F}(E^\times) \\ \downarrow{\scriptstyle r_{E'/F'}} & & \downarrow{\scriptstyle r_{E/F}} \\ \mathrm{Gal}(E'/F')^{\mathrm{ab}} & \longrightarrow & \mathrm{Gal}(E/F)^{\mathrm{ab}} \end{array}$$

où la flèche horizontale du bas est le morphisme induit par l'application de restriction $\mathrm{Gal}(E'/F') \to \mathrm{Gal}(E/F)$.

(iii) Si $\tau : E \xrightarrow{\sim} E'$ est un automorphisme de corps valués et si $F' \coloneqq \tau(F)$, on a un diagramme commutatif

$$\begin{array}{ccc} F^\times/N_{E/F}(E^\times) & \xrightarrow{\tau} & F'^\times/N_{E'/F'}(E'^\times) \\ \downarrow{\scriptstyle r_{E/F}} & & \downarrow{\scriptstyle r_{E'/F'}} \\ \mathrm{Gal}(E/F)^{\mathrm{ab}} & \longrightarrow & \mathrm{Gal}(E'/F')^{\mathrm{ab}} \end{array}$$

où la flèche horizontale du bas est l'isomorphisme de groupes induit par $\sigma \mapsto \tau\sigma\tau^{-1}$. De plus, il existe au plus une famille d'isomorphismes vérifiant les propriétés (i) et (ii).

Explicitons quelques cas particuliers de la fonctorialité (ii) dans le théorème 5.1.3.

Si $F' = F$, on a un diagramme commutatif :

$$\begin{array}{ccc} F^\times/N_{E'/F}(E'^\times) & \twoheadrightarrow & F^\times/N_{E/F}(E^\times) \\ \downarrow{\scriptstyle r_{E'/F}} & & \downarrow{\scriptstyle r_{E/F}} \\ \mathrm{Gal}(E'/F)^{\mathrm{ab}} & \twoheadrightarrow & \mathrm{Gal}(E/F)^{\mathrm{ab}}. \end{array}$$

La flèche horizontale supérieure est ici l'application quotient map et la flèche horizontale inférieure est la restriction à E.

Si $E = E'$, on a un diagramme commutatif :

$$\begin{array}{ccc} F'^{\times}/N_{E/F'}(E^{\times}) & \xrightarrow{N_{F'/F}} & F^{\times}/N_{E/F}(E^{\times}) \\ \downarrow{\scriptstyle r_{E/F'}} & & \downarrow{\scriptstyle r_{E/F}} \\ \mathrm{Gal}(E/F')^{\mathrm{ab}} & \longrightarrow & \mathrm{Gal}(E/F)^{\mathrm{ab}}. \end{array}$$

La flèche horizontale inférieure est induite par l'inclusion $\mathrm{Gal}(E/F') \subset \mathrm{Gal}(E/F)$.

Théorème 5.1.4 (Théorème d'existence local)**.** *Soit $N \subset F^{\times}$ un sous-groupe ouvert d'indice fini. Alors il existe une extension abélienne E/F telle que $N = N_{E/F}(E^{\times})$.*

Corollaire 5.1.5. *Soit $\overline{F}$ une clôture algébrique de F. L'application $E \mapsto N_{E/F}(E^{\times})$ induit une bijection décroissante de l'ensemble des extensions abéliennes finies $E \subset \overline{F}$ de F sur l'ensemble des sous-groupes ouverts d'indice fini dans $F^{\times}$.*

Démonstration. Remarquons tout d'abord que si $E \subset \overline{F}$ est une extension abélienne finie de F, alors $N_{E/F}(E^{\times})$ est un sous-groupe ouvert d'indice fini dans $F^{\times}$ d'après le théorème 5.1.3. Si $E \subset E'$, l'égalité $N_{E'/F} = N_{E/F} \circ N_{E'/E}$ implique que $N_{E'/F}(E'^{\times}) \subset N_{E/F}(E^{\times})$. L'application est donc décroissante. Elle est surjective d'après le théorème 5.1.4. Il nous reste donc à prouver son injectivité.

Supposons que $E_1, E_2 \subset \overline{F}$ sont deux extensions abéliennes finies de F telles que $N_{E_1/F}(E_1^{\times}) = N_{E_2/F}(E_2^{\times})$. Posons $E = E_1E_2$. Il s'agit d'une extension galoisienne et abélienne car

$$\mathrm{Gal}(E/F) \hookrightarrow \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F).$$

Si $i \in \{1, 2\}$, on déduit de la propriété (ii) du théorème 5.1.3 que l'on a un diagramme commutatif

$$\begin{array}{ccc} F^{\times}/N_{E/F}(E^{\times}) & \longrightarrow & F^{\times}/N_{E_i/F}(E_i^{\times}) \\ \downarrow{\scriptstyle r_{E/F}} & & \downarrow{\scriptstyle r_{E_i/F}} \\ \mathrm{Gal}(E/F) & \longrightarrow & \mathrm{Gal}(E_i/F) \end{array}$$

qui implique que $\mathrm{Gal}(E/E_i) = r_{E/F}(N_{E_i/F}(E_i^{\times}))$. On en déduit que $\mathrm{Gal}(E/E_1) = \mathrm{Gal}(E/E_2)$ et donc que $E_1 = E_2$. □

Corollaire 5.1.6. *Soit E/F une extension finie abélienne. Alors l'extension E/F est non ramifiée si et seulement si $U_F \subset N_{E/F}(E^{\times})$.*

Démonstration. Si l'extension E/F est non ramifiée, alors $U_F \subset N_{E/F}(E^\times)$ par la proposition 5.1.1. Réciproquement supposons que $U_F \subset N_{E/F}(E^\times)$. Soit $d = [E : F]$ et soit E' l'extension (unique à isomorphisme près) non ramifiée de F de degré d qui existe par le corollaire 2.3.5. On a alors $N_{E'/F}(E'^\times) = (\pi_F^d)^{\mathbb{Z}} U_F$ d'après la proposition 5.1.1. Comme $\pi_F^d = N_{E/F}(\pi_F) \in N_{E/F}(E^\times)$, on a $N_{E'/F}(E'^\times) \subset N_{E/F}(E^\times)$. On déduit du corollaire 5.1.5 qu'il existe un morphisme F-linéaire $E \hookrightarrow E'$ et donc $E \simeq E'$ par égalité des degrés. Ainsi E/F est non ramifiée. □

5.1.3 Démonstration de l'unicité de la loi de réciprocité locale

Nous démontrons l'assertion d'unicité dans le théorème 5.1.3. Nous utilisons le lemme suivant.

Lemme 5.1.7. *Soit E/F une extension finie galoisienne. Soit $\sigma \in \mathrm{Gal}(E/F)$. Il existe alors une extension finie E'/E telle que E'/F est galoisienne et il existe $\widetilde{\sigma} \in \mathrm{Gal}(E'/F)$ relevant σ tel que $E'/(E')^{\widetilde{\sigma}}$ est non ramifiée.*

Vérifions dans un premier temps que le lemme implique l'unicité de la loi de réciprocité locale. Soit E/F une extension galoisienne finie. Soit $\sigma \in \mathrm{Gal}(E/F)$ et soient E' et $\widetilde{\sigma}$ comme dans le lemme 5.1.7. Posons $F' := (E')^{\widetilde{\sigma}}$. On a $\widetilde{\sigma} \in \mathrm{Gal}(E'/E'^{\widetilde{\sigma}})$. Il existe donc un entier $m \geqslant 0$ tel que $\widetilde{\sigma} = (\mathfrak{p}_{F'}, E'/F')^m$. La propriété (i) du théorème 5.1.3 montre que $r_{E'/F'}(\pi_F^m) = \widetilde{\sigma}$ et la propriété (ii) montre alors que $r_{E/F}^{-1}(\sigma) = N_{F'/F}(\pi_{F'})^m$. Ceci implique que la famille des isomorphismes $r_{E/F}$ est entièrement caractérisée par les propriétés (i) et (ii).

Démonstration du lemme 5.1.7. Soit $K \subset E$ la sous-extension maximale non ramifiée de F. et soit $r \geqslant 0$ tel que $\sigma|_K = (\mathfrak{p}_F, K/F)^r$. Soit $N \geqslant 1$ un entier multiple de l'ordre de σ dans $\mathrm{Gal}(E/F)$. Soit E_1 la sous-extension maximale non ramifiée de E de degré rN et soit $F_1 \subset E_1$ la sous-extension maximale non ramifiée de F containue dans E_1. On a alors

$$[F_1 : F] = [k_{E_1} : k_F] = rN[k_E : k_F]$$

et $[K : F] = [k_E : k_F]$ de sorte que $[F_1 : K] = rN$. De plus, on a clairement $F_1 \cap E = K$. Ainsi $[F_1E : E] = [F_1 : K] = rN = [E_1 : E]$. Ainsi $E_1 = F_1E$. On en déduit que l'extension E_1/F est galoisienne. De plus l'application $\tau \mapsto (\tau|_E, \tau|_{F_1})$ identifie $\mathrm{Gal}(E/F)$ au sous-groupe de $\mathrm{Gal}(E/F) \times \mathrm{Gal}(F_1/F)$ constitué des paires (τ_1, τ_2) telles que $\tau_1|_K = \tau_2|_K$. Il existe donc un unique élément $\widetilde{\sigma} \in \mathrm{Gal}(E_1/F)$ tel que $\widetilde{\sigma}|_E = \sigma$ et $\widetilde{\sigma}|_{F_1} = (\mathfrak{p}_F, F_1/F)^r$ (en effet on a $(\mathfrak{p}_F, F_1/F)^r|_K = (\mathfrak{p}_F, K/F)^r =$

$\sigma|_K$). Il reste donc à vérifier que l'extension $E_1/E_1^{\widetilde{\sigma}}$ est non ramifiée. Remarquons que le morphisme de groupes induit par la restriction à F_1 est surjectif :

$$\mathrm{Gal}(E_1/E_1^{\widetilde{\sigma}}) \twoheadrightarrow \mathrm{Gal}(F_1/F_1^{\widetilde{\sigma}}). \tag{5.1}$$

En effet les deux groupes sont cycliques, engendrés respectivement par $\widetilde{\sigma}$ et $\widetilde{\sigma}|_{F_1}$. De plus, le membre de droite est un sous-groupe du groupe cyclique $\mathrm{Gal}(F_1/F) \simeq \mathbb{Z}/rN[k_E : k_F]\mathbb{Z}$. Comme $\widetilde{\sigma}|_{F_1} = (\mathfrak{p}_F, F_1/F)^r$, on voit que le groupe $\mathrm{Gal}(F_1/F)$ est cyclique d'ordre $N[k_E : k_F]$. Par ailleurs, on a $\sigma^N = 1$. Ainsi $\widetilde{\sigma}^N|_E = 1$ et $\widetilde{\sigma}|_{F_1}^{N[k_E:k_F]} = 1$, ce qui implique que $\widetilde{\sigma}^{N[k_E:k_F]} = 1$. On en déduit que le morphisme surjectif (5.1) est un isomorphisme, ce qui implique que $E_1 = E_1^{\widetilde{\sigma}} F_1$. Comme $F_1/F_1^{\widetilde{\sigma}}$ est non ramifiée, l'extension composée $F_1 E_1^{\widetilde{\sigma}}/E_1^{\widetilde{\sigma}}$ est également non ramifiée. □

5.1.4 Complément sur la norme

Soit F une extension finie de $\mathbb{Q}_p$ et soit v_F sa valuation discrète normalisée. Soit $i \geqslant 1$. Si $x \in U_F^i$, la série

$$\log(x) \coloneqq \sum_{n \geqslant 1} \frac{(-1)^{n-1}}{n} (x-1)^n$$

converge absolument et vérifie $\log(xy) = \log(x) + \log(y)$ pour $x, y \in U_F^i$. Ainsi on obtient un morphisme de groupes continu $\log : U_F^i \to \mathfrak{p}_F^i$. Si $x \in \mathfrak{p}_F^i$, la série

$$\exp(x) \coloneqq \sum_{n \geqslant 0} \frac{x^n}{n!}$$

converge absolument et vérifie $\exp(x+y) = \exp(x)\exp(y)$. De plus $\exp : \mathfrak{p}_F^i \to U_F^i$ est la bijection réciproque de log. On en déduit un isomorphisme de groupes topologiques $\mathbb{Z}_p^{[F:\mathbb{Q}_p]} \simeq \mathfrak{p}_F^i \xrightarrow{U}{}^{i}_{F}$. On en déduit le résultat suivant qui sera utile plus tard :

Lemme 5.1.8. *Soit F une extension finie de $\mathbb{Q}_p$. Alors le groupe U_F contient un sous-groupe ouvert isomorphe à $\mathbb{Z}_p^{[F:\mathbb{Q}_p]}$.*

On peut également utiliser les fonctions exp et log pour prouver le résultat suivant.

Proposition 5.1.9. *Soit E/F une extension finie d'extensions finie de $\mathbb{Q}_p$. Alors le sous-groupe $N_{E/F}(E^\times) \subset F^\times$ est ouvert.*

Démonstration. Supposons dans un premier temps E/F est galoisienne. On vérifie facilement que $N_{E/F}(U_E^1) \subset U_F^1$. De plus, si $\sigma \in \mathrm{Gal}(E/F)$, alors σ un automorphisme continu de E (en utilisant par exemple le théorème 2.2.23) et on en conclut que $\sigma \circ \log = \log \circ \sigma$. Ainsi, pour tout $x \in U_E^1$, on a $\log(N_{E/F}(x)) = \mathrm{Tr}_{E/F}(\log(x))$. Comme l'application $\mathrm{Tr}_{E/F} : E \to F$ est F-linéaire continue, elle est ouverte et donc $\log(N_{E/F}(U_F^1))$ est un sous-groupe ouvert de $\mathfrak{p}_F$ et on en conclut que $N_{E/F}(U_F^1)$ contient $\exp(\mathfrak{p}_F^m)$ pour m assez grand, qui est un sous-groupe ouvert de $F^\times$.

Supposons à présent E/F quelconque et soit K la clôture normale de E/F. Alors K/F est une extension galoisienne finie et $N_{K/F}(K^\times) \subset N_{E/F}(E^\times)$ est ouvert donc $N_{E/F}(E^\times)$ est ouvert. □

5.1.5 Le cas des corps locaux archimédiens

Si $F = \mathbb{R}$, alors F possède une unique extension non triviale. Il s'agit de $\mathbb{C}/\mathbb{R}$. Par ailleurs, on a $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times) = \mathbb{R}_{>0}$. On note donc $r_{\mathbb{C}/\mathbb{R}}$ l'unique isomorphisme de $\mathbb{R}^\times/N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times)$ sur $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Il envoie la classe de -1 sur la conjugaison complexe. Remarquons que l'analogue du corollaire 5.1.5 reste vrai mais est complètement trivial car $\mathbb{R}^\times$ possède exactement un sous-groupe ouvert d'indice fini différent de $\mathbb{R}^\times$ et $\mathbb{C}^\times$ n'en possède pas.

5.2 Extensions abéliennes des corps de nombres

5.2.1 Énoncés

Soit E/F une extension finie de corps de nombres. On a alors une inclusion naturelle d'anneaux topologiques

$$\mathbb{A}_F \hookrightarrow \mathbb{A}_E$$

définie par $(x_v)_v \mapsto (y_w)_w$ où $y_w := x_v$ si $w \mid v$. On définit également des morphismes de groupes continus

— la *norme*

$$N_{E/F} : \begin{array}{ccc} \mathbb{A}_E^\times & \longrightarrow & \mathbb{A}_F^\times \\ (y_w)_w & \longmapsto & \left(\prod_{w|v} N_{E_w/F_v}(y_w)\right)_v \end{array}$$

— et la *trace*

$$\mathrm{Tr}_{E/F} : \begin{array}{ccc} \mathbb{A}_E & \longrightarrow & \mathbb{A}_F \\ (y_w)_w & \longmapsto & \left(\sum_{w|v} \mathrm{Tr}_{E_w/F_v}(y_w)\right)_v . \end{array}$$

On a alors les compatibilités évidentes avec la norme et la trace de l'extesnion E/F :

$$\begin{array}{ccc} E^\times & \xrightarrow{N_{E/F}} & F^\times \\ \downarrow & & \downarrow \\ \mathbb{A}_E^\times & \xrightarrow{N_{E/F}} & \mathbb{A}_F^\times \end{array} \qquad \begin{array}{ccc} E & \xrightarrow{\mathrm{Tr}_{E/F}} & F \\ \downarrow & & \downarrow \\ \mathbb{A}_E & \xrightarrow{\mathrm{Tr}_{E/F}} & \mathbb{A}_F. \end{array}$$

On suppose désormais que l'extension E/F est abélienne. Rappelons que si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_F$ non ramifié dans E/F, alors pour tout $\mathfrak{q} \mid \mathfrak{p}$ idéal maximal de $\mathcal{O}_E$ divisant $\mathfrak{p}$, l'élément de Frobenius $(\mathfrak{q}, E/F) \in \mathrm{Gal}(E/F)$ ne dépend pas de $\mathfrak{q}$ et est donc noté $(\mathfrak{p}, E/F)$.

Soit v une place de F et soit $w \mid v$ une place de E divisant v. On identifie alors $\mathrm{Gal}(E_w/F_v)$ au groupe de décomposition de w dans $\mathrm{Gal}(E/F)$. La loi de réciprocité locale (théorème 5.1.3 et section 5.1.5) permet de construire un morphisme de groupes topologiques $x_v \mapsto (x_v, E/F)$ de $F_v^\times$ dans $\mathrm{Gal}(E/F)$ défini comme la composition suivante

$$F_v^\times \twoheadrightarrow F_v^\times / N_{E_w/F_v}(E_w^\times) \xrightarrow{r_{E_w/F_v}} \mathrm{Gal}(E_w/F_v) \simeq D_w \hookrightarrow \mathrm{Gal}(E/F).$$

Remarquons que l'application $x_v \mapsto (x_v, E/F)$ ne dépend pas du choix de $w \mid v$. C'est une conséquence du fait que $\mathrm{Gal}(E/F)$ est abélien et de la propriété (iii) du théorème 5.1.3. Si de plus, la place v est non ramifiée dans E, on a $(\pi_v, E/F) = (\mathfrak{p}_v, E/F)$ (pour π_v une uniformisante de F_v) et $(x_v, E/F) = 1$ pour $x_v \in U_v \coloneqq U_{F_v}$.

On peut ainsi définir un morphisme de groupes topolgoqiues :

$$\mathrm{Art}_{E/F} : \begin{array}{ccc} \mathbb{A}_F^\times & \longrightarrow & \mathrm{Gal}(E/F) \\ (x_v)_v & \longmapsto & \prod_v (x_v, E/F). \end{array}$$

Il s'agit de l'*application de réciprocité d'Artin.*

On peut à présent énoncer la *loi de réciprocité d'Artin.*

Théorème 5.2.1 (Loi de réciprocité d'Artin)**.** *On a* $\mathrm{Art}_{E/F}(F^\times) = \{1\}$*. De plus, l'application* $\mathrm{Art}_{E/F}$ *est surjective et son noyau est le sous-groupe engendré par* $F^\times$ *et* $N_{E/F}(\mathbb{A}_E^\times)$*. Autrement dit, l'application* $\mathrm{Art}_{E/F}$ *induit un isomorphisme de groupes*

$$\mathbb{A}_F^\times / F^\times N_{E/F}(\mathbb{A}_E^\times) \xrightarrow{\sim} \mathrm{Gal}(E/F).$$

Enfin l'application $\mathrm{Art}_{E/F}$ *est l'unique morphisme de groupes topologiques de* $\mathbb{A}_F^\times$ *vers* $\mathrm{Gal}(E/F)$ *tel que*

— $\mathrm{Art}_{E/F}(F^\times) = \{1\}$,

— *et, pour presque toute place finie v de F non ramifiée dans E, on a* $\mathrm{Art}_{E/F}(\varpi_v) = (\mathfrak{p}_v, E/F)$*, où* $\varpi_v = (1, \dots, 1, \pi_v, 1, \dots) \in \mathbb{A}_F^\times$ *est l'idèle dont toutes les coordonnées valent* 1 *exceptée la coordinée d'indice v qui est une uniformisante de F_v.*

Remarque 5.2.2. En utilisant l'assertion d'unicité dans le théorème 5.2.1, on démontre facilement les propriétés de compatibilités suivantes.

— Si E'/F' est une extension abélienne finie telle que $F \subset F'$ et $E \subset E'$, le diagramme suivant est commutatif

$$\begin{array}{ccc} \mathbb{A}_{F'}^\times & \xrightarrow{N_{F'/F}} & \mathbb{A}_F^\times \\ \downarrow{\scriptstyle \mathrm{Art}_{E'/F'}} & & \downarrow{\scriptstyle \mathrm{Art}_{E/F}} \\ \mathrm{Gal}(E'/F') & \longrightarrow & \mathrm{Gal}(E/F) \end{array}$$

où la flèche horizontale inférieure est l'application de restriction.

— Si $\tau : E \xrightarrow{\sim} E'$ est un automorphism et si $F' \coloneqq \tau(F)$, le diagramme suivant est commutatif

$$\begin{array}{ccc} \mathbb{A}_F^\times & \xrightarrow{\tau} & \mathbb{A}_{F'}^\times \\ \downarrow{\scriptstyle \mathrm{Art}_{E/F}} & & \downarrow{\scriptstyle \mathrm{Art}_{E'/F'}} \\ \mathrm{Gal}(E/F) & \xrightarrow{\tau\cdot\tau^{-1}} & \mathrm{Gal}(E'/F') \end{array}$$

où la f!chle horizontale inférieure est l'isomorphisme de groupe définie par $\sigma \mapsto \tau\sigma\tau^{-1}$.

En effet, il suffit de vérifier si v est une place de F non ramifiée dans E', $w \mid v$ place de E, $w' \mid w$ place de E' et v' est la restriction de w' à F', alors $(\mathfrak{p}_{w'}, E'/F' = (\mathfrak{p}_{w'}, E'/F)^{f_{\mathfrak{p}_{v'}/\mathfrak{p}_v}}$ et $(\mathfrak{p}_{w'}, E'/F)|_E = (\mathfrak{p}_w, E/F)$. Ainsi $(\mathfrak{p}_{w'}, E'/F')|_E = (\mathfrak{p}_w, E/F)^{f_{\mathfrak{p}_{v'}/\mathfrak{p}_v}}$, c'est-à-dire $(\mathfrak{p}_{v'}, E'/F')|_E = (N_{F'/F}(\mathfrak{p}_{v'}), E/F)$, ce qui fournit la compatibilité du premier digramme.

Pour le second diagramme, il suffit de vérifier, pour $\mathfrak{p}$ idéal maximal de $\mathcal{O}_F$ non ramifié dans E, que $\tau(\mathfrak{p})$ est non ramifié dans E' et que $(\tau(\mathfrak{p}), E'/F') = \tau(\mathfrak{p}, E/F)\tau^{-1}$.

Théorème 5.2.3 (Théorème d'existence (Takagi, Chevalley))**.** *Soit $N \subset \mathbb{A}_F^\times$ un sous-groupe ouvert d'indice fini contenant $F^\times$. Il existe alors une extension abélienne E/F telle que $N = F^\times N_{E/F}(\mathbb{A}_E^\times)$.*

Comme dans le cas local, on en déduit une classification des extensions abéliennes de F.

Corollaire 5.2.4. *Soit $\overline{F}$ une clôture algébrique de F. L'application $E \mapsto F^\times N_{E/F}(\mathbb{A}_E^\times)$ induit une bijection décroissante de l'ensemble des extensions abéliennes finies $E \subset \overline{F}$ de F sur l'ensemble des sous-groupes ouverts d'indice fini dans $\mathbb{A}_F^\times$ contenant $F^\times$.*

Démonstration. Remarquons tout d'abord que si $E \subset \overline{F}$ est une extension abélienne finie de F, alors $F^\times N_{E/F}(\mathbb{A}_E^\times)$ est un sous-groupe ouvert d'indice fini dans $\mathbb{A}_F^\times$ d'après le théorème 5.2.1. Comme dans la démonstration du corollaire 5.1.5, on montre la décroissance de l'application. Elle est surjective d'après le théorème 5.2.3. Il nous reste donc à prouver son injectivité.

Supposons que $E_1, E_2 \subset \overline{F}$ sont deux extensions abéliennes finies de F telles que $F^\times N_{E_1/F}(\mathbb{A}_{E_1}^\times) = N_{E_2/F}(\mathbb{A}_{E_2}^\times)$. Posons $E = E_1E_2$. Il s'agit d'une extension galoisienne et abélienne car

$$\mathrm{Gal}(E/F) \hookrightarrow \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F).$$

Si $i \in \{1, 2\}$, on déduit de la remarque 5.2.2 que l'on a un diagramme commutatif

$$\begin{array}{ccc} \mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times) & \longrightarrow & \mathbb{A}_F^\times/F^\times N_{E_i/F}(\mathbb{A}_{E_i}^\times) \\ \downarrow{\scriptstyle \mathrm{Art}_{E/F}} & & \downarrow{\scriptstyle \mathrm{Art}_{E_i/F}} \\ \mathrm{Gal}(E/F) & \longrightarrow & \mathrm{Gal}(E_i/F) \end{array}$$

qui implique que $\mathrm{Gal}(E/E_i) = \mathrm{Art}_{E/F}(F^\times N_{E_i/F}(\mathbb{A}_{E_i}^\times))$. On en déduit que $\mathrm{Gal}(E/E_1) = \mathrm{Gal}(E/E_2)$ et donc que $E_1 = E_2$. □

5.2.2 Le corps de classes de Hilbert

Proposition 5.2.5. *Soit E/F une extension abélienne finie de corps de nombres. Les propriétés suivantes sont équivalents.*

(i) L'extension E/F est non ramifiée en toute place finie.

(ii) On a $\prod_{v\nmid\infty} U_v \subset N_{E/F}(\mathbb{A}_E^\times)$.

(iii) On a $\prod_{v\nmid\infty} U_v \subset F^\times N_{E/F}(\mathbb{A}_E^\times)$.

Démonstration. Supposons (i). Alors si v est une place finie de F et $w \mid v$ est une place de E divisant v, l'extension E_w/F_v est non ramifiée. D'après le corollaire 5.1.6, on a $U_v \subset N_{E_w/F_v}(E_w^\times)$. On en conclut qu'on est dans le cas (ii). Il est clair que (ii) implique (iii). Supposons enfin (iii). Soit v une place finie de F et $w \mid v$ une

place de E divisant v. Par définition de $\mathrm{Art}_{E/F}$, on a un diagramme commutatif

$$\begin{array}{ccc} F_v^\times & \hookrightarrow & \mathbb{A}_F^\times \\ \downarrow{\scriptstyle r_{E_w/F_v}} & & \downarrow{\scriptstyle \mathrm{Art}_{E/F}} \\ \mathrm{Gal}(E_w/F_v) & \hookrightarrow & \mathrm{Gal}(E/F). \end{array}$$

Comme $F^\times N_{E/F}(\mathbb{A}_E^\times) = \mathrm{Ker}(\mathrm{Art}_{E/F})$, on a $r_{E_w/F_v}(U_v) = \{1\}$, et donc E_w/F_v est non ramifiée d'après le corollaire 5.1.6. On a donc prouvé (i). □

Si v est une place archimédienne de F et si w est une place de E divisant F, on dit que w est *non ramifiée* dans E/F si $E_w = F_v$. On dit qu'une place archimédienne de F est *non ramifiée* dans E/F si w est non ramifiée dans E/F pour tout $w \mid v$.

On démontre, de façon analogue à la proposition 5.2.5, le critère de non ramification suivant.

Proposition 5.2.6. *Soit E/F une extension abélienne finie de corps de nombres. Les propriétés suivantes sont équivalents.*

(i) L'extension E/F est non ramifiée en toute place de F (y compris les places archimédiennes).

(ii) On a $\prod_{v|\infty} F_v^\times \prod_{v\nmid\infty} U_v \subset N_{E/F}(\mathbb{A}_E^\times)$.

(iii) On a $\prod_{v|\infty} F_v^\times \prod_{v\nmid\infty} U_v \subset F^\times N_{E/F}(\mathbb{A}_E^\times)$.

Considérons le sous-groupe $N = F^\times \prod_{v|\infty} F_v^\times \prod_{v\nmid\infty} U_v \subset \mathbb{A}_F^\times$. Il s'agit d'un sous-groupe ouvert de $\mathbb{A}_F^\times$. On déduit de plus de (3.1) qu'il s'agit d'un groupe fini, naturellement isomorphe au groupe des classes $\mathrm{Cl}(\mathcal{O}_F)$. Le théorème 5.2.3 implique donc qu'il existe une extension abélienne finie H/F telle que $F^\times N_{H/F}(\mathbb{A}_H^\times) = N$. On déduit du corollaire 5.2.4 et de la proposition 5.2.6 que H/F est la plus grande extension abélienne de F qui est non ramifiée en toutes les places de F (y compris les places archimédiennes). Le corps H est appelé *corps de classes de Hilbert* de F.

Le théorème 5.2.1 et l'équation (3.1) impliquent qu'il existe un isomorphisme de groupes

$$\mathrm{Art}_{H/F} : \mathrm{Cl}(\mathcal{O}_F) \xrightarrow{\sim} \mathrm{Gal}(H/F)$$

tel que, pour tout idéal maximal $\mathfrak{p} \subset \mathcal{O}_F$, $\mathrm{Art}_{H/F}([\mathfrak{p}]) = (\mathfrak{p}, H/F)$. En particulier la décomposition d'un idéal maximal $\mathfrak{p} \subset \mathcal{O}_F$ est caractérisée par la classe de $\mathfrak{p}$ dans $\mathrm{Cl}(\mathcal{O}_F)$. En particulier, $\mathfrak{p}$ est principal si et seulement si il est complètement décomposé dans $\mathcal{O}_H$.

Exemple 5.2.7. Soit $F = \mathbb{Q}(i\sqrt{5})$. On sait que $\mathrm{Cl}(\mathcal{O}_F)$ est de cardinal 2, de sorte que le corps de classes de Hilbert de F est une extension quadratique de F. L'extensions $F(\sqrt{5})/F$ est non ramifiée en toute place finie puisque $F(\sqrt{5}) = F(i)$. De plus, le corps F possède une unique place archimédienne dont le complété est $\mathbb{C}$. Toute extension de F est donc non ramifiée à l'infini. On en conclut que $F(\sqrt{5})/F$ est non ramifiée en toute place et donc $F(\sqrt{5})$ est le coprs de classes de Hilbert de F.

Exemple 5.2.8. Soit $F = \mathbb{Q}(\sqrt{3})$. L'extension $F(i\sqrt{3})$ est non ramifiée en toute place finie de F. Cependant les places archimédiennes de F sont réelles alors que celles de $F(i\sqrt{3})$ sont complexes. On en déduit que $F(i\sqrt{3})$ n'est pas le corps de classes de Hilbert de F. En fait, puisque $\mathcal{O}_F = \mathbb{Z}[\sqrt{3}]$ est principal, le corps de classes de Hilbert de F est F lui-même.

5.2.3 Reformulation en termes d'idéaux

Soit F un corps de nombres. Un *module* de F est une fonction

$$\mathfrak{m} : \Sigma_F \longrightarrow \mathbb{N}$$

telle que

— le support $\mathrm{Supp}(\mathfrak{m}) \coloneqq \{v \in \Sigma_F \mid \mathfrak{m}(v) > 0\}$ de $\mathfrak{m}$ est fini ;

— si $F_v \simeq \mathbb{C}$, alors $\mathfrak{m}(v) = 0$;

— si $F_v \simeq \mathbb{R}$, alrs $\mathfrak{m}(v) \in \{0, 1\}$.

On définit une relation d'ordre sur les modules en définissant $\mathfrak{m}_1 \leqslant \mathfrak{m}_2$ lorsque $\mathfrak{m}_1(v) \leqslant \mathfrak{m}_2(v)$ pour toute v.

Si $\mathfrak{m}$ est un module, on définit un sous-groupe ouvert de $\mathbb{A}_F^\times$ en posant

$$V_\mathfrak{m} \coloneqq \prod_{\substack{v|\infty \\ \mathfrak{m}(v)=0}} F_v^\times \prod_{\substack{v|\infty \\ \mathfrak{m}(v)=1}} \mathbb{R}_{>0}^\times \prod_{v\nmid\infty} U_v^{\mathfrak{m}(v)}.$$

La famille $(V_\mathfrak{m})_\mathfrak{m}$ forme une base de sous-groupes ouverts de $\mathbb{A}_F^\times$ dans le sens où, si H est un sous-groupe ouvert de $\mathbb{A}_F^\times$, alors il existe un module $\mathfrak{m}$ tel que $V_\mathfrak{m} \subset H$.

Remarque 5.2.9. Attention, même si la famille $(V_\mathfrak{m})_\mathfrak{m}$ forme une base de sous-groupes ouverts de $\mathbb{A}_F^\times$, elle ne forme pas une base de voisinages de 1 dans $\mathbb{A}_F^\times$!

Soit $J_F^\mathfrak{m}$ le sous-groupe de $\mathbb{A}_F^\times$ défini comme le produit restreint des $F_v^\times$ sur l'ensemble des places finies v telles que $v \notin \mathrm{Supp}(\mathfrak{m})$. Notons également $I(\mathcal{O}_F)^\mathfrak{m}$ le

sous-groupe des idéaux fractionnaires de $\mathcal{O}_F$ qui sont premiers aux idéaux $\mathfrak{p}_v$ pour $v \in \mathrm{Supp}(\mathfrak{m})$. On a alors un morphisme surjectif de groupes

$$J_F^{\mathfrak{m}} \twoheadrightarrow I(\mathcal{O}_F)^{\mathfrak{m}}$$

défini par $\varpi_v = (1, \dots, 1, \pi_v, 1, \dots) \mapsto \mathfrak{p}_v$ dont le noyau est $\prod_{\substack{v \notin \mathrm{Supp}(\mathfrak{m}) \\ v \nmid \infty}} U_v$. Si E/F est une extension finie de F, on note également $J_E^{\mathfrak{m}}$ le produit restreint des $E_w^\times$ pour w place finie de E telle que $w|_F \notin \mathrm{Supp}(\mathfrak{m})$ et $I(\mathcal{O}_E)^{\mathfrak{m}}$ le sous-groupe des idéaux fractionnaires de $\mathcal{O}_E$ qui sont premiers aux idéaux $\mathfrak{p}_w$ pour $w|_F \in \mathrm{Supp}(\mathfrak{m})$. Remarquons que $N_{E/F}(I(\mathcal{O}_E)^{\mathfrak{m}}) \subset I(\mathcal{O}_F)^{\mathfrak{m}}$.

Lemme 5.2.10. *Soit S un ensemble fini de places de F. Alors le plongement diagonal $F^\times \to \prod_{v \in S} F_v^\times$ a une image dense.*

Démonstration. Soit $(x_v) \in \prod_{v \in S} F_v^\times$ et soit $\varepsilon > 0$ suffisamment petit pour que $\varepsilon < |x_v|$ pour au moins une place $v \in S$. Le théorème 3.1.12 implique qu'il existe $\xi \in F$ tel que $|\xi - x_v| < \varepsilon$ pour tout $v \in S$. Notre hypothèse sur ε, implique alors $\xi \neq 0$ et donc $\xi \in F^\times$. □

Pour $\mathfrak{m}$ un module de F, on définit $F_{\mathfrak{m}}^\times \coloneqq F^\times \cap J_F^{\mathfrak{m}} V_{\mathfrak{m}} \subset \mathbb{A}_F^\times$. Explicitement, les éléments de $F^\times$ sont les $\xi \in F^\times$ tels que

— si v est une place non archimédienne et si $\mathfrak{m}(v) > 0$, alors $v_{\mathfrak{p}_v}(\xi - 1) \geqslant \mathfrak{m}(v)$;

— si v est une place archimédienne correspondant à un plongement réel $\tau_v : F \hookrightarrow \mathbb{R}$ et si $\mathfrak{m}(v) = 1$, alors $\tau_v(\xi) \in \mathbb{R}_{>0}$.

Les éléments du groupes $F_{\mathfrak{m}}^\times$ sont appelés les $\mathfrak{m}$-*unités*. On note alors $P_{\mathfrak{m}}$ le sous-groupe de $I(\mathcal{O}_F)^{\mathfrak{m}}$ des idéaux fractionnaires principaux, engendrés par un élément de $F_{\mathfrak{m}}^\times$:

$$P_{\mathfrak{m}} \coloneqq \{(a) \mid a \in F_{\mathfrak{m}}^\times\}.$$

Proposition 5.2.11. *Soit $\mathfrak{m}$ un module de F. L'inclusion $J_F^{\mathfrak{m}} \to \mathbb{A}_F^\times$ composée avec l'application quotient $\mathbb{A}_F^\times \to \mathbb{A}_F^\times / F^\times V_{\mathfrak{m}}$ se factorise en un morphisme $I(\mathcal{O}_F)^{\mathfrak{m}} \to \mathbb{A}_F^\times / F^\times V_{\mathfrak{m}}$ et induit des isomorphismes*

$$I(\mathcal{O}_F)^{\mathfrak{m}} / P_{\mathfrak{m}} \xrightarrow{\sim} \mathbb{A}_F^\times / F^\times V_{\mathfrak{m}}$$
$$I(\mathcal{O}_F)^{\mathfrak{m}} / P_{\mathfrak{m}} N_{E/F}(I(\mathcal{O}_E)^{\mathfrak{m}}) \xrightarrow{\sim} \mathbb{A}_F^\times / F^\times N_{E/F}(\mathbb{A}_E^\times).$$

Démonstration. Si $v \notin \mathrm{Supp}(\mathfrak{m})$, on a $U_v \subset V_{\mathfrak{m}}$, ce qui implique que l'application $J_F^{\mathfrak{m}} \to \mathbb{A}_F^\times / F^\times V_{\mathfrak{m}}$ se factorise à travers $I(\mathcal{O}_F)^{\mathfrak{m}}$. Pour démontrer la surjectivité, il suffit de vérifier que $\mathbb{A}_F^\times = J_F^{\mathfrak{m}} V_{\mathfrak{m}} F^\times$. Cette égalité est une conséquence du lemme 5.2.10 puisque $\mathbb{A}_F^\times / J_F^{\mathfrak{m}} \simeq \prod_{v \in \mathrm{Supp}\,\mathfrak{m}} F_v^\times$. Enfin, si $x = (x_v)_v \in J_F^{\mathfrak{m}} \cap F^\times V_{\mathfrak{m}}$, il existe

$\xi \in F^\times$ et $y \in V_\mathfrak{m}$ tels que $x = \xi y$. En particulier $x_v = \xi y_v \in \xi U_v$ pour tout $v \nmid \infty$, ce qui implique que $v_\mathfrak{p}(x_v) = v_\mathfrak{p}(\xi)$ pour tout idéal maximal $\mathfrak{p}$ de $\mathcal{O}_F$. Ainsi l'idéal fractionnaire de $\mathcal{O}_F$ défini par (x_v) est l'idéal fractionnaire principal (ξ). Comme on a de plus $\xi = xy^{-1} \in J_F^\mathfrak{m} V_\mathfrak{m} \cap F^\times = F_\mathfrak{m}^\times$, on a bien $(\xi) \in P_\mathfrak{m}$.

Remarquons à présent que l'image de $N_{E/F}(I(\mathcal{O}_E)^\mathfrak{m})$ dans $\mathbb{A}_F^\times / F^\times N_{E/F}(\mathbb{A}_E^\times)$ coïncide avec l'image de $J_E^\mathfrak{m}$ par $N_{E/F}$. Il s'agit donc du sous-groupe $N_{E/F}(J_E^\mathfrak{m})F^\times V_\mathfrak{m}/F^\times V_m$. Pour obtenir le second isomorphisme, il suffit donc de prouver que

$$N_{E/F}(J_E^\mathfrak{m})F^\times V_\mathfrak{m} = N_{E/F}(\mathbb{A}_E^\times)F^\times V_\mathfrak{m}.$$

L'inclusion du terme de gauche dans le terme de droite est évidente. Prouvons donc l'inclusion du terme de droite dans le terme de gauche. Il suffit en fait de prouver que $N_{E/F}(\mathbb{A}_E^\times)$ est inclus dans le terme de gauche. Soit $x = (x_v) \in \mathbb{A}_E^\times$. Le lemme 5.2.10 implique qu'il existe $\xi \in E^\times$ tel que $x\xi^{-1} \in J_E^\mathfrak{m} N_{E/F}^{-1}(V_\mathfrak{m})$. Ainsi $N_{E/F}(x) \in N_{E/F}(\xi) N_{E/F}(J_E^\mathfrak{m}) V_\mathfrak{m}$ et donc $N_{E/F}(x) \in N_{E/F}(J_E^\mathfrak{m}) F^\times V_\mathfrak{m}$. Ceci achève la démonstration. □

Nous allons à présent vérifier que la loi de réciprocité d'Artin peut être formulée en termes d'idéaux. Soit E/F une extension abélienne finie de corps de nombres et soit $\mathfrak{a}$ un idéal fractionnaire de $\mathcal{O}_F$, premier à tous les idéaux maximaux de $\mathcal{O}_F$ qui sont ramifiés dans E/F. On peut alors poser

$$(\mathfrak{a}, E/F) \coloneqq \prod_\mathfrak{p} (\mathfrak{p}, E/F)^{v_\mathfrak{p}(\mathfrak{a})}.$$

L'application $(-, E/F)$ est un morphisme de groupes du groupe des idéaux fractionnaires de $\mathcal{O}_F$ premiers aux idéaux ramifiés dans E/F vers le groupe $\mathrm{Gal}(E/F)$ parfois appelé *symbole d'Artin*. La loi de réciprocité d'Artin (théorème 5.2.1) implique le théorème suivant.

Théorème 5.2.12. *Soit E/F une extension abélienne finie de corps de nombres et soit S l'ensemble des places de F qui se ramifient dans E. Il existe alors un module $\mathfrak{m}$ de F tel que $S = \mathrm{Supp}(\mathfrak{m})$ et tel que, pour tout $\xi \in F_\mathfrak{m}^\times$, on a $((\xi), E/F) = 1$. Le morphisme $(-, E/F)$ alors un morphisme de groupes surjectifs $I_F^\mathfrak{m}/P_\mathfrak{m} \twoheadrightarrow \mathrm{Gal}(E/F)$ dont le noyau est engendré par les $N_{E/F}(\mathfrak{b})$ où $\mathfrak{b}$ parcourt les idéaux fractionnaires de $\mathcal{O}_E$ premiers aux idéaux maximaux au-dessus de S. De plus, pour tout élément $x \in J_F^\mathfrak{m}$, engendrant l'idéal fractionnaire $\mathfrak{a} \in I(\mathcal{O}_F)^\mathfrak{m}$, on a $\mathrm{Art}_{E/F}(x) = (\mathfrak{a}, E/F)$.*

Démonstration. D'après le théorème 5.2.1, le morphisme $\mathrm{Art}_{E/F}$ induit un isomorphisme de $\mathbb{A}_F^\times / F^\times N_{E/F}(\mathbb{A}_E^\times)$ sur $\mathrm{Gal}(E/F)$. La proposition 5.1.1 implique que $U_v \subset N_{E/F}(\mathbb{A}_E^\times)$ si $v \nmid \infty$ et $\mathfrak{p}_v$ est non ramifié dans E/F et si $v \mid \infty$ est non ramifiée

dans E/F, on a $F_v^\times \subset N_{E/F}(\mathbb{A}_E^\times)$ (voir section 5.1.5). On peut donc trouver un module $\mathfrak{m}$ tel que $\mathrm{Supp}(\mathfrak{m}) = S$ et $V_\mathfrak{m} \subset N_{E/F}(\mathbb{A}_E^\times)$. L'application $\mathrm{Art}_{E/F}$ induit une surjection $\mathbb{A}_F^\times / F^\times V_\mathfrak{m} \twoheadrightarrow \mathrm{Gal}(E/F)$. De plus, composée avec l'inclusion $J_F^\mathfrak{m} \subset \mathbb{A}_F^\times$, la proposition 5.2.11 montre que l'on obtient une surjection $J_F^\mathfrak{m} \twoheadrightarrow \mathrm{Gal}(E/F)$ qui se factorise en une surjection $I(\mathcal{O}_F)^\mathfrak{m}/P_\mathfrak{m} \twoheadrightarrow \mathrm{Gal}(E/F)$. Un calcul explicite montre alors que l'application induite $I(\mathcal{O}_F)^\mathfrak{m} \twoheadrightarrow \mathrm{Gal}(E/F)$ n'est autre que $\mathfrak{a} \mapsto (\mathfrak{a}, E/F)$. On déduit alors le résultat de la proposition 5.2.11. □

Remarque 5.2.13. On déduit de la proposition 5.2.11, que si S est un ensemble fini de places de F contenant les places ramifiées dans E/F et si $\mathfrak{m}$ est un module de support contenant S, alors l'application $J_F^\mathfrak{m} \to \mathbb{A}_F^\times / F^\times V_\mathfrak{m}$ est surjective. On en déduit que l'application d'Artin $\mathrm{Art}_{E/F}$ est complètement déterminée par ses valeurs sur les éléments $\varpi_v = (1, \dots, 1, \pi_v, 1, \dots)$ pour $v \notin \mathrm{Supp}(\mathfrak{m})$. On en déduit l'assertion d'unicité dans le théorème 5.2.1.

5.3 La première inégalité

5.3.1 Densité de Dirichlet

Soit F un corps de nombres et soit $\mathcal{P}_F$ l'ensemble des idéaux maximaux de $\mathcal{O}_F$. On dit qu'une partie $\mathcal{P}$ de $\mathcal{P}_F$ a une *densité naturelle* $\delta \in [0,1]$ si

$$\lim_{x \to +\infty} \frac{\mathrm{Card}(\{\mathfrak{p} \in \mathcal{P} \mid N(\mathfrak{p}) \leqslant x\})}{\mathrm{Card}(\{\mathfrak{p} \in \mathcal{P}_F \mid N(\mathfrak{p}) \leqslant x\})} = \delta.$$

Par ailleurs on dit que l'ensemble $\mathcal{P}$ a une *densité de Dirichlet* $\delta \in [0,1]$ si

$$\frac{\sum_{\mathfrak{p} \in \mathcal{P}} N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}_F} N\mathfrak{p}^{-s}} \longrightarrow_{\substack{s \to 1 \\ \mathrm{Re}(s) > 1}} \delta.$$

Rappelons que si $\mathrm{Re}\, s > 1$, la somme $\sum_{\mathfrak{p} \in \mathcal{P}} N\mathfrak{p}^{-s}$ est absolument convergente et que l'application $s \mapsto \sum_{\mathfrak{p} \in \mathcal{P}} N\mathfrak{p}^{-s}$ définit une fonction holomorphe sur l'ouvert des $s \in \mathbb{C}$ tels que $\mathrm{Re}(s) > 1$ (voir la démonstration de la proposition 4.3.7).

Notons log l'unique branche du logarithme, définie sur $\mathbb{C} \smallsetminus \mathbb{R}_{\leqslant 0}$ et égale à

$$\log(s) = \sum_{n \geqslant 1} \frac{(-1)^{n-1}}{n} (s-1)^n$$

lorsque $|s-1| < 1$. Il s'agit d'une fonction holomorphe sur $\mathbb{C} \smallsetminus \mathbb{R}_{\leqslant 0}$.

Proposition 5.3.1. *On a*

$$\sum_{\mathfrak{p} \in \mathcal{P}_F} N\mathfrak{p}^{-s} \sim_{\substack{s \to 1 \\ \mathrm{Re}(s) > 1}} \log\left(\frac{1}{s-1}\right).$$

Démonstration. Rappelons que l'on a (remarque 4.3.12 et corollaire 4.3.15), pour $\mathrm{Re}(s) > 1$,

$$\zeta_F(s) = \prod_{\mathfrak{p}\in\mathcal{P}_F} \frac{1}{1 - N\mathfrak{p}^{-s}} \sim_{s\to 1} \frac{a}{s-1}$$

pour un certain $a > 0$ explicite. Ainsi

$$\log(\zeta_F(s)) \sim_{s\to 1} \log\left(\frac{1}{s-1}\right).$$

De plus, lorsque $\mathrm{Re}(s) > 1$, on a

$$\begin{aligned}
\log \zeta_F(s) &= -\sum_{\mathfrak{p}\in\mathcal{P}_F} \log(1 - N\mathfrak{p}^{-s}) = \sum_{\mathfrak{p}\in\mathcal{P}_F}\sum_{n\geqslant 1} \frac{1}{n} N\mathfrak{p}^{-ns} \\
&= \sum_{n\geqslant 1} \frac{1}{n} \sum_{\mathfrak{p}\in\mathcal{P}_F} N\mathfrak{p}^{-ns} \\
&= \sum_{\mathfrak{p}\in\mathcal{P}_F} N\mathfrak{p}^{-s} + \sum_{n\geqslant 2} \frac{1}{n} \sum_{\mathfrak{p}\in\mathcal{P}_F} N\mathfrak{p} p^{-sn} \\
&= \sum_{\mathfrak{p}\in\mathcal{P}_F} N\mathfrak{p}^{-s} + g(s).
\end{aligned}$$

Comme

$$|g(s)| \leqslant [F:\mathbb{Q}] \sum_p \sum_{n\geqslant 1} \frac{1}{n} p^{-n\,\mathrm{Re}\,s} \leqslant \frac{1}{2[F:\mathbb{Q}]} \sum_p p^{-2\,\mathrm{Re}\,s} \frac{1}{1-p^{-s}}$$

est normalement convergente sur toute partie compacte de $]\frac{1}{2}, +\infty[$, on en déduit que la fonction g is holomorphic sur l'ouvert $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \frac{1}{2}\}$. On en déduit le résultat. □

Corollaire 5.3.2. *Si $\mathcal{P}$ est une partie finie de $\mathcal{P}_F$, alors $\mathcal{P}$ a une densité de Dirichlet égale à 0.*

On dit qu'un idéal maximal $\mathfrak{p}$ de $\mathcal{O}_F$ est *totalement décomposé* dans une extension finie E/F si, pour tout $\mathfrak{q} \mid \mathfrak{p}$ dans $\mathcal{O}_E$, on a $f_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{q}/\mathfrak{p}} = 1$. De façon équivalente, $\mathfrak{p}\mathcal{O}_E$ se décompose en un produit de $[E : F]$ idéaux maximaux distincts dans $\mathcal{O}_E$. Si l'extension E/F est galoisienne, un idéal maximal de $\mathcal{O}_F$ est totalement décomposé dans E si et seulement si il est non ramifié dans E et si $(\mathfrak{q}, E/F) = 1$ pour un (resp. tous) idéal maximal $\mathfrak{q}$ de $\mathcal{O}_E$ divisant $\mathfrak{p}$.

Théorème 5.3.3. *Soit E/F une extension galoisienne finie de corps de nombres. Alors l'ensemble des idéaux maximaux de $\mathcal{O}_F$ qui sont totalement décomposés dans E possède une densité de Dirichlet égale à $[E : F]^{-1}$.*

Démonstration. Soit $\mathcal{P}$ l'ensemble des idéaux maximaux de $\mathcal{O}_F$ totalement décomposés dans E/F et soit $\mathcal{P}'$ l'ensemble des idéaux maximaux de $\mathcal{O}_E$ au-dessus d'un idéal de $\mathcal{P}$. Par définition l'application $\mathcal{P}' \to \mathcal{P}$ est surjective et ses fibres sont toutes de cardinal $d \coloneqq [E : F]$. De plus, si $\mathfrak{q} \in \mathcal{P}'$ et $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_F$, alors $f_{\mathfrak{q}/\mathfrak{p}} = 1$ et donc $N(\mathfrak{q}) = N(\mathfrak{p})$. On en déduit que, pour $\mathrm{Re}(s) > 1$, on a

$$\sum_{\mathfrak{p} \in \mathcal{P}} N(\mathfrak{p})^{-s} = d^{-1} \sum_{\mathfrak{q} \in \mathcal{P}'} N(\mathfrak{q})^{-s}.$$

Par ailleurs, si $\mathfrak{q} \in \mathcal{P}_E \smallsetminus \mathcal{P}'$, et si $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_F$, soit $e_{\mathfrak{q}/\mathfrak{p}} \geqslant 2$ soit $f_{\mathfrak{q}/\mathfrak{p}} \geqslant 2$. Dans le second cas, on a nécessairement $N(\mathfrak{q}) \geqslant p^2$ où $(p) = \mathfrak{q} \cap \mathbb{Z}$. Comme il n'y a qu'un nombre fini d'idéaux qui sont dans le premier cas, et que la série

$$\sum_{\substack{\mathfrak{q} \in \mathcal{P}_E \smallsetminus \mathcal{P}' \\ f_{\mathfrak{q}/\mathfrak{p}} \geqslant 2}} |N(\mathfrak{q})^{-s}| \leqslant [E : \mathbb{Q}] \sum_p p^{-2s}$$

est absolument convergente sur $\{\mathrm{Re}(s) > \frac{1}{2}\}$, on en déduit que la fonction $s \mapsto \sum_{\mathfrak{q} \in \mathcal{P}_E \smallsetminus \mathcal{P}'} N(\mathfrak{q})^{-s}$ est holomorphe sur un voisinage de 1 et donc, en utilisant la proposition 5.3.1, on a

$$\sum_{\mathfrak{q} \in \mathcal{P}'} N(\mathfrak{q})^{-s} \sim_{s \to 1} \log\left(\frac{1}{s-1}\right).$$

On en déduit le résultat. □

On en déduit en particulier qu'il existe une infinité d'idéaux maximaux de $\mathcal{O}_F$ qui sont totalement décomposés dans une extension galoisienne finie E/F.

Corollaire 5.3.4. *Soit E/F une extension galoisienne finie de corps de nombres. Si $[E : F] > 1$, il existe une infinité d'idéaux maximaux de $\mathcal{O}_F$ qui ne sont pas totalement décomposé dans E/F.*

5.3.2 La première inégalité

Proposition 5.3.5. *Soit E/F une extension finie de corps de nombres. Alors le sous-groupe $N_{E/F}(\mathbb{A}_E^\times)$ est ouvert dans $\mathbb{A}_F^\times$ et le quotient $\mathbb{A}_F^\times / F^\times N_{E/F}(\mathbb{A}_E^\times)$ est fini.*

Démonstration. Si v est une place de F et $w \mid v$ est une place de E, alors le groupe $N_{E_w/F_v}(E_w^\times)$ est ouvert dans $F_v^\times$. C'est une conséquence de la proposition 5.1.9 dans le cas ultramétrique et c'est évident dans le cas archimédien. De plus $N_{E_w/F_v}(E_w^\times)$ contient U_v si v est non ramifiée dans E/F (par la proposition 5.1.1). On en conclut que le groupe $N_{E/F}(\mathbb{A}_E^\times)$ est ouvert dans $\mathbb{A}_F^\times$. Pour vérifier que

$\mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times)$ est fini, on raisonne comme dans le corollaire 3.2.9 en utilisant le fait que $\mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times)$ est un quotient discret du groupe compact $(\mathbb{A}_F^\times)^1/F^\times$. □

Théorème 5.3.6. *Soit E/F une extension galoisienne finie. On a alors*

$$\mathrm{Card}(\mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times)) \leqslant [E:F].$$

Démonstration. Notons $C_E \coloneqq \mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times)$. Il s'agit d'un groupe abélien fini d'après la proposition 5.3.5. Si χ est un caractère de C_E, on note encore χ le caractère de $\mathbb{A}_F^\times$ obtenu par précomposition avec $\mathbb{A}_F^\times \twoheadrightarrow C_E$. Le caractère χ est alors un caractère de Hecke unitaire (car d'image fini). Ainsi, pour tout $\mathrm{Re}(s) > 1$, on peut écrire la fonction L de ce caractère en s sous la forme d'un produit absolument convergeant (remarque 4.3.12) :

$$L(\chi, s) = \prod_{\mathfrak{p}\in\mathcal{P}_F} L(\chi_\mathfrak{p}|\cdot|_\mathfrak{p}^s) = \prod_{\mathfrak{p}\in\mathcal{P}_F} \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}}$$

où l'on a posé $\chi(\mathfrak{p}) = \chi_\mathfrak{p}(\pi_\mathfrak{p}) = \chi(\varpi_\mathfrak{p})$ si $\chi_\mathfrak{p}$ est non ramifié et $\chi(\mathfrak{p}) = 0$ si $\chi_\mathfrak{p}$ est ramifié. Notons $\delta_\chi \in \mathbb{Z}$ l'ordre d'annulation de la fonction $L(\chi, -)$ en 1, autrement dit $L(\chi, s) \sim a_\chi(s-1)^{\delta_\chi}$ pour un certain $a_\chi \in \mathbb{C}^\times$. On montre alors, comme dans la démonstration de la proposition 5.3.1, que

$$\sum_{\mathfrak{p}\in\mathcal{P}_F} \chi(\mathfrak{p})N(\mathfrak{p})^{-s} = \delta_\chi \log(s-1) + g_\delta(s) \tag{5.2}$$

pour $Re(s) > 1$ où g_χ est une fonction bornée au voisinage de 1. On déduit du théorème 4.3.13 que $\delta_\chi \geqslant -1$ pour tout χ et que $\delta_\chi = -1$ si et seulement si le caractère χ est trivial (en effet, on a $\chi = 1$ si et seulement si $\chi((\mathbb{F}_F^\times)^1) = \{1\}$ puisque l'application $(\mathbb{A}_F^\times)^1 \twoheadrightarrow C_E$ est surjective). En particulier on a $\sum_{\chi\in\widehat{C_E}} \delta_\chi \geqslant -1$.

Soit $g \in C_E$. Le lemme 4.1.21 implique que

$$\sum_{\chi\in\widehat{C_E}} \chi(g) = \begin{cases} \mathrm{Card}(C_E) & \text{si } g = 1 \\ 0 & \text{si } g \neq 1. \end{cases}$$

Notons $\mathcal{P}$ l'ensemble des idéaux maximaux $\mathfrak{p} \in \mathcal{P}_F$ tels que $\chi_\mathfrak{p}$ est non ramifié dans E/F et tels que l'image de $\varpi_\mathfrak{p}$ dans C_E est triviale. En sommant la relation (5.2) sur tous les $\chi \in \widehat{C_E}$, on obtient donc l'égalité

$$\sum_{\mathfrak{p}\in\mathcal{P}} N(\mathfrak{p})^{-s} = \mathrm{Card}(C_E)^{-1}\left(\sum_{\chi\in\widehat{C_E}} \delta_\chi\right)\log(s-1) + G(s) \tag{5.3}$$

où G est une fonction bornée au voisinage de 1.

Notons également $\mathcal{P}'$ l'ensemble des idéaux maximaux $\mathfrak{p} \in \mathcal{P}_F$ tels que $\mathfrak{p}$ est totalement décomposé dans E/F et $\chi_\mathfrak{p}$ est non ramifié. Comme $\chi_\mathfrak{p}$ n'est ramifié qu'en un nombre fini d'idéaux maximaux, le théorème 5.3.3 (et le corollaire 5.3.2) implique que $\mathcal{P}'$ est un ensemble de densité de Dirichlet $[E : F]^{-1}$, en particulier $\mathcal{P}'$ est infini. Remarquons par ailleurs que si $\mathfrak{p} \in \mathcal{P}'$, et si $\mathfrak{q} \in \mathcal{P}_E$ divise $\mathfrak{p}$, alors $N_{E/F}(\varpi_\mathfrak{q}) = \varpi_\mathfrak{p}$, de sorte que l'image de $\varpi_\mathfrak{p}$ dans C_E est triviale, et donc que $\mathcal{P}' \subset \mathcal{P}$.

Ainsi le membre de gauche dans l'équation (5.3) est équivalent à $-[E : F]^{-1} \log(s-1)$. Comme $\sum_\chi \delta_\chi \geqslant -1$, on a nécessairement $\sum_\chi \delta_\chi = -1$ et $[E : F]^{-1} \leqslant \mathrm{Card}(C_E)^{-1}$. On en déduit donc que $\mathrm{Card}(C_E) \leqslant [E : F]$ et que $\delta_\chi = 0$ si $\chi \neq 1$. □

Remarque 5.3.7. Au cours de la démonstration du théorème 5.3.6, on a prouvé que $L(\chi, 1) \neq 0$ si χ est un caractère de Hecke non trivial qui se factorise à travers le quotient C_E pour une certaine extension galoisienne finie E/F.

5.3.3 Autres conséquences

Corollaire 5.3.8. *Soit F un corps de nombres et soit $\overline{F}$ une clôture algébrique de F. Soient $E_1, E_2 \subset \overline{F}$ deux extensions galoisiennes finies de F. Pour $i \in \{1, 2\}$, notons $\mathcal{P}_i$ l'ensemble des $\mathfrak{p} \in \mathcal{P}_F$ tels que $\mathfrak{p}$ est totalement décomposé dans E_i/F. Si $\mathcal{P}_2 \smallsetminus \mathcal{P}_1$ est de densité de Dirichlet nulle, alors $E_2 \subset E_1$.*

Démonstration. Posons $E = E_1E_2$. Remarquons dans un premier temps que si $\mathfrak{p} \in \mathcal{P}_F$ est totalement décomposé dans E_1 et E_2, il est totalement décomposé dans E. En effet, on a alors, d'après le théorème 2.3.9, des isomorphismes $E_i \otimes_F F_\mathfrak{p} \simeq F_\mathfrak{p}^{[E_i:F]}$. L'algèbre $E \otimes_F F_\mathfrak{p}$ est alors un quotient de $E_1 \otimes_F E_2 \otimes_F F_\mathfrak{p} \simeq F_\mathfrak{p}^{[E_1:F][E_2:F]}$ et donc isomorphe à une somme directe de copies de $F_\mathfrak{p}$. Le théorème 2.3.9 montre alors que $\mathfrak{p}$ est totalement ramifié dans E.

On en déduit donc que $\mathcal{P}_1$ est, à un ensemble de densité Dirichlet nulle, l'ensemble des idéaux maximaux totalement décomposé dans E. On déduit du théorème 5.3.3 que $[E : F] = [E_1 : F]$, c'est-à-dire $E = E_1$ et donc $E_2 \subset E_1$. □

Corollaire 5.3.9. *Soit p un nombre premier et soit E/F une extension cyclique de corps de nombres de degré une puissance de p. Alors il existe une infinité d'idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_F$ qui sont inertes dans E/F, c'est-à-dire tels que $\mathfrak{p}\mathcal{O}_E$ est premier.*

Démonstration. Le groupe de Galois E/F est cyclique d'ordre p^r pour $r \geqslant 0$. On peut supposer $r \geqslant 1$ sinon le résultat est évident. Soit $K \subset E$ l'unique sous-corps

de E tel que $[K : F]$. Le groupe $\mathrm{Gal}(K/F)$ est alors l'unique quotient cyclique d'ordre p de $\mathrm{Gal}(E/F)$. On déduit de la section que 1.3.1 $\mathfrak{p}$ est inerte dans E/F si et seulement si l'élément de Frobenius $(\mathfrak{p}, E/F)$ est d'ordre $[E : F]$, c'est-à-dire est un générateur de $\mathrm{Gal}(E/F)$. Cette condition est encore équivalente à demander que l'image de $(\mathfrak{p}, E/F)$ dans $\mathrm{Gal}(K/F)$ est un générateur de $\mathrm{Gal}(K/F)$. Or cette image est $(\mathfrak{p}, K/F)$. Comme le groupe $(\mathfrak{p}, K/F)$ est cyclique d'ordre p, $(\mathfrak{p}, K/F)$ est un générateur si et seulement si il n'est non trivial c'est-à-dire si et seulement si $\mathfrak{p}$ n'est pas totalement décomposé dans K/F. Le résultat est alors une conséquence du corollaire 5.3.4. □

5.4 La seconde inégalité

Dans cette partie, on montre que si E/F est une extension *cyclique* de corps de nombres, alors

$$[E : F] \leqslant \mathrm{Card}(\mathbb{A}_F^\times / F^\times N_{E/F}(\mathbb{A}_E^\times)).$$

5.4.1 Le quotient de Herbrand

Soit G un groupe cyclique, soit n son cardinal et soit g un générateur de G. On appelle *G-module* un $\mathbb{Z}[G]$-module. Si A est un G-module, on définit deux endomorphismes N et $1 - g$ de A par les formules, pour $a \in A$,

$$N(a) \coloneqq a + g(a) + \cdots + g^{n-1}(a), \quad (1 - g)(a) \coloneqq a - g(a).$$

On vérifie que $N \circ (1 - g) = (1 - g) \circ N = 1 - g^n = 0$. On définit alors les groupes abéliens

$$\widehat{H}^0(A) \coloneqq \mathrm{Ker}(1 - g)/\mathrm{Im}(N) = A^G/N(A), \quad \widehat{H}^1(A) \coloneqq \mathrm{Ker}(N)/\mathrm{Im}(1 - g).$$

On note $h_0(A) \coloneqq \mathrm{Card}(\widehat{H}^0(A))$ et $h_1(A) \coloneqq \mathrm{Card}(\widehat{H}^1(A))$. Lorsque $h_0(A)$ et $h_1(A)$ sont finis, on définit le *quotient de Herbrand* de A comme la quantité

$$\theta(A) \coloneqq \frac{h_0(A)}{h_1(A)}.$$

Nous aurons parfois besoin de nous placer dans un cadre un peu plus général. Soit A un groupe abélien muni de deux endomorphismes f et g qui commutent et vérifient $g \circ f = f \circ g = 0$. Si les indices $[\mathrm{Ker}(f) : \mathrm{Im}(g)]$ et $[\mathrm{Ker}(g) : \mathrm{Im}(f)]$ sont finis, on pose

$$q_{f,g}(A) \coloneqq \frac{[\mathrm{Ker}(f) : \mathrm{Im}(g)]}{[\mathrm{Ker}(g) : \mathrm{Im}(f)]}.$$

Exemple 5.4.1. Si G est un groupe cyclique et si A est un G-module, en posant $f = 1 - \gamma$ et $g = N$, pour γ un générateur de G, on a $q_{f,g}(A) = \theta(A)$.

Proposition 5.4.2. *Soit $0 \to A \to B \to C \to 0$ une suite exacte courte de groupes abéliens. Supposons que pour $X \in \{A, B, C\}$, le groupe abélien X est muni d'endomorphismes f_X et g_X tels que $f_X \circ g_X = g_X \circ f_X = 0$. Supposons également que tous les carrés du diagramme ci-dessous sont commutatifs*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & {\scriptstyle g_A}\uparrow\downarrow{\scriptstyle f_A} & & {\scriptstyle g_B}\uparrow\downarrow{\scriptstyle f_B} & & {\scriptstyle g_C}\uparrow\downarrow{\scriptstyle f_C} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

Alors, si deux des quantités $q_{f_A,g_A}(A)$, $q_{f_B,g_B}(B)$ et $q_{f_C,g_C}(C)$ sont définies, la troisième également et on a $q_{f_B,g_B}(B) = q_{f_A,g_A}(A) q_{f_C,g_C}(C)$.

Démonstration. On applique le lemme du serpent au diagramme commutatif

$$\begin{array}{ccccccc} & & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_A} & & \downarrow{\scriptstyle f_B} & & \downarrow{\scriptstyle f_C} & & \\ 0 & \longrightarrow & \mathrm{Ker}(g_A) & \longrightarrow & \mathrm{Ker}(g_B) & \longrightarrow & \mathrm{Ker}(g_C) & & \end{array}$$

On obtient donc une suite exacte longue et un diagramme commutatif

$$\begin{array}{ccccccccccc} \mathrm{Ker}(f_A) & \longrightarrow & \mathrm{Ker}(f_B) & \longrightarrow & \mathrm{Ker}(f_C) & \xrightarrow{\delta} & \mathrm{Ker}(g_A)/\mathrm{Im}(f_A) & \longrightarrow & \mathrm{Ker}(g_B)/\mathrm{Im}(f_B) & \longrightarrow & \mathrm{Ker}(g_C)/\mathrm{Im}(f_C) \\ \downarrow & & \downarrow & & \downarrow & \nearrow & & & & & \\ \mathrm{Ker}(f_A)/\mathrm{Im}(g_A) & \longrightarrow & \mathrm{Ker}(f_B)/\mathrm{Im}(g_B) & \longrightarrow & \mathrm{Ker}(f_C)/\mathrm{Im}(g_C) & & & & & & \end{array}$$

L'existence de la flèche pointillée provient de l'égalité $\delta(\mathrm{Im}(g_C)) = \{0\}$ qui se vérifie directement en revenant à la définition du morphisme de connexion δ provenant du lemme du serpent. On obtient donc une suite exacte longue

$$\begin{aligned} \mathrm{Ker}(f_B)/\mathrm{Im}(g_B) &\longrightarrow \mathrm{Ker}(f_C)/\mathrm{Im}(g_C) \longrightarrow \\ &\longrightarrow \mathrm{Ker}(g_A)/\mathrm{Im}(f_A) \longrightarrow \mathrm{Ker}(g_B)/\mathrm{Im}(f_B) \longrightarrow \mathrm{Ker}(g_C)/\mathrm{Im}(f_C) \end{aligned}$$

que l'on peut prolonger à gauche et à droite en inversant les rôles de f et g. Pour conclure, on obtient une suite exacte longue périodique ou encore un « hexagone exact » :

$$\begin{array}{ccccc} & & \mathrm{Ker}(f_A)/\mathrm{Im}(g_A) & \longrightarrow & \mathrm{Ker}(f_B)/\mathrm{Im}(g_B) & & \\ & \nearrow & & & & \searrow & \\ \mathrm{Ker}(g_C)/\mathrm{Im}(g_C) & & & & & & \mathrm{Ker}(f_C)/\mathrm{Im}(g_C) \\ & \nwarrow & & & & \swarrow & \\ & & \mathrm{Ker}(g_B)/\mathrm{Im}(f_B) & \longleftarrow & \mathrm{Ker}(g_A)/\mathrm{Im}(f_A) & & \end{array}$$

On en déduit le résultat. □

Corollaire 5.4.3. *Soit $0 \to A \to B \to C \to 0$ une suite exacte courte de G-modules. Si, parmi $\theta(A)$, $\theta(B)$ et $\theta(C)$, deux sont définis, alors le troisième est défini et on a l'égalité $\theta(B) = \theta(A)\theta(C)$.*

Lemme 5.4.4. *Supposons que A est un groupe abélien fini et que f et g sont deux endomorphismes de A tels que $f \circ g = g \circ f = 0$, alors $q_{f,g}(A) = 1$.*

Démonstration. On a simplement

$$q_{f,g}(A) = \frac{Card(\mathrm{Ker}(f))\,\mathrm{Card}(\mathrm{Im}(g))^{-1}}{\mathrm{Card}(\mathrm{Ker}(g))\,\mathrm{Card}(\mathrm{Im}(f))^{-1}} = \frac{\mathrm{Card}(A)}{\mathrm{Card}(A)} = 1. \qquad \square$$

Lemme 5.4.5. *Soit A un groupe abélien et soient f et g deux endomorphismes de A qui commutent. Alors si $q_{0,f}(A)$ et $q_{0,g}(A)$ existent, $q_{0,fg}(A)$ existe et $q_{0,fg}(A) = q_{0,f}(A)q_{0,g}(A)$.*

Démonstration. Comme $q_{0,f}(A)$ et $q_{0,g}(A)$, les groupes $\mathrm{Ker}(f)$, $\mathrm{Ker}(g)$, $\mathrm{Coker}(f)$ et $\mathrm{Coker}(g)$ sont finis. En utilisant la proposition 5.4.2 et le lemme 5.4.4, on en déduit que $q_{0,g}(f(A))$ est défini et que $q_{0,g}(A) = q_{0,g}(f(A))$. Par ailleurs la suite exacte

$$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow \mathrm{Ker}(gf) \xrightarrow{f} \mathrm{Ker}(g) \cap f(A) \longrightarrow 0$$

implique que $\mathrm{Ker}(fg)$ est fini et que $\mathrm{Card}(fg) = \mathrm{Card}(\mathrm{Ker}(g) \cap f(A))\,\mathrm{Card}(\mathrm{Ker}(f))$. On en conclut que $q_{0,fg}(A)$ est bien défini et que

$$q_{0,f}(A)q_{0,g}(A) = \frac{\mathrm{Card}(A/f(A))\,\mathrm{Card}(f(A)/fg(A))}{\mathrm{Card}(\mathrm{Ker}(f))\,\mathrm{Card}(\mathrm{Ker}(g) \cap f(A))} = \frac{\mathrm{Card}(A/fg(A))}{\mathrm{Ker}(fg)} = q_{0,fg}(A).$$

□

Théorème 5.4.6 (Chevalley)**.** *Soit G un groupe cyclique d'ordre premier p. Soit A un G-module. Si $q_{0,p}(A)$ et $q_{0,p}(A^G)$ sont définis, $\theta(A)$ l'est aussi et on a la relation*

$$\theta(A)^{p-1} = \frac{q_{0,p}(A^G)^p}{q_{0,p}(A)}.$$

Démonstration. Fixons g un générateur de G. On a, en utilisant la proposition 5.4.2, $q_{0,p}(A) = q_{0,p}(A^G)q_{0,p}((1-g)A)$. Comme par ailleurs g agit trivialement sur A^G, on a $q_{0,p}(A^G) = \theta(A^G)$. L'endomorphime $N = 1 + g + \cdots + g^{p-1}$ annule $(1-g)A$. Ainsi $(1-g)(A)$ est un $\mathbb{Z}[\zeta_p] \simeq \mathbb{Z}[X]/(1 + X + \cdots + X^{p-1})$-module. Comme $p = (1-\zeta_p)^{p-1}\varepsilon$ avec $\varepsilon \in \mathbb{Z}[\zeta_p]^\times$, on a, en utilisant le lemme 5.4.5,

$$q_{0,p}((1-g)A) = q_{0,1-g}((1-g)A)^{p-1}.$$

Par ailleurs $q_{0,1-g}((1-g)A) = q_{1-g,0}((1-g)A)^{-1}$. Comme N agit trivialement sur $(1-g)A$, on a $q_{1-g,0}((1-g)A) = \theta(A)$ et donc $q_{0,p}((1-g)A) = \theta((1-g)A)^{1-p}$. On en déduit finalement que

$$\theta(A)^{p-1} = q_{0,p}(A^G)^{p-1} q_{0,p}((1-g)A)^{-1} = q_{0,p}(A^G)^{p-1} q_{0,p}(A)^{-1}. \qquad \square$$

5.4.2 Le quotient de Herbrand de $\mathbb{A}_E^\times/E^\times$

Soit E/F une extension cyclique de corps de nombres de degré n. Le groupe $G = \mathrm{Gal}(E/F)$ agit sur $\mathbb{A}_E^\times$ par des automorphismes continus. Il a été vu en TD que le foncteur des invariants sous G appliqué à la suite exacte

$$0 \longrightarrow E^\times \longrightarrow \mathbb{A}_E^\times \longrightarrow \mathbb{A}_E^\times/E^\times \longrightarrow 0$$

fournit une suite exacte courte

$$0 \longrightarrow F^\times \longrightarrow \mathbb{A}_F^\times \longrightarrow (\mathbb{A}_E^\times/E^\times)^G \longrightarrow 0.$$

La seconde inégalité du corps de classes est alors une conséquence immédiate du théorème suivant, dont la preuve est le but de cette section.

Théorème 5.4.7. *Soit E/F une extension cyclique de corps de nombres. Alors le quotient de Herbrand de $\mathbb{A}_E^\times/E^\times$ est défini et vaut $[E:F]$.*

Vérifions en effet que ceci implique la seconde inégalité. Si $A = \mathbb{A}_E^\times/E^\times$. On a alors $\widehat{H}^0(A) = \mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times)$ et $\widehat{H}^1(A) = \mathrm{Ker}(N_{E/F})/\mathrm{Im}(g-1)$ où g est un générateur de G. On a donc bien

$$[E:F] = \theta(A) \leqslant \mathrm{Card}(\widehat{H}^0(A)) = \mathrm{Card}(\mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times)).$$

Remarque 5.4.8. En combinant les théorèmes 5.3.6 et 5.4.7, on montre que si E/F est une extension cyclique de corps de nombres, alors $\widehat{H}^1(\mathbb{A}_E^\times/E^\times) = 0$.

5.4.3 Le cas cyclique d'ordre premier

On suppose désormais que E/F est une extension galoisienne finie de corps de nombres de degré p où p est un nombre premier. On va calculer le quotient de Herbrand du $\mathrm{Gal}(E/F)$-module $\mathbb{A}_E^\times/E^\times$.

Posons $V = V_0 = \prod_{w|\infty} E_w^\times \prod_{v\nmid\infty} \mathcal{O}_w^\times$. On a $\mathbb{A}_E^\times/E^\times V \simeq \mathrm{Cl}(\mathcal{O}_E)$ d'après les résultats de la section 3.2.2 (ou la proposition 5.2.11), qui est un groupe fini. En utilisant le lemme 5.4.4 et le corollaire 5.4.3, on en déduit que le quotient

de Herbrand de $\mathbb{A}_E^\times/E^\times$ est bien défini si et seulement si celui de $E^\times V/E^\times \simeq V/(V\cap E^\times)$ est bien défini, et on a

$$\theta(\mathbb{A}_E^\times/E^\times) = \theta(V/(V\cap E^\times)).$$

Notons que $V\cap E^\times = \mathcal{O}_E^\times$.

Nous allons montrer que les quotient de Herbrand des groupes $\prod_{w\nmid} \mathcal{O}_w^\times$, $\prod_{w|\infty} E_w^\times$ et $\mathcal{O}_E^\times$ sont bien définis et utiliser le corollaire 5.4.3 pour conclure.

Lemme 5.4.9. *Soit v une place finie de F. Alors $\theta(\prod_{w|v}\mathcal{O}_w^\times) = 1$.*

Démonstration. Posons $A = \prod_{w|v}\mathcal{O}_w^\times$. Soit ℓ la caractéristique résiduel de F_v. En utilisant le lemme 5.1.8, on voit que chaque $\mathcal{O}_w^\times$ contient un sous-groupe ouvert isomorphe à $\mathbb{Z}_\ell^{[E_w:\mathbb{Q}_\ell]}$. Ainsi A contient un sous-goupe ouvert B isomorphe à $\mathbb{Z}_\ell^{[E:F][F_v:\mathbb{Q}_\ell]}$. Comme A est compact, le quotient A/B est fini. Ainsi on déduit du corollaire 5.4.3 et du lemme 5.4.4 que $\theta(A)$ est défini si et seulement si $\theta(B)$ est défini et $\theta(A) = \theta(B)$. Par ailleurs $B^{\mathrm{Gal}(E/F)} = A^{\mathrm{Gal}(E/F)}\cap B = \mathcal{O}_v^\times \cap B$ est un $\mathbb{Z}_\ell$-module libre de rang $[F_v:\mathbb{Q}_\ell]$. On déduit alors du théorème 5.4.6 que

$$\theta(B)^{p-1} = q_{0,p}(B^{\mathrm{Gal}(E/F)})^p q_{0,p}(B)^{-1}.$$

Comme $q_{0,p}(\mathbb{Z}_\ell^m) = 1$ si $\ell\neq p$ et p^m si $\ell = p$, on en conclut que $\theta(B)^{p-1} = 1$ si $\ell\neq p$ et $p^{[F_v:\mathbb{Q}_p]p}p^{-[F_v:\mathbb{Q}_p][E:F]} = 1$ puisque $[E:F] = p$. On en déduit donc que $\theta(B) = 1$. □

Soit S l'ensemble des places finies de F telles qui sont ramifiées dans E et S' l'ensemble des places de E qui sont au-dessus d'une place de S.

Lemme 5.4.10. *On a $\theta(\prod_{w\notin S'}\mathcal{O}_w^\times) = 1$.*

Démonstration. Fixons $v\notin S$ et posons $A_v = \prod_{w|v}\mathcal{O}_w^\times$. D'après la proposition 5.1.1, on a $\mathcal{O}_v^\times = N(A_v)$. De plus, en utilisant la proposition 1.2.15, on montre que $A_v^{\mathrm{Gal}(E/F)} = (\mathcal{O}_w^\times)^{D_w} = \mathcal{O}_v^\times$ pour un choix de $w\mid v$. Ainsi $\widehat{H}^0(A_v) = 0$. On en déduit que $\widehat{H}^0(\prod_{v\notin S}A_v) = 0$. On déduit donc du lemme 5.4.9 que $\widehat{H}^1(A_v) = 0$. On vérifie alors sans difficulté que

$$\widehat{H}^0(\prod_{v\notin S}A_v) = \widehat{H}^1(\prod_{v\notin S}A_v) = 0.$$

Ainsi $\theta(\prod_{v\notin S}A_v) = 1$. □

Proposition 5.4.11. *On a $\theta(\prod_{w\nmid\infty}\mathcal{O}_w^\times) = 1$.*

Démonstration. On décompose le $\mathrm{Gal}(E/F)$-module en un produit fini

$$\prod_{w\nmid\infty} \mathcal{O}_w^\times = \left(\prod_{v\notin S}\left(\prod_{w|v}\mathcal{O}_w^\times\right)\right)\prod_{v\in S}\left(\prod_{w|v}\mathcal{O}_w^\times\right).$$

D'après les lemmes 5.4.10 et 5.4.9, chaque terme de ce produit a un quotient de Herbrand égal à 1. On déduit alors le résultat du corollaire 5.4.3. □

Proposition 5.4.12. *On a $\theta(\prod_{w|\infty} E_w^\times) = 2^{s_2-pr_2}$ où r_2 désigne le nombre de places complexes de F et s_2 celui de E.*

Démonstration. Soit v une place archimédienne de F et soit $w \mid v$ une place de E. Si $D_w = \{1\}$, alors $E_{w'} = F_v$ pour tout place $w' \mid v$ et le groupe $\mathrm{Gal}(E/F)$ agit simplement transitivement sur les places au-dessus de v et on a un isomorphisme de $\mathrm{Gal}(E/F)$-modules

$$\prod_{w|v} E_w^\times \simeq F_v^\times \otimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{Gal}(E/F)].$$

De plus les endomorphismes N et $(g-1)$ (pour un générateur g de $\mathrm{Gal}(E/F)$ sont de la forme $\mathrm{Id}_{\mathbb{F}_v^\times}\otimes N$ et $\mathrm{Id}_{\mathbb{F}_v^\times}\otimes(g-1)$ sur $F_v^\times\otimes_{\mathbb{Z}}\mathbb{Z}[\mathrm{Gal}(E/F)]$. Comme $\mathbb{Z}[\mathrm{Gal}(E/F)]$ est un $\mathbb{Z}$-module libre, on en déduit que $\widehat{H}^i(\prod_{w|v} E_w^\times) \simeq F_v^\times \otimes_{\mathbb{Z}} \widehat{H}^i(\mathbb{Z}[\mathrm{Gal}(E/F)])$ pour $i \in \{0,1\}$. Cependant un calcul direct montre que $\widehat{H}^i(\mathbb{Z}[\mathrm{Gal}(E/F)]) = 0$ pour tout $i \in \{0,1\}$. On en déduit que $\theta(\prod_{w|v} E_w^\times) = 1$.

Supposons à présent que D_w est non trivial. Il est donc d'ordre 2. Cela implique en particulier que p est pair et donc que $p = 2$. On a donc dans ce cas $D_w = \mathrm{Gal}(E/F)$ et il n'y a qu'une seule place au-dessus de v. On a de plus $F_v \simeq \mathbb{R}$ et $E_w \simeq \mathbb{C}$ et on vérifie facilement que $\theta(\mathbb{C}^\times) = 2$ (où $\mathbb{C}^\times$ est vu comme $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-module). On conclut alors en utilisant le corollaire 5.4.3. □

Proposition 5.4.13. *On a $\theta(\mathcal{O}_E^\times) = p^{s_2-pr_2-1}$ où r_2 désigne le nombre de places complexes de F et s_2 celui de E. De plus $s_2 = pr_2$ si $p \neq 2$.*

Démonstration. Soit r_1 le nombre de places réelles de F, r_2 le nombre de places complexes de F, s_1 le nombre de places réelles de E et s_2 le nombre de places complexes de E. D'après le théorème 3.2.14, le groupe $\mathcal{O}_E^\times$ est isomorphe à $\mu_E \times \mathbb{Z}^{s_1+s_2-1}$. On déduit donc de la proposition 5.4.2 et du lemme 5.4.4 que $q_{0,p}(\mathcal{O}_E^\times) = q_{0,p}(\mathbb{Z}^{s_1+s_2-1}) = p^{s_1+s_2-1}$. De même, $q_{0,p}((\mathcal{O}_E^\times)^{\mathrm{Gal}(E/F)}) = q_{0,p}(\mathcal{O}_F^\times) = p^{r_1+r_2-1}$. Ainsi le théorème 5.4.6 implique que

$$\theta(\mathcal{O}_E^\times)^{p-1} = p^{p(r_1+r_2-1)}p^{-(s_1+s_2-1)} = p^{pr_1-s_1+pr_2-s_2-(p-1)}.$$

Comme $[E : F] = p$, on a $s_1 + 2s_2 = p(r_1 + 2r_2)$, on en déduit

$$\theta(\mathcal{O}_E^\times) = p^{s_2 - pr_2 - (p-1)}.$$

Si p est impair, toutes les places archimédiennes sont non ramifiées dans E/F et on a donc $s_2 = pr_2$, et le résultat voulu. Si par contre $p = 2$, alors $p - 1 = 1$ et on obtient à nouveau le résultat cherché. □

Corollaire 5.4.14. *Soit E/F une extension cyclique de corps de nombres de degré premier, alors $\theta(\mathbb{A}_E^\times / E^\times) = [E : F]$.*

Démonstration. Soit p le degré de E/F. On a alors

$$\begin{aligned}\theta(\mathbb{A}_E^\times / E^\times) &= \theta\left(\prod_{w\nmid\infty} \mathcal{O}_E^\times\right) \theta\left(\prod_{w|\infty} E_w^\times\right) \theta(\mathcal{O}_E^\times)^{-1} \\ &= 2^{s_2 - pr_2} p^{pr_2 - s_2 + 1} = p.\end{aligned}$$

En effet, d'après la proposition 5.4.13, on a $s_2 - pr_2 = 0$ si $p \neq 2$. □

5.5 La loi de réciprocité

5.5.1 Construction

Soit E/F une extension abélienne de corps de nombres. Soit S l'ensemble des places de F qui sont ramifiées dans E/F et soit $\mathfrak{m}$ un module de F tel que $S \subset \mathrm{Supp}(\mathfrak{m})$. On définit alors un morphisme de groupes $A_{E/F} : I(\mathcal{O}_F)^{\mathfrak{m}} \to \mathrm{Gal}(E/F)$ en posant, pour $\mathfrak{a} \in I(\mathcal{O}_F)^{\mathfrak{m}}$,

$$A_{E/F}(\mathfrak{a}) \coloneqq (\mathfrak{a}, E/F).$$

Remarque 5.5.1. Soit $\mathfrak{b} \in I(\mathcal{O}_E)^{\mathfrak{m}}$. On a alors $(N_{E/F}(\mathfrak{b}), E/F) = 1$. En effet, il suffit de le vérifier lorsque $\mathfrak{b}$ est un idéal maximal de $\mathcal{O}_E$. On a alors $N_{E/F}(\mathfrak{b}) = \mathfrak{p}^{f_{\mathfrak{b}/\mathfrak{p}}}$ où $\mathfrak{p} = \mathfrak{b} \cap \mathcal{O}_F$. Ainsi

$$(N_{E/F}(\mathfrak{b}), E/F) = (\mathfrak{p}, E/F)^{f_{\mathfrak{b}/\mathfrak{p}}}$$

et, comme $(\mathfrak{p}, E/F)$ est d'ordre $f_{\mathfrak{b}/\mathfrak{p}}$, on a $A_{E/F}(N_{E/F}(\mathfrak{b})) = 1$. Ainsi $N_{E/F}(I(\mathcal{O}_E)^{\mathfrak{m}}) \subset \mathrm{Ker}(A_{E/F})$.

Supposons à présent que le module $\mathfrak{m}$ vérifie la propriété $V_{\mathfrak{m}} \subset N_{E/F}(\mathbb{A}_E^\times)$.

D'après la proposition 5.2.11, il existe une surjection naturelle $I(\mathcal{O}_F)^{\mathfrak{m}} \twoheadrightarrow \mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times)$ dont le noyau est le sous-groupe $P_{\mathfrak{m}}N_{E/F}(I(\mathcal{O}_E)^{\mathfrak{m}})$. La remarque 5.5.1 implique que $P_{\mathfrak{m}}N_{E/F}(I(\mathcal{O}_E)^{\mathfrak{m}})$ est dans le noyau de $\mathrm{Ker}(A_{E/F})$ si et seulement si $P_{\mathfrak{m}} \subset \mathrm{Ker}(A_{E/F})$. Si tel est le cas, l'application $A_{E/F}$ se factorise en un morphisme de groupes $\mathrm{Art}_{E/F} : \mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times)$.

Proposition 5.5.2. *Soit E/F une extension abélienne finie de corps de nombres. Supposons que*

a) l'application $A_{E/F} : I(\mathcal{O}_F)^{\mathfrak{m}} \to \mathrm{Gal}(E/F)$ est surjective ;

b) on a $P_{\mathfrak{m}} \subset \mathrm{Ker}(A_{E/F})$.

Alors il existe un isomorphisme de groupes $\mathrm{Art}_{E/F} : \mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times) \xrightarrow{\sim} \mathrm{Gal}(E/F)$ tel que pour presque toute place finie v de F non ramifiée dans E, on a $\mathrm{Art}_{E/F}(\varpi_v) = (\mathfrak{p}_v, E/F)$, où ϖ_v est défini dans l'énoncé du théorème 5.2.1.

Démonstration. Le point b) implique que l'application $A_{E/F}$ se factorise en un morphisme $\mathrm{Art}_{E/F} : \mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times) \to \mathrm{Gal}(E/F)$. Le point a) implique que ce morphisme est surjectif et on déduit du théorème 5.3.6 qu'il est en fait bijectif. La caractérisation en presque toutes les places finies se déduit de la définition de $A_{E/F}$ car, si $v \notin \mathrm{Supp}(\mathfrak{m})$, l'élément $\mathfrak{p}_v \in I(\mathcal{O}_F)^{\mathfrak{m}}$ est envoyé sur la classe de ϖ_v dans le quotient $\mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times)$ et donc $\mathrm{Art}_{E/F}(\varpi_v) = A_{E/F}(\mathfrak{p}_v) = (\mathfrak{p}_v, E/F)$. □

Remarque 5.5.3. Soit K/F une extension finie de F. L'extension EK/K est alors abélienne est son groupe de Galois est isomorphe à un sous-groupe de $\mathrm{Gal}(E/F)$. On a de plus le diagramme commutatif suivant

$$\begin{array}{ccc} I(\mathcal{O}_K^{\mathfrak{m}}) & \xrightarrow{N_{K/F}} & I(\mathcal{O}_F)^{\mathfrak{m}} \\ \downarrow{\scriptstyle A_{EK/K}} & & \downarrow{\scriptstyle A_{E/F}} \\ \mathrm{Gal}(EK/K) & \hookrightarrow & \mathrm{Gal}(E/F). \end{array}$$

De même si $F \subset E' \subset E$ est une sous-extension, l'extension E'/F est abélienne et on a des diagrammes commutatifs

$$\begin{array}{ccc} I(\mathcal{O}_F)^{\mathfrak{m}} & \xrightarrow{A_{E/F}} & \mathrm{Gal}(E/F) \\ & \searrow^{A_{E'/F}} & \downarrow \\ & & \mathrm{Gal}(E'/F) \end{array} \qquad \begin{array}{ccc} I(\mathcal{O}_{E'})^{\mathfrak{m}} & \xrightarrow{N_{E'/F}} & I(\mathcal{O}_F)^{\mathfrak{m}} \\ \downarrow{\scriptstyle A_{E/E'}} & & \downarrow{\scriptstyle A_{E/F}} \\ \mathrm{Gal}(E/E') & \hookrightarrow & \mathrm{Gal}(E/F). \end{array}$$

Ces trois diagrammes se vérifient directement en calculant l'image d'un idéal maximal par les différents chemins possibles et en utilisant les formules de la proposition 1.3.3.

5.5.2 Surjectivité de $A_{E/F}$

Théorème 5.5.4. *Le morphisme $A_{E/F} : I(\mathcal{O}_F)^{\mathfrak{m}} \to \mathrm{Gal}(E/F)$ est surjectif.*

Démonstration. Le groupe $\mathrm{Gal}(E/F)$ est abélien fini. Le théorème de structure des groupes abéliens finis montre qu'il est engendré par ses éléments d'ordre une puissance d'un nombre premier. Il suffit donc de prouver que si $\sigma \in \mathrm{Gal}(E/F)$ est d'ordre une puissance d'un nombre premier, alors σ est dans l'image de $A_{E/F}$. Soit σ un tel élément et soit H le sous-groupe de $\mathrm{Gal}(E/F)$ engendré par σ. Posons $K = E^H$. L'extension E/K est alors cyclique d'ordre une puissance de nombre premier. Le corollaire 5.3.9 implique qu'il existe un idéal maximal $\mathfrak{q} \subset \mathcal{O}_K$ tel que $\mathfrak{q} \cap \mathcal{O}_F \notin \mathrm{Supp}(\mathfrak{m})$ et $(\mathfrak{q}, E/K)$ est un générateur de H. Il existe donc $m \geqslant 1$ tel que $(\mathfrak{q}^m, E/K) = \sigma$. On déduit alors de la remarque 5.5.3 que $A_{E/F}(N_{K/F}(\mathfrak{q}^m), E/F) = \sigma$. □

5.5.3 Le noyau de $A_{E/F}$

Soit E/F une extension abélienne finie. On veut à présent montrer qu'il existe un module $\mathfrak{m}$ tel que $P_{\mathfrak{m}} \subset \mathrm{Ker}(A_{E/F})$.

Définition 5.5.5. *On dit qu'une paire $(E/F, \mathfrak{m})$ constituée d'une extension abélienne finie de corps de nombres et d'un module de F est* admissible *si les conditions suivantes sont satisfaires*

a) l'ensemble $\mathrm{Supp}(\mathfrak{m})$ *contient les places de F qui sont ramifiées dans E/F ;*

b) on a $V_{\mathfrak{m}} \subset N_{E/F}(\mathbb{A}_E^{\times})$;

c) on a $P_{\mathfrak{m}} \subset \mathrm{Ker}(A_{E/F})$.

Remarque 5.5.6. Si la paire $(E/F, \mathfrak{m})$ est admissible alors le théorème 5.5.4 implique que les propriétés de la proposition 5.5.2 sont vérifiées et l'existence de la loi de réciprocité d'Artin $\mathrm{Art}_{E/F}$ pour l'extension E/F.

Proposition 5.5.7. *Soit E/F une extension abélienne finie de corps de nombres.*

1) Si $\mathfrak{m} \leqslant \mathfrak{m}'$, alors si $(E/F, \mathfrak{m})$ est admissible, $(E/F, \mathfrak{m}')$ est admissible.

2) Soit K/F une extension finie. Soit $\mathfrak{m}_K$ le module de K défini par

$$\mathfrak{m}_K(w) = \begin{cases} e_{w/v}\mathfrak{m}(v) & \text{si } w \text{ est finie et } v = w|_F \\ 0 & \text{si } E_w \simeq \mathbb{C} \\ \mathfrak{m}(v) & \text{si } E_w \simeq \mathbb{R}. \end{cases}$$

Alors $N_{K/F}(K_{\mathfrak{m}_K}^{\times}) \subset F_{\mathfrak{m}}^{\times}$ et si $(E/F, \mathfrak{m})$ est admissible, alors $(EK/K, \mathfrak{m}_K)$ est admissible.

3) Si $F \subset E' \subset E$ est une sous-extension. Si $(E/F, \mathfrak{m})$ est admissible, alors $(E'/F, \mathfrak{m})$ est admissible.

4) Si $F \subset E_1, \ldots, E_r \subset E$ sont des sous-extensions telles que $E = E_1 \cdots E_r$. Alors si les paires $(E_i/F, \mathfrak{m}_i)$ sont admissibles, alors la paire $(E/F, \mathfrak{m})$ est admissible où $\mathfrak{m}$ désigne le module défini par

$$\mathfrak{m}(v) = \sup_i \mathfrak{m}_i(v) \quad \forall v \in \Sigma_F.$$

Démonstration. La propriété 1) est une conséquence immédiate du fait que $\mathfrak{m} \leqslant \mathfrak{m}'$ implique $\mathrm{Supp}(\mathfrak{m}) \subset \mathrm{Supp}(\mathfrak{m}')$, $V_{\mathfrak{m}'} \subset V_{\mathfrak{m}}$ et $P_{\mathfrak{m}'} \subset P_{\mathfrak{m}}$.

Les propriétés 2) et 3) se déduisent des diagrammes commutatifs de la remarque 5.5.3.

Dans la situation de la propriété 4), l'application $\sigma \mapsto (\sigma_{E_1}, \ldots, \sigma_{E_r})$ induit une injection de $\mathrm{Gal}(E/F)$ dans $\mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_r/F)$. Comme par ailleurs $P_{\mathfrak{m}} \subset P_{\mathfrak{m}_i}$ pour tout $1 \leqslant i \leqslant r$. On déduit encore de la remarque 5.5.3 que l'image de $A_{E/F}(P_{\mathfrak{m}})$ est contenu dans le noyau de $\mathrm{Gal}(E/F) \to \mathrm{Gal}(E_i/F)$ pour tout $1 \leqslant i \leqslant r$ et donc que $A_{E/F}(P_{\mathfrak{p}}) = \{1\}$. □

Proposition 5.5.8. *Soit $n \geqslant 1$ un entier et soit $\mathfrak{m}_n$ le module de $\mathbb{Q}$ défini par $\mathfrak{m}_n(p) = v_p(n)$ pour p premier et $\mathfrak{m}_n(\infty) = 1$. Alors il existe un module $\mathfrak{m} \geqslant \mathfrak{m}_n$ de même support tel que $(\mathbb{Q}(\zeta_n)/\mathbb{Q}, \mathfrak{m})$ est admissible.*

Remarque 5.5.9. On peut en fait montrer que $(\mathbb{Q}(\zeta_n)/\mathbb{Q}, \mathfrak{m}_n)$ est admissible mais cela demande de démontrer en plus que $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\mathbb{A}^\times_{\mathbb{Q}(\zeta_n)}) = V_{\mathfrak{m}_n}$.

Démonstration. L'ensemble $\mathrm{Supp}(\mathfrak{m})$ est l'ensemble des diviseurs premiers p de n ainsi que la place ∞. Il contient donc l'ensemble des places ramifiées dans $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ (voir exemple 1.2.26). On peut donc trouver $\mathfrak{m} \geqslant \mathfrak{m}_n$ de même support que $\mathfrak{m}_n$ tel que $V_{\mathfrak{m}} \subset N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\mathbb{A}^\times_{\mathbb{Q}(\zeta_n)})$. Il reste à vérifier que $P_{\mathfrak{m}} \subset \mathrm{Ker}(A_{\mathbb{Q}(\zeta_n)/\mathbb{Q}})$. On va en fait vérifier que $P_{\mathfrak{m}_n} \subset \mathrm{Ker}(A_{\mathbb{Q}(\zeta_n)/\mathbb{Q}})$. Le groupe $\mathbb{Q}^\times_{\mathfrak{m}_n}$ est le groupe des nombres rationnels x tels que $v_p(x-1) \geqslant v_p(n)$ pour p premier divisant n et $x > 0$. Ainsi une fraction réduite $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ appartient à $\mathbb{Q}^\times_{\mathfrak{m}_n}$ si et seulement si $a > 0$, $b \wedge n = 1$ et $v_p(a-b) \geqslant v_p(n)$, c'est-à-dire si et seulement si $a > 0$ et $a \equiv b \bmod n$. Par ailleurs on a vu (exemple 1.3.6) que le groupe de Galois qu'il existe un isomorphisme de groupes entre $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ envoyant $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ sur p pour $p \nmid n$. On en conclut que si $\frac{a}{b} \in P_{\mathfrak{m}_n}$, on a

$$A_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\tfrac{a}{b}) = A_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(a) A_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(b)^{-1} = ab^{-1} \bmod n = 1 \bmod n. \qquad \square$$

Corollaire 5.5.10. *Soit E/F une extension abélienne de corps de nombres telle que $E \subset F(\zeta_n)$ pour un certain $n \geqslant 1$. Il existe un module $\mathfrak{m}$ de F tel que $(E/F, \mathfrak{m})$ est admissible.*

Démonstration. On déduit en effet de la proposition 5.5.8 ainsi que des propriétés 2) et 3) de la proposition 5.5.7 que la paire $(E/F, \mu_{n,F})$ est admissible. □

Théorème 5.5.11. *Soit E/F une extension cyclique de corps de nombres telle que*

$$\mathrm{Card}(\mathbb{A}_F^\times / F^\times \mathbb{A}_E^\times) = [E : F].$$

Soit $\mathfrak{m}$ un module de F dont le support contient toutes les places de F ramifiées dans E/F et tel que $V_\mathfrak{m} \subset N_{E/F}(\mathbb{A}_E^\times)$. Alors la paire $(E/F, \mathfrak{m})$ est admissible.

Au cours de la preuve nous aurons besoin du lemme suivant, qui sera démontré plus tard.

Lemme 5.5.12 (« Lemme d'Artin »)**.** *Soit E/F une extension cyclique de corps de nombres. Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_F$ et soit $s \in \mathbb{N}^*$ tel que $s \in \mathfrak{p}$. Il existe alors un entier $m \in \mathbb{N}^*$ et un élément $\tau \in \mathrm{Gal}(F(\zeta_m)/F)$ tels que*

1) on a $m \wedge s = 1$;

2) on a $E \cap F(\zeta_m) = F$ et $F \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$;

3) les éléments $(\mathfrak{p}, F(\zeta_m)/F)$ et τ ont des ordres multiples de $[E : F]$ dans $\mathrm{Gal}(F(\zeta_m)/F)$;

4) les sous-groupes de $\mathrm{Gal}(F(\zeta_m)/F)$ engendrés par τ et par $(\mathfrak{p}, F(\zeta_m)/F)$ ont pour intersection le sous-groupe réduit à 1.

Démonstration. Voir [Jan, Prop. 5.5]. □

Remarque 5.5.13. Soit E/F une extension cyclique de corps de nombres et soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_F$, $s \in \mathbb{N}^*$, $m \in \mathbb{N}^*$ et $\tau \in \mathrm{Gal}(F(\zeta_m)/F)$ les conditions du lemme 5.5.12. Supposons de plus que $\mathfrak{p}$ est non ramifié dans E/F. Comme s est premier à m, les nombres premiers divisant s sont non ramifiés dans $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ et donc $\mathfrak{p}$ est non ramifié dans $F(\zeta_m)/F$. Ainsi $\mathfrak{p}$ est non ramifié dans $E(\zeta_m)/F$. Comme $E \cap F(\zeta_m) = F$, on a un isomorphisme de groupes $\mathrm{Gal}(E(\zeta_m)/F) \xrightarrow{\sim} \mathrm{Gal}(E/F) \times \mathrm{Gal}(F(\zeta_m)/F)$ donné par $\sigma \mapsto (\sigma|_E, \sigma|_{F(\zeta_m)})$. On utilise cet isomorphisme pour identifier ces deux groupes. Fixons σ un générateur du groupe $\mathrm{Gal}(E/F)$. Soit H le sous-groupe de $\mathrm{Gal}(E(\zeta_m)/F)$ engendré par les éléments (σ, τ) et $(\mathfrak{p}, E(\zeta_m)/F) = ((\mathfrak{p}, E/F), (\mathfrak{p}, F(\zeta_m)/F))$. Posons $K = E^H$. Le groupe $\mathrm{Gal}(E(\zeta_m)/K(\zeta_m))$ est le noyau de l'application $\mathrm{Gal}(E(\zeta_m)/F) \to \mathrm{Gal}(E(\zeta_m)/K) \times \mathrm{Gal}(E(\zeta_m)/F(\zeta_m))$, on a donc $\mathrm{Gal}(E(\zeta_m)/K(\zeta_m)) = H \cap \langle(\sigma, 1)\rangle$. Soit $x \in H \cap \langle(\sigma, 1)\rangle$. On peut écrire

$$x = (\sigma, \tau)^a (\mathfrak{p}, E(\zeta_m)/F)^b = (\sigma^c, 1)$$

pour des entiers a, b, c. Autrement dit on a les égalités

$$\begin{cases} \sigma^a(\mathfrak{p}, E/F)^b = \sigma^c \\ \tau^a(\mathfrak{p}, F(\zeta_m)/F)^b = 1. \end{cases}$$

Ainsi $\tau^a = (\mathfrak{p}, F(\zeta_m)/F)^{-b} \in \langle\tau\rangle \cap \langle(\mathfrak{p}, F(\zeta_m)/F)\rangle$ dans $\mathrm{Gal}(F(\zeta_m)/F)$, de sorte que $\tau^a = (\mathfrak{p}, F(\zeta_m)/F)^b = 1$ et donc que $a, b \in \mathbb{Z}[E : F]$. Comme le groupe $\mathrm{Gal}(E/F)$ est d'ordre $[E : F]$, on a finalement $x = 1$. Ainsi $\mathrm{Gal}(E(\zeta_m)/K(\zeta_m)) = 1$ et $E(\zeta_m) = K(\zeta_m)$. De plus, puisque $(\mathfrak{p}, E(\zeta_m)/F) \in H$, l'idéal maximal $\mathfrak{p}$ est totalement décomposé dans K/F.

Démonstration du théorème 5.5.11. Fixons σ un générateur du groupe cyclique $\mathrm{Gal}(E/F)$. Fixons aussi $M \in \mathbb{N}^*$ un entier tel que, pour tout $n \geqslant 1$, $E \cap F(\zeta_n) \subset F(\zeta_M)$ et $F \cap \mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_M)$. Un tel M existe bien car les corps E et F ne contiennent qu'un nombre fini de sous-corps.

Soit $\mathfrak{a} \in I(\mathcal{O}_F)^{\mathfrak{m}}$ tel que $A_{E/F}(\mathfrak{a}) = 1$ et posons $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ sa décomposition en produit d'idéaux maximaux (on suppose les $\mathfrak{p}_i$ distincts). Soit $s_1 \in \mathbb{N}^*$ un entier multiple de M, appartenant à tous les idéaux maximaux du support de $\mathfrak{m}$ et appartenant à $\mathfrak{p}_1$. On construit alors, pour $1 \leqslant i \leqslant r$ des éléments $s_i \in \mathbb{N}^*$, $m_i \in \mathbb{N}^*$ et $\tau_i \in \mathrm{Gal}(F(\zeta_{m_i})/F)$ tels que $s_{i+1} = s_i m_i$ pour $1 \leqslant i \leqslant r-1$ et tels que m_i et τ_i satisfont les propriétés du lemme 5.5.12 pour les données $\mathfrak{p}_i$ et s_i lorsque $1 \leqslant i \leqslant r$.

Pour $1 \leqslant i \leqslant r$, notons H_i le sous-groupe de $\mathrm{Gal}(F(\zeta_{m_i})/F) \simeq \mathrm{Gal}(E/F) \times \mathrm{Gal}(F(\zeta_{m_i})/F)$ engendrés par (σ, τ) et $(\mathfrak{p}, E(\zeta_{m_i})/F)$. Soit $K_i := E(\zeta_{m_i})^{H_i}$. D'après la remarque 5.5.13, on a $E(\zeta_{m_i}) = K(\zeta_{m_i})$. Posons alors $m = m_1 \cdots m_r$ et $K = K_1 \cdots K_r \subset E(\zeta_m)$.

Les entiers $m_1, \ldots, m_r$ sont premiers entre eux deux à deux, et premiers à M. Ainsi le lemme 5.5.18 implique que

$$\mathrm{Gal}(E(\zeta_m)/F) \simeq \mathrm{Gal}(E/F) \times \mathrm{Gal}(F(\zeta_{m_1})/F) \times \cdots \times \mathrm{Gal}(F(\zeta_{m_r})/F).$$

En identifiant ces deux groupes au moyen de cet isomorphisme, on voit que l'élément $(\sigma, \tau_1, \ldots, \tau_r)$ est dans $\mathrm{Gal}(E(\zeta_{m_i})/K_i)$ pour tout $1 \leqslant i \leqslant r$. On a donc

$$(\sigma, \tau_1, \ldots, \tau_r) \in \mathrm{Gal}(E(\zeta_m)/K).$$

Comme la restriction de cet élément à E est σ, on en conclut que $F = E \cap K$.

On déduit de la remarque 5.5.3 que, pour tout module $\mathfrak{m}' \geqslant \mathfrak{m}$, le diagramme

suivant commute

$$\begin{array}{ccc} I(\mathcal{O}_K^{\mathfrak{m}'}) & \xrightarrow{N_{K/F}} & I(\mathcal{O}_F)^{\mathfrak{m}'} \\ \downarrow{\scriptstyle A_{EK/K}} & & \downarrow{\scriptstyle A_{E/F}} \\ \mathrm{Gal}(EK/K) & \hookrightarrow & \mathrm{Gal}(E/F). \end{array}$$

L'égalité $F = E \cap K$ implique que la flèche horizontale inférieure est un isomorphisme. On déduit donc du théorème 5.5.4 qu'il existe un idéal $\mathfrak{b}_0 \in I(\mathcal{O}_K)^{\mathfrak{m}'}$ tel que $A_{E/F}(N_{K/F}(\mathfrak{b}_0)) = \sigma$. Quitte à agrandir $\mathfrak{m}'$ pour que son support contienne les diviseurs de m, on peut donc supposer que $\mathfrak{b}_0 \in I(\mathcal{O}_K)^{\mathfrak{m}'}$ et que $\mathfrak{b}_0$ est premier à m.

Pour $1 \leqslant i \leqslant r$, posons $A_{E/F}(\mathfrak{p}_i^{a_i}) = \sigma^{d_i}$. Soit $d = d_1 + \cdots + d_r$. L'égalité $A_{E/F}(\mathfrak{a}) = 1$ implique alors $d \in \mathbb{Z}[E : F]$. Comme $\mathfrak{p}_i$ est totalement décomposé dans K_i (voir remarque 5.5.13), il existe $\mathfrak{q}_i$ idéal maximal de $\mathcal{O}_{K_i}$ tel que $N_{K_i/F}(\mathfrak{q}_i) = \mathfrak{p}_i$. Posons alors $\mathfrak{c}_i := \mathfrak{q}_i^{a_i} N_{K/K_i}(\mathfrak{b}_0)^{-d_i} \in I(\mathcal{O}_{K_i})^{\mathfrak{m}}$. On a alors $A_{EK_i/K_i}(\mathfrak{c}_i) = A_{E/F}(N_{K_i/F}(\mathfrak{c}_i)) = 1$. Or $EK_i \subset E(\zeta_{m_i}) = K(\zeta_{m_i})$ (voir la remarque 5.5.13). On déduit donc du corollaire 5.5.10 (et de la propriété 1) de la proposition 5.5.7) qu'il existe un module $\mathfrak{m}_i \geqslant \mathfrak{m}_{K_i}$ de K_i dont le support est inclus dans l'union de $\mathrm{Supp}(\mathfrak{m})$ et de l'ensemble des diviseurs de m_i et tel que la paire $(EK_i/K_i, \mathfrak{m}_i)$ est admissible. On en déduit alors (voir remarque 5.5.6) que $\mathrm{Ker}(A_{EK_i/K_i}) = P_{\mathfrak{m}_i} N_{EK_i/K_i}(I(\mathcal{O}_{EK_i})^{\mathfrak{m}_i})$. Il existe donc $\gamma_i \in K_{i,\mathfrak{m}_i}^{\times}$ et $\mathfrak{d}_i \in I(\mathcal{O}_{EK_i})^{\mathfrak{m}_i}$ tels que $\mathfrak{c}_i = (\gamma_i) N_{EK_i/K_i}(\mathfrak{d}_{K_i})$ (noter que l'on a bien $\mathfrak{c}_i \in I(\mathcal{O}_{K_i})^{\mathfrak{m}_i}$).

Posons $\mathfrak{b} = N_{K/F}(\mathfrak{b}_0)$. On peut donc écrire

$$\begin{aligned} \mathfrak{a}\mathfrak{b}^{-d} &= \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} \mathfrak{b}^{-d_i} = \prod_{i=1}^{r} N_{K_i/F}(\mathfrak{c}_i) \\ &= \prod_{i=1}^{r} N_{K_i/F}((\gamma_i) N_{EK_i/F_i}(\mathfrak{d}_i) \\ &= (\alpha) N_{E/F}\left(\prod_{i=1}^{r} N_{EK_i/E}(\mathfrak{d}_i) \right) \end{aligned}$$

où $\alpha = \prod_{i=1}^{r} N_{K_i/F}(\gamma_i)$. Comme $\gamma_i \in K_{i,\mathfrak{m}_i}^{\times} \subset K_{i,\mathfrak{m}_{K_i}}^{\times}$, on a $N_{K_i/F}(\gamma_i) \in F_{\mathfrak{m}}^{\times}$ (par la propriété 2) de la proposition 5.5.7) et donc $\alpha \in F_{\mathfrak{m}}^{\times}$. Par ailleurs $N_{EK_i/E}(\mathfrak{d}_i) \in I(\mathcal{O}_E)^{\mathfrak{m}}$ pour tout i, donc $\mathfrak{a}\mathfrak{b}^{-d} \in P_{\mathfrak{m}} N_{E/F}(\mathrm{i}(\mathcal{O}_E)^{\mathfrak{m}})$. Enfin remarquons que $d \in \mathbb{Z}[E : F]$, on peut donc écrire $d = [E : F]d'$ et $\mathfrak{b}^d = N_{E/F}(\mathfrak{b}^{d'} \mathcal{O}_E)$ de sorte que $\mathfrak{a} \in P_{\mathfrak{m}} N_{E/F}(I(\mathcal{O}_E)^{\mathfrak{m}})$.

On a donc prouvé que $\mathrm{Ker}(A_{E/F}) \subset P_{\mathfrak{m}} N_{E/F}(I(\mathcal{O}_E)^{\mathfrak{m}})$. On déduit du théorème 5.5.4 que $\mathrm{Ker}(A_{E/F})$ est un sous-groupe d'indice $[E : F]$ de $I(\mathcal{O}_F)^{\times}$ et de la proposition 5.2.11 que $P_{\mathfrak{m}} N_{E/F}(I(\mathcal{O}_E)^{\mathfrak{m}})$ est un sous-groupe d'indice $\mathrm{Card}(\mathbb{A}_F^{\times}/F^{\times} N_{E/F}(\mathbb{A}_E^{\times}))$. Par notre hypothèse ces deux sous-groupes ont le même indice, ils sont donc égaux.

En particulier $P_{\mathfrak{m}}N_{E/F}(I(\mathcal{O}_E)^{\mathfrak{m}}) \subset \mathrm{Ker}(A_{E/F})$. La paire $(E/F, \mathfrak{m})$ est donc admissible. □

5.5.4 Conclusions

On peut à présent démontrer le cas général de la seconde inégalité.

Lemme 5.5.14. *Soit E/F une extension abélienne de corps de nombres et soit $F \subset K \subset E$ une sous-extension telle que E/K est cyclique d'ordre premier. Alors le groupe $\mathrm{Gal}(K/F)$ agit trivialement sur le quotient $\mathbb{A}_K^\times/K^\times N_{E/K}(\mathbb{A}_E^\times)$.*

Démonstration. On déduit du corollaire 5.4.14, du théorème 5.5.11 et de la remarque 5.5.6, l'existence de l'isomorphisme de réciprocité d'Artin $\mathrm{Art}_{E/K} : \mathbb{A}_K^\times/K^\times N_{E/K}(\mathbb{A}_E^\times) \simeq \mathrm{Gal}(E/K)$. Si $\tau \in \mathrm{Gal}(E/F)$, on a alors un diagramme commutatif (voir remarque 5.2.2)

$$\begin{array}{ccc} \mathbb{A}_K^\times & \xrightarrow{\quad\tau\quad} & \mathbb{A}_K^\times \\ \downarrow{\scriptstyle \mathrm{Art}_{E/K}} & & \downarrow{\scriptstyle \mathrm{Art}_{E/K}} \\ \mathrm{Gal}(E/K) & \xrightarrow{\tau\cdot\tau^{-1}} & \mathrm{Gal}(E/K). \end{array}$$

Comme le groupe $\mathrm{Gal}(E/F)$ est abélien, la flèche horizontale inférieure est triviale, ce qui implique que la flèche horizontale supérieure est triviale, ce qui fournit le résultat. □

Théorème 5.5.15. *Soit E/F une extension cyclique de corps de nombres. Alors on a $h_0(\mathbb{A}_E^\times/E^\times) = [E : F]$ et $h_1(\mathbb{A}_E^\times/E^\times) = 1$. En particulier $\theta(\mathbb{A}_E^\times/E^\times) = [E : F]$.*

Démonstration. Si K est un corps de nombres, on note C_K le groupe $\mathbb{A}_K^\times/K^\times$. On démontre le résultat par récurrence sur $[E : F]$. Lorsque $[E : F]$ est premier, on a $\theta(C_E) = [E : F]$ par le corollaire 5.4.14. La preuve de 5.4.2 montre qu'il existe une suite exacte

$$\widehat{H}^0(E^\times) \longrightarrow \widehat{H}^0(\mathbb{A}_E^\times) \longrightarrow \widehat{H}^0(C_E) \longrightarrow \widehat{H}^1(E^\times).$$

Comme $\widehat{H}^0(E^\times) = F^\times/N_{E/F}(E^\times)$, $\widehat{H}^0(\mathbb{A}_E^\times) = \mathbb{A}_F^\times$ et $\widehat{H}^1(E^\times) = 0$ (par le lemme 5.5.19), on en déduit que $\widehat{H}^0(C_E) \simeq C_F/N_{E/F}(C_E)$. En particulier $h_0(C_E) = \mathrm{Card}(\mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times))$ et on déduit de l'égalité $\theta(C_E) = [E : F]$ et du théorème 5.3.6 que $h_0(C_E) = [E : F]$ et $h_1(C_E) = 1$.

Supposons à présent que $[E : F]$ est composé et soit p un diviseur premier de $[E : F]$. Soit $F \subset K \subset E$ l'unique sous-extension telle que $[E : K] = p$. Fixons également γ un générateur du groupe $\mathrm{Gal}(E/F)$. Le morphisme $N_{K/F}$:

$\mathbb{A}_K^\times \to \mathbb{A}_F^\times$ induit un morphisme de groupes $N_{K/F} : C_K \to C_F$. On a de plus $N_{K/F}(N_{E/K}(C_E)) = N_{E/F}(C_E)$ de sorte que l'on a un morphisme surjectif de groupes

$$N_{K/F} : C_K/N_{E/K}(C_E) \twoheadrightarrow N_{K/F}(C_K)/N_{E/F}(C_E).$$

Montrons que ce morphisme est en fait un isomorphisme. Soit $x \in C_K$ tel que $N_{K/F}(x) \in N_{E/F}(C_E)$. Il existe donc $y \in C_E$ tel que $N_{K/F}(x) = N_{E/F}(y)$, c'est-à-dire $N_{K/F}(xN_{E/K}(y)^{-1}) = 1$. Comme $[K : F] = [E : F]/p < [E : F]$, par récurrence on a $\widehat{H}^1(C_K) = \{0\}$ (où C_K est vu comme $\mathrm{Gal}(K/F)$-module), ce qui implique qu'il existe $z \in C_E$ tel que $xN_{E/K}(y)^{-1} = z\gamma(z)^{-1}$. Le lemme 5.5.14 implique que γ agit trivialement sur $C_K/N_{E/K}(C_E)$, c'est-à-dire qu'il existe $u \in C_E$ tel que $z\gamma(z)^{-1} = N_{E/K}(u)$. On a alors $x = N_{E/K}(yu)$. On a donc un isomorphisme de groupes $C_K/N_{E/K}(C_E) \simeq N_{K/F}(C_K)/N_{E/F}(C_E)$. Ainsi

$$\begin{aligned} h_0(C_F) = [C_F : N_{E/F}(C_E)] &= [C_F : N_{K/F}(C_K)][N_{K/F}(C_K) : N_{E/F}(C_E)] \\ &= [C_F : N_{K/F}(C_K)][C_K : N_{E/K}(C_E)]. \end{aligned}$$

Par récurrence, on a bien $[C_F : N_{K/F}(C_K)] = [K : F]$ et $[C_K : N_{E/K}(C_E)] = [E : K]$, ce qui implique $h_0(C_E) = [E : F]$.

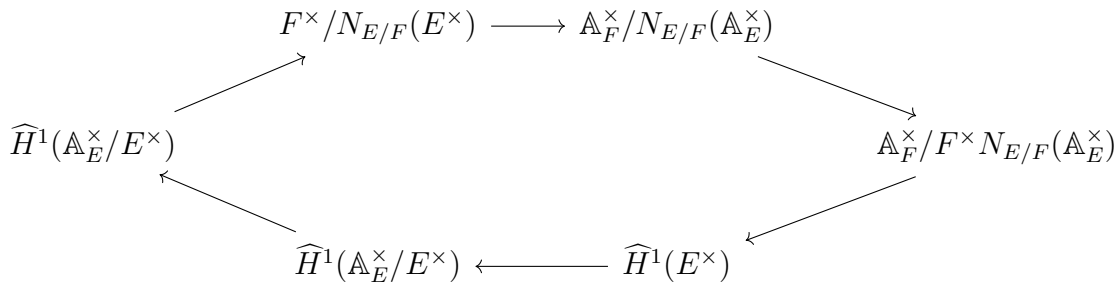
Prouvons à présent que $h_1(C_E) = 1$. Posons $m = [E : F]/p$ et notons $\alpha : C_E \to C_E$ l'application $x \mapsto \prod_{i=0}^{m-1} \gamma^i(x)$. On a $\mathrm{Gal}(E/K) = \langle \gamma^m \rangle$ de sorte que si $x \in C_E$, $N_{E/K}(x) = \prod_{i=0}^{p} \gamma^{mi}(x)$. On en déduit que $N_{E/K} \circ \alpha = N_{E/F}$ et donc que $\alpha(\mathrm{Ker}(N_{E/F})) \subset \mathrm{Ker}(N_{E/K})$. Par récurrence, on a $\widehat{H}^1(C_E) = \{0\}$ (où C_E est vu comme $\mathrm{Gal}(E/K)$-module). Ce qui implique que $\mathrm{Ker}(N_{E/K}) = \{z\gamma^m(z)^{-1} \mid z \in C_E\}$. Si $x \in \mathrm{Ker}(N_{E/F})$, il existe donc $y \in C_E$ tel que $\alpha(x) = y\gamma^m(y)^{-1}$. Par ailleurs, on a $\alpha(y\gamma(y)^{-1}) = y\gamma^m(y)^{-1}$ de sorte que $\alpha(x\gamma(y)y^{-1}) = 1$. Comme $\alpha(z)\gamma(\alpha(z))^{-1} = z\gamma^m(z)^{-1}$ pour tout $z \in C_E$, on a que $x\gamma(y)y^{-1}$ est un élément de $C_E^{\mathrm{Gal}(E/K)} = C_K$ (voir TD pour cette dernière égalité). Comme de plus $\alpha|_{C_K} = N_{K/F}$, on a $x\gamma(y)y^{-1} \in \mathrm{Ker}(N_{K/F})$. Par récurrence (encore), on a $\widehat{H}^1(C_K) = \{0\}$, ce qui implique l'existence de $z \in C_K$ tel que $x\gamma(y)y^{-1} = u\gamma(u)^{-1}$ et donc $x = yu\gamma(yu)^{-1}$. Ceci prouve que $\widehat{H}^1(C_E) = \{0\}$ (vu comme $\mathrm{Gal}(E/F)$-module) et achève la récurrence. □

Corollaire 5.5.16. *Soit E/F une extension cyclique de corps de nombres. Soit $x \in F$. Alors il existe $y \in E$ tel que $N_{E/F}(y) = x$ si et seulement si pour toute place v de F et toute place $w \mid v$ de E, il existe $y_w \in E_w$ tel que $N_{E_w/F_v}(y_w) = x$.*

Démonstration. On a une suite exacte de $\mathrm{Gal}(E/F)$-modules

$$0 \longrightarrow E^\times \longrightarrow \mathbb{A}_E^\times \longrightarrow \mathbb{A}_E^\times/E^\times \longrightarrow 0.$$

Dans la preuve de la proposition 5.4.2, on a démontré qu'il existe un hexagone exact



D'après le théorème 5.5.15, on a $\widehat{H}^1(\mathbb{A}_E^\times/E^\times) = \{0\}$, ce qui implique l'injectivité de $F^\times/N_{E/F}(E^\times) \to \mathbb{A}_F^\times/N_{E/F}(\mathbb{A}_E^\times)$, ce qui est exactement l'énoncé cherché (en remarquant que pour tout $w \mid v$ le groupe $N_{E_w/F_v}(E_w^\times) \subset F_v^\times$ ne dépend pas de w). □

Remarque 5.5.17. L'énoncé du corollaire 5.5.16 ne se généralise pas aux extensions abéliennes de corps de nombres quelconques.

On peut enfin donner une démonstration complète de la loi de réciprocité d'Artin.

Démonstration du théorème 5.2.1. Soit E/F une extension abélienne de corps de nombres. D'après la remarque 5.5.6, il suffit de prouver qu'il existe un module $\mathfrak{m}$ tel que la paire $(E/F, \mathfrak{m})$ est admissible. Le théorème de classification des groupes abéliens finis et la propriété 4) de la proposition 5.5.7 implique qu'il suffit de traiter le cas où E/F est une extension cyclique. Le théorème 5.5.15 implique alors que $[E : F] = \mathrm{Card}(\mathbb{A}_F^\times/F^\times N_{E/F}(\mathbb{A}_E^\times))$ et on conclut en utilisant le théorème 5.5.12. □

5.5.5 Quelques lemmes utiles

Lemme 5.5.18. *Soit E/F une extension finie de corps de nombres. Soit $M \geqslant 1$ un entier tel que, pour tout entier $n \geqslant 1$, $F \cap \mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_M)$ et $E \cap F(\zeta_n) \subset F(\zeta_M)$. Alors si $m \geqslant 1$ est un entier premier à M, on a $F \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ et $E \cap F(\zeta_m) = F$ et, si m_1 et m_2 sont deux entiers premiers entre eux et premiers à m, $F(\zeta_{m_1}) \cap F(\zeta_{m_2}) = F$.*

Démonstration. Soit $m \geqslant 1$ un entier premier à M. On a alors

$$F \cap \mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_M) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{m \wedge M}) = \mathbb{Q}.$$

Par ailleurs, on a $[F(\zeta_m) : F] = [\mathbb{Q}(\zeta_m) : F \cap \mathbb{Q}(\zeta_m)] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ et

$$\begin{aligned}[F(\zeta_m) : F(\zeta_m) \cap F(\zeta_M)] = [F(\zeta_{mM}) : F(\zeta_M)] &= \frac{[F(\zeta_{mM}) : F]}{[F(\zeta_M) : F]} \\ &= \frac{[\mathbb{Q}(\zeta_{mM}) : F \cap \mathbb{Q}(\zeta_{mM})]}{[\mathbb{Q}(\zeta_M) : F \cap \mathbb{Q}(\zeta_M)]} = \frac{[\mathbb{Q}(\zeta_{mM}) : F \cap \mathbb{Q}(\zeta_M)]}{[\mathbb{Q}(\zeta_M) : F \cap \mathbb{Q}(\zeta_M)]} \\ &= [\mathbb{Q}(\zeta_{mM}) : \mathbb{Q}(\zeta_M)] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_M) \cap \mathbb{Q}(\zeta_m)] \\ &= [\mathbb{Q}(\zeta_m) : \mathbb{Q}].\end{aligned}$$

On en déduit que $[F(\zeta_m) : F] = [F(\zeta_m) : F(\zeta_m) \cap F(\zeta_M)]$ et donc que $F(\zeta_m) \cap F(\zeta_M) = F$. (...) □

Lemme 5.5.19. *Soit E/F une extension cyclique de corps. Alors $\widehat{H}^1(E^\times) = \{0\}$.*

Démonstration. Voir TD. □

5.6 Le théorème d'existence

Soit F un corps de nombres. Si E/F est une extension finie abélienne, on note $N_E \coloneqq N_{E/F}(\mathbb{A}_E^\times)F^\times$. C'est un sous-groupe ouvert d'indice fini de $\mathbb{A}_F^\times$ (d'après la proposition 5.3.5). Un sous-groupe de $\mathbb{A}_F^\times$ est dit *normique* s'il est de la forme N_E pour E/F extension abélienne de F.

Le but de cette section est de démontrer le théorème 5.2.3.

5.6.1 Réductions

Lemme 5.6.1. *(i) Soit N un sous-groupe normique de $\mathbb{A}_F^\times$. Si N' est un sous-groupe de $\mathbb{A}_F^\times$ contenant N, alors N' est normique.*

(ii) Si N et N' sont deux sous-groupes normiques de $\mathbb{A}_F^\times$, il en est de même de $N \cap N'$.

Démonstration. Prouvons le point (i). Soit E/F une extension abélienne finie de F telle que $N = N_E$. Considérons l'isomorphisme de réciprocité d'Artin

$$\mathrm{Art}_{E/F} : \mathbb{A}_F^\times / N_E \xrightarrow{\sim} \mathrm{Gal}(E/F).$$

Soit $E' \subset E$ l'unique sous-extension de F telle que $\mathrm{Gal}(E/E') = \mathrm{Art}_{E/F}(N'/N_E)$. On a alors un diagramme commutatif

$$\begin{array}{ccc} \mathbb{A}_F^\times/N_E & \xrightarrow[\mathrm{Art}_{E/F}]{\sim} & \mathrm{Gal}(E/F) \\ \downarrow & & \downarrow \\ \mathbb{A}_F^\times/N_{E'} & \xrightarrow[\mathrm{Art}_{E'/F}]{\sim} & \mathrm{Gal}(E'/F). \end{array}$$

qui identifie N'/N_E et $N_{E'}/N_E$ de sorte que $N' = N_{E'}$.

Prouvons à présent le point (ii). Soient E et E' deux extensions abéliennes de F telles que $N_E = N$ et $N_{E'} = N'$. Posons $E'' = EE'$. C'est une extension abélienne de F. De plus, on a $\mathrm{Gal}(E''/F) \hookrightarrow \mathrm{Gal}(E/F) \times \mathrm{Gal}(E'/F)$ de sorte que $N_{E''}$, qui est le noyau de l'application $\mathrm{Art}_{E''/F}$ est aussi le noyau de l'application $(\mathrm{Art}_{E/F}, \mathrm{Art}_{E'/F})$ qui est $N \cap N'$. On a donc $N_{E''} = N \cap N'$. □

Lemme 5.6.2. *Soit K/F une extension cyclique. Soit N un sous-groupe d'indice fini de $\mathbb{A}_F^\times$ contenant $F^\times$ et tel que $N_{K/F}^{-1}(N) \subset \mathbb{A}_K^\times$ est normique. Alors N est normique.*

Démonstration. Posons $N' = N_{K/F}^{-1}(N)$. On a donc $N' = N_L$ pour une extension abélienne finie L/K. Soit $\widetilde{L}$ une clôture galoisienne de L/F. Soit σ un générateur du groupe cyclique $\mathrm{Gal}(K/F)$ et soit $\tilde{\sigma}$ un endomorphisme de $\widetilde{L}$ prolongeant σ. Remarquons que $\sigma(N') = N'$ et donc $\tilde{\sigma}(L) = L$. Comme $\mathrm{Gal}(K/F)$ est cyclique, on en conclut que L/F est galoisienne. On a alors un diagramme commutatif (remarque 5.2.2) :

$$\begin{array}{ccc} \mathbb{A}_K^\times/N' & \xrightarrow[\mathrm{Art}_{L/K}]{\sim} & \mathrm{Gal}(L/K) \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \tilde{\sigma}\cdot\tilde{\sigma}^{-1}} \\ \mathbb{A}_K^\times/N' & \xrightarrow[\mathrm{Art}_{L/K}]{\sim} & \mathrm{Gal}(L/K). \end{array}$$

Soit $x \in \mathbb{A}_K^\times$. On a alors $N_{K/F}(\sigma(x)) = N_{K/F}(x)$. En particulier $\sigma(x)x^{-1} \in N'$ et donc σ agit trivialement sur le quotient $\mathbb{A}_K^\times$. On en conclut que la conjugaison par σ est triviale sur $\mathrm{Gal}(L/K)$. Comme σ engendre $\mathrm{Gal}(K/F)$, on en conclut que $\mathrm{Gal}(L/F)$ est abélien. Comme $N_{L/K}(\mathbb{A}_L^\times) \subset N'$, on a $N_{L/F}(\mathbb{A}_L^\times) \subset N$ et donc $N_L = F^\times N_{L/F}(\mathbb{A}_L^\times) \subset N$. On déduit donc du lemme 5.6.1 que N est normique. □

Nous allons prouver un peu plus loin le résultat suivant.

Théorème 5.6.3. *Soit p un nombre premier. Supposons que $F^\times$ contient un élément d'ordre p. Alors, tout sous-groupe ouvert de $\mathbb{A}_F^\times$ contenant $F^\times$ et d'indice p est normique.*

Lemme 5.6.4. *Le théorème 5.6.3 implique le théorème 5.2.3.*

Démonstration. Soit $N \subset \mathbb{A}_F^\times$ un sous-groupe ouvert contenant $F^\times$ et d'indice fini. On va démontrer le résultat par récurrence sur $[\mathbb{A}_F^\times : N]$. Le cas $[\mathbb{A}_F^\times : N] = 1$ est trivial.

Fixons p un diviseur premier de $[\mathbb{A}_F^\times : N]$. Posons $K = F(\zeta_p)$. L'extension K/F est cyclique car $\mathrm{Gal}(K/F) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. Posons $N' = N_{K/F}^{-1}(N)$. Alors N' est un sous-groupe ouvert d'indice fini de $\mathbb{A}_K^\times$ contenant $K^\times$. Si $[\mathbb{A}_K^\times : N'] < [\mathbb{A}_F^\times : N]$, alors le sous-groupe N' est normique par récurrence et N est normique par le lemme 5.6.2. Supposons donc que $[\mathbb{A}_K^\times : N'] = [\mathbb{A}_F^\times : N]$. Soit $N'' \subset \mathbb{A}_K^\times$ un sous-groupe contenant N' et d'indice p. D'après le théorème 5.6.3, le sous-groupe N'' est normique. Soit L/K une extension abélienne telle que $N_L = N'' \subset \mathbb{A}_K^\times$. L'extension L/K est alors cyclique de degré p. Posons $N''' = N_{L/K}^{-1}(N')$. Comme $N_{L/K}^{-1}(N'') = \mathbb{A}_L^\times$, il s'agit d'un sous-groupe ouvert contenant $L^\times$ est d'indice $< [\mathbb{A}_F^\times : N]$ dans $\mathbb{A}_L^\times$. Par récurrence N''' est normique. Ainsi le lemme 5.6.2 implique que N' est normique, puis que N est normique. □

5.6.2 Théorie de Kummer

Soit $n \geqslant 1$. On suppose dans cette section que F contient toutes le sous-groupe des racines n-ièmes de l'unité, c'est-à-dire que $F^\times$ contient un élément d'ordre n. Soit K/F une extension galoisienne finie. Posons $G = \mathrm{Gal}(K/F)$. On considère la suite exacte suivante de G-modules

$$0 \longrightarrow \mu_n \longrightarrow K^\times \xrightarrow{x \mapsto x^n} (K^\times)^n \longrightarrow 0.$$

On vérifie facilement qu'en lui appliquant le foncteur des G-invariants, on a une suite exacte de groupes abéliens

$$0 \longrightarrow \mu_n \longrightarrow F^\times \xrightarrow{x \mapsto x^n} (K^\times)^n \cap F^\times.$$

Cependant la flèche la plus à droite n'est pas toujours surjective. Décrivons son conyau. Soit $x \in (K^\times)^n \cap F^\times$. Il existe alors $y \in K^\times$ tel que $x = y^n$. Pour $g \in G$, posons $\alpha_x(g) \coloneqq \frac{g(y)}{y} \in \mu_n$. On vérifie facilement que α_x est un morphismes de groupes $G \to \mu_n$. En effet, pour $g, h \in G$, on a

$$\frac{g(h(x))}{x} = \frac{g(h(x))}{h(x)} \frac{h(x)}{x} = \frac{g(x\alpha_x(h))}{x\alpha_x(h)} \frac{h(x)}{x} = \frac{g(x)}{x} \frac{h(x)}{x}$$

car $g(\alpha_x(h)) = \alpha_x(h)$ puisque $\mu_n \subset F^\times$. Le nombre $\alpha_x(g)$ ne dépend pas du choix de y. En effet si y' est un autre élément de $K^\times$ tel que $(y')^n = x$, alors $y' = \zeta y$

avec $\zeta \in \mu_n$, et on a $\frac{g(y)}{y} = \frac{g(y')}{y'}$. Enfin si $x, x' \in (K^\times)^n \cap F^\times$ et $y, y' \in K^\times$ vérifient $x = y^n$, $x' = (y'^n)$, on a, pour tout $g \in G$,

$$\alpha_{xx'}(g) = \frac{g(yy')}{yy'} = \alpha_x(g)\alpha_{x'}(g).$$

Ainsi $x \mapsto \alpha_x$ définit un morphisme de groupes de $F^\times$ dans le groupe $\mathrm{Hom}(G, \mu_n)$ des morphismes de G dans μ_n.

Lemme 5.6.5. *Le morphisme $x \mapsto \alpha_x$ induit un isomorphisme de groupes*

$$((K^\times)^n \cap F^\times)/(F^\times)^n \xrightarrow{\mathrm{Hom}} (G, \mu_n).$$

Démonstration. L'injectivité est clair car si $\alpha_x(g) = 1$ pour tout $g \in G$, alors $x = y^n$ avec $g(y) = y$ pour tout $g \in \mathrm{Gal}(K/F)$, c'est-à-dire $y \in F^\times$ et $x \in (F^\times)^n$.

Prouvons la surjectivité. Soit $\alpha : G \to \mu_n$ un morphisme de groupes. La famille $(x \mapsto g(x))_{g \in G}$ est une famille de caractères du groupes $K^\times$ (à valeurs dans $K^\times$). Le lemme d'indépendance des caractères implique que cette famille est une famille libre du K-espace vectoriel des applications de $K^\times$ dans K. Comme $\alpha(g) \neq 0$ pour tout $g \in G$, on en déduit que l'application $x \mapsto \sum_{g \in G} \alpha(g^{-1})g(x)$ de $K^\times$ dans K est non nulle et qu'il existe donc $z \in K^\times$ tel que

$$y \coloneqq \sum_{g \in G} \alpha(g^{-1})g(z) \neq 0.$$

On a alors, pour $h \in G$, en utilisant le fait que $\mu_n \subset F$,

$$h(y) = \sum_{g \in G} \alpha(g^{-1})hg(z) = \sum_{g \in G} \alpha(g^{-1}h)g(z) = \alpha(h)y.$$

On en déduit en particulier que $h(y^n) = y^n$ pour tout $h \in G$ et donc que $y^n \in (K^\times)^n \cap F^\times$ ainsi que $\alpha_{y^n} = \alpha$. □

On déduit du lemme 5.6.5 que l'on a une suite exacte longue

$$0 \longrightarrow \mu_n \longrightarrow F^\times \xrightarrow{x \mapsto x^n} (K^\times)^n \cap F^\times \xrightarrow{x \mapsto \alpha_x} \mathrm{Hom}(G, \mu_n) \longrightarrow 0.$$

On suppose désormais que G est un groupe abélien d'exposant n, c'est-à-dire que pour tout $g \in G$, $g^n = 1$. Dans ce cas, la théorie des caractères d'un groupe abélien fini implique que les groupes G et $\mathrm{Hom}(G, \mu_n)$ ont le même cardinal. En particulier on déduit du lemme 5.6.5 que

$$\mathrm{Card}(G) = [K : F] = \mathrm{Card}((K^\times)^n \cap F^\times/(F^\times)^n).$$

Soit $\beta : G \to \mathrm{Hom}((K^\times)^n \cap F^\times/(F^\times)^n, \mu_n)$ définit par $g \mapsto (x \mapsto \alpha_x(g))$. Il s'agit d'un morphisme de groupes. Remarquons que si $g \in G \smallsetminus \{1\}$, il existe un caractère χ du groupe G (à valeurs dans μ_n) tel que $\chi(g) \neq 1$. Soit $x \in (K^\times)^n \cap F^\times$ tel que $\chi = \alpha_x$, on a alors $\alpha_x(g) \neq 1$, ce qui prouve que $\beta(g) \neq 1$. Le morphisme β est donc injectif et bijectif par un argument de cardinal. On en déduit le résultat suivant :

Théorème 5.6.6. *Soit $\overline{F}$ une clôture algébrique de F. Il existe une bijection croissante de l'ensemble des extensions abéliennes $K \subset \overline{F}$ de F d'exposant n et l'ensemble des sous-groupes $H \subset F^\times$ d'indice fini contenant $(F^\times)^n$ donnée par $K \mapsto (K^\times)^n \cap F^\times$. La bijection réciproque est donnée par $H \mapsto F(\sqrt[n]{H})$. De plus on a l'égalité*

$$[F(\sqrt[n]{H}) : F] = \mathrm{Card}(H/(F^\times)^n).$$

5.6.3 Démonstration du théorème 5.6.3

Soit p un nombre premier. On suppose que F est un corps de nombres contenant toutes les racines p-ièmes de l'unité. On fixe $N \subset \mathbb{A}_F^\times$ un sous-groupe ouvert d'indice p contenant $F^\times$. Remarquons que, comme N est d'indice p, on a $(F_v^\times)^p \subset N$ pour toute place v de F. Soit S un ensemble fini de places de F tels que

— l'ensemble S contient toutes les places archimédiennes ;

— l'ensemble S contient toutes les places de F divisant p ;

— l'ensemble des places ultramétriques v de F telles que $U_v \not\subset N$;

— on a $\mathbb{A}_F^\times = F^\times \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v$.

Comme N est un sous-groupe ouvert de $\mathbb{A}_F^\times$, l'ensemble des places archimédiennes de F telles que $U_v \not\subset N$ est fini et on peut bien choisir un tel S. On pose alors

$$N_S \coloneqq F^\times \prod_{v\in S} (F_v^\times)^p \prod_{v\notin S} U_v$$

et on remarque que N_S est un sous-groupe ouvert de $\mathbb{A}_F^\times$, contenant $F^\times$ et tel que $N_S \subset N$. Pour démontrer le théorème 5.6.3, il suffit donc de prouver que N_S est normique (d'après le lemme 5.6.1).

Posons $\mathcal{O}_S^\times \coloneqq F^\times \cap \prod_{v\notin S} U_v$. Il s'agit d'un sous-groupe de $F^\times$ appelé sous-groupes des « S-unités ». Nous allons prouver que $N_S = N_{F(\sqrt[p]{\mathcal{O}_S^\times})}$. Remarquons que, puisque $\mu_p \subset F$, l'extension $F(\sqrt[p]{\mathcal{O}_S^\times})/F$ est galoisienne et même abélienne d'exposant p. On pose désormais $K \coloneqq F(\sqrt[p]{\mathcal{O}_S^\times})$.

Lemme 5.6.7. *Si $v \notin S$, l'extension K/F est non ramifiée en v.*

Démonstration. Soit $v \notin S$. Il suffit de prouver que pour $\alpha \in \mathcal{O}_S^\times$, l'extension $F(\sqrt[p]{\alpha})/F$ est non ramifiée en v. Posons $E = F(\sqrt[p]{\alpha})$. Soit w une place de E divisant v. Alors (théorème 2.3.9), le complété E_w de E en w est un quotient de $E \otimes_F F_v$, on a donc $E_w = F_v(\sqrt[p]{\alpha})$. Le polynôme minimal de $\sqrt[p]{\alpha}$ sur F_v est un diviseur Q de $X^p - \alpha$. Comme $\alpha \in U_v$, l'image $\overline{\alpha}$ de α dans le corps résiduel k_v est non nulle. Comme de plus v ne divise pas p, p est inversible dans k_v, ce qui implique que le polynôme $X^p - \overline{\alpha}$ est séparable dans $k_v[X]$. Ainsi l'image de Q dans $k_v[X]$ est également séparable. On déduit alors du lemme de Hensel 2.2.17 que toute racine de Q dans k_w se relève de façon unique en une racine de Q dans la sous-extension maximale non ramifiée de E_w/F_v, ce qui prouve que E_w/F_v est non ramifiée. □

Corollaire 5.6.8. *On a $N_S \subset N_K$.*

Démonstration. On a clairement $F^\times \subset N_K$. Comme de plus K/F est d'exposant p, le théorème 5.2.1 implique que $\mathbb{A}_F^\times/N_K$ est d'exposant p et donc que $(F_v^\times)^p \subset N_K$ pour tout v. On déduit alors du lemme 5.6.7 et de la proposition 5.1.1 que $U_v \subset N_K$ pour tout $v \notin S$ de sorte que $N_S \subset N_K$. □

Le corollaire 5.6.8 implique donc qu'il suffit de prouver l'égalité $[\mathbb{A}_F^\times : N_S] = [\mathbb{A}_F^\times : N_K]$ pour conclure. Calculons dans un premier temps $[\mathbb{A}_F^\times : N_K]$. On a, en utilisant le théorème 5.2.1, l'égalité $K = F(\sqrt[p]{(F^\times)^p \mathcal{O}_S^\times})$ et le lemme 5.6.5,

$$[\mathbb{A}_F^\times : N_K] = [K : F] = [\mathcal{O}_S^\times (F^\times)^p : (F^\times)^p] = [\mathcal{O}_S^\times : \mathcal{O}_S^\times \cap (F^\times)^p] = [\mathcal{O}_S^\times : (\mathcal{O}_S^\times)^p].$$

La dernière inégalité provient de $\mathcal{O}_S^\times \cap (F^\times)^p = (\mathcal{O}_S^\times)^p$ qui revient à dire que si $x = y^p \in \mathcal{O}_S^\times$ est une puissance p-ième, alors y est une unité en toute place $v \notin S$.

On prouve le résultat suivant, qui généralise le théorème 3.2.14.

Lemme 5.6.9. *On a un isomorphisme de groupes abéliens*

$$\mathcal{O}_S^\times \simeq \mu_F \times \mathbb{Z}^{\operatorname{Card} S - 1}.$$

Démonstration. Considérons le morphisme de groupes $L_S : \mathcal{O}_S^\times \to \mathbb{Z}^{\operatorname{Card}(S \smallsetminus \Sigma_\infty)}$ défini par $L_S(x) = (v_\mathfrak{p}(x))_{\mathfrak{p} \in S \smallsetminus \Sigma_\infty}$. Son noyau est le sous-groupe $\mathcal{O}_F^\times$ qui est un groupe abélien de type fini de rang $\operatorname{Card}(\Sigma_\infty) - 1$ d'après le théorème 3.2.14. Il suffit donc de prouver que l'image de L_S est un groupe abélien libre de rang $\operatorname{Card}(S \smallsetminus \Sigma_\infty)$ ou, de façon équivalente, que L_S est de conoyau fini. Rappelons que le groupe quotient $(\mathbb{A}_F^\times)^1/F^\times$ est compact (théorème 3.2.4). L'image du sous-groupe

$$(\prod_{v \in S} F_v^\times \prod_{v \notin S} U_v)^1 \coloneqq (\prod_{v \in S} F_v^\times \prod_{v \notin S} U_v) \cap (\mathbb{A}_F^\times)^1$$

dans $(\mathbb{A}_F^\times)^1/F^\times$ est donc compacte (car ouverte par le lemme B.3.4 et donc fermée par le lemme B.3.3). Cette image est homéomorphe au quotient $(\prod_{v\in S} F_v^\times \prod_{v\notin S} U_v)^1/\mathcal{O}_S^\times$. Le morphisme de groupes continu L_S induit donc un morphisme continu surjectif

$$L_S : (\prod_{v\in S} F_v^\times \prod_{v\notin S} U_v)^1/\mathcal{O}_S^\times \twoheadrightarrow \mathbb{Z}^{\mathrm{Card}(S\smallsetminus\Sigma_\infty)}/L_S(\mathcal{O}_S^\times).$$

Le terme de droite est donc un quotient discret d'un groupe compact et est donc fini. □

Corollaire 5.6.10. *On a* $[\mathbb{A}_F^\times : N_K] = p^{\mathrm{Card}(S)}$.

Démonstration. On déduit du lemme 5.6.9 que

$$\mathcal{O}_S^\times/(\mathcal{O}_S^\times)^p \simeq \mu_F/\mu_F^p \times (\mathbb{Z}/p\mathbb{Z})^{\mathrm{Card}(S)-1}.$$

Comme μ_F est un groupe cyclique de cardinal divisible par p, on en déduit le résultat. □

On calcule enfin $[\mathbb{A}_F^\times : N_S]$. Notre choix de S implique que

$$\mathbb{A}_F^\times = F^\times \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v.$$

On a donc des isomorphismes de groupes finis

$$\mathbb{A}_F^\times/N_S \simeq \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v/(F^\times \prod_{v\in S} (F_v^\times)^p \prod_{v\notin S} U_v \cap \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v).$$

Or

$$F^\times \prod_{v\in S} (F_v^\times)^p \prod_{v\notin S} U_v \cap \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v = \mathcal{O}_S^\times \prod_{v\in S} (F_v^\times)^p \prod_{v\notin S} U_v.$$

Ainsi

$$[\mathbb{A}_F^\times : N_S] = \left[\prod_{v\in S} F_v^\times \prod_{v\notin S} U_v : \prod_{v\in S} (F_v^\times)^p \prod_{v\notin S} U_v\right] \left[\mathcal{O}_S^\times \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v : \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v\right]^{-1}$$

(à condition que ces deux indices soient finis).

Lemme 5.6.11. *Pour toute place v de F, on a* $[F_v^\times : (F_v^\times)^p] = p^2|p|_v^{-1}$.

Démonstration. Commençons par le cas où v est ultramétrique. Rappelons que, au cours de la preuve du lemme 5.4.9, on a prouvé que

$$q_{0,p}(U_v) = \begin{cases} p^{[F_v:\mathbb{Q}_p]} & \text{si } v \mid p \\ 1 & \text{sinon} \end{cases}$$

c'est-à-dire $q_{0,p}(U_v) = |p|_v^{-1}$. Par ailleurs on vérifie facilement que $q_{0,p}(\mathbb{Z}) = p$. L'isomorphisme $F_v^\times \simeq \mathbb{Z} \times U_v$ (voir la discussion suviant l'exemple 2.2.18) et la proposition 5.4.2 impliquent que $q_{0,p}(F_v^\times) = p|p|_v^{-1}$. Rappelons que $\mu_p \subset F_v^\times$ et que μ_p est exactement le sous-groupe des éléments de p-torsion de $F_v^\times$. En revenant à la définition de $q_{0,p}(F_v^\times)$, on obtient que $[F_v^\times : (F_v^\times)^p] = p^2|p|_v^{-1}$.

Supposons à présent que v est archimédienne. Remarquons que si $p > 2$, puisque $\mu_p \subset F_v^\times$, on doit avoir $F_v = \mathbb{C}$. Dans ce cas $[\mathbb{C}^\times : (\mathbb{C}^\times)^p] = 1 = p^2|p|_{\mathbb{C}}^{-1}$. Si $p = 2$ et $F_v \simeq \mathbb{R}$, on a bien $[\mathbb{R}^\times : (\mathbb{R}^\times)^2] = 2 = p^2|p|_{\mathbb{R}}^{-1}$. □

Lemme 5.6.12. *On a* $\mathcal{O}_S^\times \cap \prod_{v\in S}(F_v^\times)^p = (\mathcal{O}_S^\times)^p$.

Démonstration. Une inclusion est triviale, prouvons l'autre. Soit $\alpha \in \mathcal{O}_S^\times \cap \prod_{v\in S}(F_v^\times)^p$. Posons $E = F(\sqrt[p]{\alpha})$. Le lemme 5.6.7 implique que l'extension E/F est non ramifiée en toute place $v \notin S$. Par ailleurs si $v \in S$ et si $w \mid v$, alors $\alpha \in (F_v^\times)^p$ de sorte que $E_w = F_v$ et $F_v^\times \subset N_E$. On a donc $\prod_{v\in S} F_v^\times \prod_{v\notin S} U_v \subset N_E$ et donc $N_E = \mathbb{A}_F^\times$. On en conclut que $E = F$ et donc que $\alpha \in (F^\times)^p$. Ainsi $\alpha \in (\mathcal{O}_S^\times)^p$. □

Corollaire 5.6.13. *On a* $[\mathbb{A}_F^\times : N_S] = p^{\mathrm{Card}(S)}$.

Démonstration. On déduit du lemme 5.6.11 et de la formule du produit (théorème 2.3.12) que

$$\prod_{v\in S} F_v^\times \prod_{v\notin S} U_v / \prod_{v\in S}(F_v^\times)^p \prod_{v\notin S} U_v \simeq \prod_{v\in S} F_v^\times/(F_v^\times)^p$$

est un groupe fini de cardinal $p^{2\,\mathrm{Card}(S)}$. On déduit des lemmes 5.6.12 et 5.6.9 que le groupe

$$\mathcal{O}_S^\times \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v / \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v \simeq \mathcal{O}_S^\times/(\mathcal{O}_S^\times \cap \prod_{v\in S} F_v^\times \prod_{v\notin S} U_v) \simeq \mathcal{O}_S^\times/(\mathcal{O}_S^\times)^p$$

est un groupe fini de cardinal $p^{\mathrm{Card}(S)}$. On en déduit le résultat. □

Les corollaires 5.6.8, 5.6.10 et 5.6.13 impliquent bien que $N_S = N_K$, ce qui achève la démonstration du théorème 5.6.3.

5.7 Compléments

5.7.1 Le théorème de densité de Tchebotarev

Théorème 5.7.1. *Soit E/F une extension galoisienne finie de corps de nombres. Soit C une classe de conjugaison de* $\mathrm{Gal}(E/F)$. *Notons $\mathcal{P}_C$ l'ensemble des idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_F$ qui sont non ramifiés dans E/F et tels que $(\mathfrak{p}, E/F) \in C$. Alors $\mathcal{P}_C$ a une densité de Dirichlet égale à* $\frac{\mathrm{Card}(C)}{[E:F]}$.

Remarque 5.7.2. Noter que l'extension E/F n'est pas supposée abélienne. La notation $(\mathfrak{p}, E/F)$ n'a donc aucun sens. Si $\mathfrak{q}$ divise $\mathfrak{p}$, l'élément de Frobenius $(\mathfrak{q}, E/F))$ ne dépend uniquement de $\mathfrak{p}$ mais aussi du choix de $\mathfrak{q}$. Cependant on déduit de la proposition 1.2.15 que sa classe de conjugaison ne dépend que de $\mathfrak{p}$. Ainsi la notation $(\mathfrak{p}, E/F) \in C$ signifie « pour un (de façon équivalente, pour tout) idéal maximal $\mathfrak{q}$ de $\mathcal{O}_E$ divisant $\mathfrak{p}$, on a $(\mathfrak{q}, E/F) \in C$ ».

Démonstration. Commençons par démontrer le cas où l'extension E/F est cyclique. Soit σ un générateur de $\mathrm{Gal}(E/F)$ et considérons la classe de conjugaison $C = \{\sigma\}$ réduite à σ. Notons H le groupe fini $\mathbb{A}_F^\times / F^\times N_{E/F}(\mathbb{A}_E^\times)$. Soit $x_0 \in H$ l'unique élément tel que $\mathrm{Art}_{E/F}(x_0) = \sigma$. Si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_F$, notons $\varpi_\mathfrak{p}$ l'idèle $(x_v) \in \mathbb{A}_F^\times$ tel que $x_v = 1$ si $\mathfrak{p}_v \neq \mathfrak{p}$ et $x_v = \pi_\mathfrak{p}$ uniformisante si $\mathfrak{p}_v = \mathfrak{p}$. Si $\mathfrak{p}$ est non ramifié dans E/F, l'image de $\varpi_\mathfrak{p}$ dans H coïncide avec x_0 si et seulement si $(\mathfrak{p}, E/F) = \sigma$. De plus, puisque H est un groupe abélien fini de cardinal $[E : F]$, on a

$$\frac{1}{[E:F]} \sum_{\chi \in \widehat{H}} \chi(x_0)^{-1} \chi(\varpi_\mathfrak{p}) = \begin{cases} 1 & \text{si } \varpi_\mathfrak{p} \equiv x_0 \\ 0 & \text{sinon.} \end{cases}$$

Par ailleurs, on a montré au cours de la démonstration du théorème 5.3.6 que $\log(L(\chi, s)) \sim_{s \to 1} \log\left(\frac{1}{s-1}\right)$ si χ est le caractère trivial de H et que $L(\chi, 1) \neq 0$ sinon. On en déduit que

$$\sum_{\mathfrak{p} \in \mathcal{P}_C} N(\mathfrak{p})^{-s} = \frac{1}{[E:F]} \sum_{\chi \in \widehat{H}} \log(L(\chi, s)) \sim_{s \to 1} \frac{1}{[E:F]} \log\left(\frac{1}{s-1}\right).$$

On en déduit que $\mathcal{P}_C$ possède une densité de Dirichlet égale à $[E : F]^{-1}$.

Considérons à présent le cas général. Soit C une classe de conjugaison de $\mathrm{Gal}(E/F)$. Posons $H \subset \mathrm{Gal}(E/F)$ le sous-groupe engendré par σ et $K = E^H$. Notons $\mathcal{P}_\sigma$ l'ensemble des idéaux maximaux de $\mathcal{O}_E$ non ramifiés dans E/F tels que $(\mathfrak{q}, E/F) = \sigma$. Notons $\mathcal{P}'_\sigma$ l'ensemble des idéaux maximaux $\mathfrak{r}$ de $\mathcal{O}_K$ qui sont non ramifiés dans E/K et tels que $(\mathfrak{r}, E/K) = \sigma$ (remarqons que E/K est cyclique donc abélienne). Et enfin notons $\mathcal{P}'$ l'ensemble des idéaux maximaux $\mathfrak{r}$ de $\mathcal{O}_K$ tels que $N_{K/F}(\mathfrak{r})$ est un idéal maximal de $\mathcal{O}_F$ (c'est-à-dire $f_{\mathfrak{r}/\mathfrak{r} \cap \mathcal{O}_F} = e_{\mathfrak{r}/\mathfrak{r} \cap \mathcal{O}_F} = 1$). Montrons que l'application $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}_K$ induit une bijection de $\mathcal{P}_\sigma$ sur $\mathcal{P}'_\sigma \cap \mathcal{P}'$. Soit $\mathfrak{q} \in \mathcal{P}_\sigma$. Posons $\mathfrak{r} \coloneqq \mathfrak{q} \cap \mathcal{O}_K$ et $\mathfrak{p} \coloneqq \mathfrak{q} \cap \mathcal{O}_F$. Par définition le groupe de décomposition $D_{\mathfrak{q}/\mathfrak{p}}$ est le sous-groupe H engendré par σ. De plus $D_{\mathfrak{q}/\mathfrak{r}} = D_{\mathfrak{q}/\mathfrak{p}} \cap H = H = D_{\mathfrak{q}/\mathfrak{p}}$. On en conclut que $f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{r}}$ et que $f_{\mathfrak{r}/\mathfrak{p}} = 1$. Ainsi $N_{K/F}(\mathfrak{r}) = \mathfrak{p}$ et $(\mathfrak{q}, E/F) = (\mathfrak{q}, E/K) = (\mathfrak{r}, E/K) = \sigma$, donc $\mathfrak{r} \in \mathcal{P}'_\sigma \cap \mathcal{P}'$. Réciproquement soit $\mathfrak{r} \in \mathcal{P}'_\sigma \cap \mathcal{P}'$. Posons $\mathfrak{p} = \mathfrak{r} \cap \mathcal{O}_F = N_{K/F}(\mathfrak{r})$. Soit $\mathfrak{q}$ un idéal maximal de $\mathcal{O}_E$ divisant $\mathfrak{r}$. On a alors $f_{\mathfrak{r}/\mathfrak{p}} = 1$ et donc $(\mathfrak{q}, E/F) = (\mathfrak{q}, E/K) = \sigma$. En particulier

$f_{\mathfrak{q}/\mathfrak{r}} = [E : K]$ et $\mathfrak{q}$ est donc l'unique idéal maximal au-dessus de $\mathfrak{r}$. Ceci prouve la bijectivité de l'application.

On montre, comme dans la preuve du théorème 5.3.3 que

$$\sum_{\mathfrak{r}\in\mathcal{P}'} N(\mathfrak{r})^{-s} \sim_{s\to 1} \log\left(\frac{1}{s-1}\right)$$

de sorte que l'ensemble $\mathcal{P}'$ est un ensemble d'idéaux de densité 1. De plus, on déduit du cas cyclique que $\mathcal{P}'_\sigma$ est un ensemble de densité $[E : K]^{-1}$. Ainsi $\mathcal{P}'_\sigma \cap \mathcal{P}'$ est un ensemble de densité $[E : K]^{-1}$.

Déterminons le cardinal des fibres de l'application $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}_F$ de $\mathcal{P}_\sigma$ vers $\mathcal{P}_C$. On déduit de la proposition 1.2.15 que cette application est surjective. Soit $\mathfrak{q} \in \mathcal{P}_\sigma$. Soit $\mathfrak{q}'$ un autre élément de $\mathcal{P}_\sigma$ idéal maximal de $\mathcal{O}_E$ au-dessus de $\mathfrak{p}$. Il existe alors $g \in \mathrm{Gal}(E/F)$ tel que $\mathfrak{q}' = g(\mathfrak{q})$ et donc $(\mathfrak{q}', E/F) = g(\mathfrak{q}, E/F)g^{-1}$. On a donc $(\mathfrak{q}', E/F) = \sigma$ si et seulement si g appartient au commutant $C_{\mathrm{Gal}(E/F)}(\sigma)$ de σ dans $\mathrm{Gal}(E/F)$. De plus $\mathfrak{q}' = \mathfrak{q}$ si et seulement si $g \in D_{\mathfrak{q}/\mathfrak{p}} = \langle\sigma\rangle$. Les fibres sont donc exactement de cardinal $\frac{\mathrm{Card}(C_{\mathrm{Gal}(E/F)}(\sigma))}{\mathrm{Card}(\langle\sigma\rangle)}$.

On peut à présent conclure. Remarquons que $\mathrm{Card}(\langle\sigma\rangle) = [E : K]$. On a, pour $\mathrm{Re}(s) > 1$,

$$\begin{aligned}
\sum_{\mathfrak{p}\in\mathcal{P}_C} N(\mathfrak{p})^{-s} &= \frac{\mathrm{Card}(\langle\sigma\rangle)}{\mathrm{Card}(C_{\mathrm{Gal}(E/F)}(\sigma))} \sum_{\mathfrak{r}\in\mathcal{P}'_\sigma\cap\mathcal{P}'} N(\mathfrak{r})^{-s} \\
&= \frac{\mathrm{Card}(\langle\sigma\rangle)}{\mathrm{Card}(C_{\mathrm{Gal}(E/F)}(\sigma))}[E : K]^{-1} \log\left(\frac{1}{s-1}\right) + o\left(\log\left(\frac{1}{s-1}\right)\right) \\
&= \frac{1}{\mathrm{Card}(C_{\mathrm{Gal}(E/F)}(\sigma))} \log\left(\frac{1}{s-1}\right) + o\left(\log\left(\frac{1}{s-1}\right)\right)
\end{aligned}$$

Ainsi l'ensemble $\mathcal{P}_C$ est de densité $\mathrm{Card}(C_{\mathrm{Gal}(E/F)(\sigma)})^{-1} = \frac{\mathrm{Card}(C)}{[E:F]}$. □

Annexe A

Résultats d'algèbre commutative

A.1 Anneaux locaux

Définition A.1.1. *Un anneau est dit* local *s'il possède un unique idéal maximal.*

Si un anneau A est local d'idéal maximal $\mathfrak{m}$, on vérifie facilement que l'ensemble $A \smallsetminus \mathfrak{m}$ est exactement l'ensemble $A^\times$ des éléments inversibles de A. Inversement, si I est un idéal d'un anneau A tel que $A^\times = A \smallsetminus I$, alors I est maximal et est l'unique idéal maximal de A, ainsi A est un anneau local.

Si A est un anneau local d'idéal maximal $\mathfrak{m}$, l'anneau quotient $A/\mathfrak{m}$ est un corps appelé *corps résiduel* de A.

Si A est un anneau et si $\mathfrak{p}$ est un idéal premier de A, alors le localisé $A_\mathfrak{p}$ de A en $\mathfrak{p}$ (c'est-à-dire relativement à la partie multiplicative $A \smallsetminus \mathfrak{p}$) est un anneau local, son idéal maximal est $\mathfrak{p}A_\mathfrak{p}$.

Exercice A.1.1. Montrer que $\mathfrak{p}A_\mathfrak{p}$ est l'idéal maximal de $A_\mathfrak{p}$ et que le corps résiduel de $A_\mathfrak{p}$ est isomorphe au corps des fractions de l'anneau $A/\mathfrak{p}$.

Lemme A.1.2 (Lemme de Nakayama)**.** *Soit A un anneau local d'idéal maximal $\mathfrak{m}$ et soit M un A-module de type fini. On a $M = 0$ si et seulement si $M/\mathfrak{m}M = 0$.*

Démonstration. Supposons que $M = \mathfrak{m}M$. Soit $(e_1, \dots, e_n)$ une famille génératrice de M. Pour tout $1 \leqslant i \leqslant n$, il existe des éléments $a_{1,i}, \dots, a_{n,i} \in \mathfrak{m}$ tels que $e_i = \sum_{j=1}^n a_{i,j}e_j$. Posons $B = (a_{i,j})_{1\leqslant i,j\leqslant n} \in M_n(A)$. On a donc $(e_1, \dots, e_r)(I_n - B) = (0, \dots, 0)$. Comme les coefficients de B sont dans $\mathfrak{m}$, on a $\det(I_n - B) \in 1 + \mathfrak{m}$. Comme l'anneau A est local, $\det(I_n - B) \in A^\times$, c'est-à-dire $I_n - B \in \mathrm{GL}_n(A)$. On en déduit $(e_1, \dots, e_r) = (0, \dots, 0)$ et donc $M = 0$. □

A.2 Localisation

Lemme A.2.1. *Soit A un anneau. Soient $M \subset N$ deux A-modules. On suppose que $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ pour tout idéal maximal $\mathfrak{p}$ de A. Alors $M = N$.*

Démonstration. Comme la localisation est un foncteur exact, il suffit de montrer que si M est un A-module non nul, alors il existe un idéal maximal $\mathfrak{p}$ de A tel que $M_{\mathfrak{p}} \neq 0$. Soit donc $v \in M$ non nul et soit $\mathrm{Ann}(v)$ l'annulateur de v dans A. C'est un idéal non trivial. Le lemme de Krull implique qu'il existe $\mathfrak{p}$ idéal maximal contenant $\mathrm{Ann}(v)$. On a donc $(Av)_{\mathfrak{p}} \simeq (A/\mathrm{Ann}(v))_{\mathfrak{p}} \neq 0$ et donc $M_{\mathfrak{p}} \neq 0$. □

Lemme A.2.2. *Soit A un anneau et soit M un A-module de présentation fini (en particulier un A-module de type fini si A est noethérien). Alors M est un A-module projectif si et seulement si $M_{\mathfrak{p}}$ est un $A_{\mathfrak{p}}$-module projectif pour tout idéal maximal $\mathfrak{p}$ de A.*

Démonstration. Soit M un A-module. Le A-module M est projectif si et seulement si le foncteur $\mathrm{Hom}_A(M, -)$ de la catégorie des A-modules vers elle-même est exact. Si N est un A-module et $\mathfrak{p}$ un idéal maximal de A, on a un isomorphisme de $A_{\mathfrak{p}}$-modules $\mathrm{Hom}_A(M, N)_{\mathfrak{p}} \simeq \mathrm{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})$. On déduit alors le résultat du lemme A.2.1. □

Lemme A.2.3. *Soit A un anneau et soit $\mathfrak{p}$ un idéal maximal de A. Alors pour tout $n \geqslant 1$, le morphisme naturel $A/\mathfrak{p}^n \to A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^n$ est un isomorphisme.*

Démonstration. Prouvons l'injectivité. Si l'image de $x \in A$ dans $A_{\mathfrak{p}}$ appartient à $(\mathfrak{p}A_{\mathfrak{p}})^n = \mathfrak{p}^n A_{\mathfrak{p}}$, il existe $s \in A \setminus \mathfrak{p}$ tel que $sa \in \mathfrak{p}^n$. L'idéal $As + \mathfrak{p}$ contient strictement $\mathfrak{p}$, on a donc $As + \mathfrak{p} = A$. Ainsi on peut écrire $1 = st + u$ ave $t \in A$ et $u \in \mathfrak{p}$. On en conclut que $a = tsa + ua \in \mathfrak{p}^n$. Prouvons maintenant la surjectivité. Soit $x \in A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}$, soit $\tilde{x} \in A_{\mathfrak{p}}$ relevant x et soit $s \in A \setminus \mathfrak{p}$ tel que $s\tilde{x} \in A$. L'anneau $A/\mathfrak{p}^n$ est local d'idéal maximal l'image de $\mathfrak{p}$, de sorte que s est inversible dans $A/\mathfrak{p}^n$. Il existe donc $t \in A$ et $u \in \mathfrak{p}^n$ tels que $1 = st + u$. L'image de $ts\tilde{x}$ dans $A/\mathfrak{p}^n$ s'envoie donc sur x dans $A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}$. □

A.3 Entiers

Soit A un anneau et soit B une A-algèbre. On dit qu'un élément $x \in B$ est *entier sur A* s'il existe un polynôme $P \in A[X]$, unitaire, tel que $P(x) = 0$ dans B.

Théorème A.3.1. *Soit A un anneau et soit B une A-algèbre. Si $x \in B$, les assertions suivantes sont équivalentes :*

(i) l'élément x est entier sur A ;

(ii) la sous-A-algèbre $A[x]$ de B engendrée par x est un A-module de type fini ;

(iii) il existe une sous-A-algèbre $C \subset B$ telle que $x \in C$ et qui est un A-module de type fini.

Démonstration. Voir [Bou85, Ch. V §1 Thm.1]. □

Une A-algèbre est dite *entière* si tous ses éléments sont entiers sur A. On déduit du théorème A.3.1 qu'une A-algèbre qui est de plus un A-module de type fini est entière sur A.

Corollaire A.3.2. *Soit B une A-algèbre. L'ensemble des éléments de B qui sont entiers sur A forment une sous-A-algèbre de B.*

Proposition A.3.3. *Soit B un anneau intègre et soit A un sous-anneau de B tel que B est entier sur A. Si I est un idéal non nul de B, alors $I \cap A$ est un idéal premier non nul de A.*

Démonstration. Soit $x \in I \smallsetminus \{0\}$. Comme x est entier sur A, il existe $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in A[X]$ annulant x. Comme B est intègre, on peut choisir P de sorte que $a_0 \neq 0$. On a alors

$$a_0 = -(x^d + \cdots + a_x) \in I \cap A.$$ □

Proposition A.3.4. *Soit A est un anneau et soit B une A-algèbre entière. Soit $\mathfrak{p}$ un idéal premier de B et $\mathfrak{q}$ son image inverse dans A. Alors $\mathfrak{p}$ est maximal si et seulement si $\mathfrak{q}$ est maximal.*

Démonstration. En quotientant A par $\mathfrak{q}$ et B par $\mathfrak{p}$, on est ramené à prouver que si A est un sous-anneau d'un anneau intègre B qui est entier sur A. Alors B est un corps si et seulement si A est un corps

Supposons donc $A \subset B$ intègres avec B entier sur A. Si A est un corps et si $x \in B \smallsetminus \{0\}$, alors $A[x]$ est un A-algèbre finie et intègre, c'est donc un corps, et $x \in A[x]^\times \subset B^\times$. Ainsi B est un corps. Supposons réciproquement que B est un corps. Soit $x \in A \smallsetminus \{0\}$. Alors $x^{-1} \in B$ est entier sur A et donc il existe $a_1, \ldots, a_r \in A$ tels que $x^{-r} + a_1 x^{-r+1} + \cdots + a_r = 0$. En multipliant cette égalité par x^{r-1}, on obtient $x^{-1} \in A$. Ainsi A est un corps. □

Définition A.3.5. *Un anneau A est dit* intégralement clos *s'il est intègre et si tout élément de son corps des fractions qui est entier sur A est un élément de A.*

Définition A.3.6. *Soit A un anneau et soit B une A-algèbre. La* clôture intégrale *de A dans B est l'ensemble des éléments de B qui sont entiers sur A. D'après le corollaire A.3.2 c'est une sous-A-algèbre de B.*

A.4 Quelques résultats sur les idéaux

Lemme A.4.1. *Soit A un anneau. Soit $\mathfrak{p}$ un idéal premier de A. Si $\mathfrak{p}$ contient un produit d'idéaux $\mathfrak{p}_1 \cdots \mathfrak{p}_r$, alors il existe $1 \leqslant i \leqslant r$ tel que $\mathfrak{p}_i \subset \mathfrak{p}$.*

Démonstration. Supposons par l'absurde que pour tout $1 \leqslant i \leqslant r$, il existe $x_i \in \mathfrak{p}_i \smallsetminus \mathfrak{p}$. Comme $\mathfrak{p}$ est un idéal premier, on a $\prod_{i=1}^r x_i \notin \mathfrak{p}$. Cependant $\prod_{i=1}^r x_i \in \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Ceci contredit l'inclusion $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{p}$. □

Lemme A.4.2. *Soit A un anneau. Soient $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ des idéaux maximaux de A distincts. Alors pour tout $1 \leqslant i \leqslant r$, on a*

$$\mathfrak{q}_i^{e_i} + \prod_{j \neq i} \mathfrak{q}_j^{e_j} = A.$$

Démonstration. Soit $\mathfrak{m}$ un idéal maximal de A contenant $\mathfrak{q}_i^{e_i} + \prod_{j \neq i} \mathfrak{q}_j^{e_j}$. D'après le lemme A.4.1, on a $\mathfrak{q}_i \subset \mathfrak{m}$ et il existe $j \neq i$ tel que $\mathfrak{q}_j \subset \mathfrak{m}$. Ainsi, puisque $\mathfrak{q}_i$ et $\mathfrak{q}_j$ sont maximaux distincts, $A = \mathfrak{q}_i + \mathfrak{q}_j \subset \mathfrak{m}$ et $\mathfrak{m} = A$. Le lemme de Krull implique donc que $\mathfrak{q}_i^{e_i} + \prod_{j \neq i} \mathfrak{q}_j^{e_j} = A$. □

Lemme A.4.3. *Soit A un anneau. Soient $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ des idéaux maximaux distincts et $e_1, \ldots, e_r$ des entiers. On a alors*

$$\prod_{i=1}^r \mathfrak{q}_i^{e_i} = \bigcap_{i=1}^r \mathfrak{q}_i^{e_i}.$$

Démonstration. Si I et J sont deux idéaux de A tels que $I+J = A$, alors $IJ = I \cap J$. On en déduit le résultat par récurrence si l'on sait démontrer que $\mathfrak{q}_i^{e_i} + \prod_{j=1}^{i-1} \mathfrak{q}_j^{e_j} = A$ pour tout i, ce qui découle du lemme A.4.2. □

Lemme A.4.4. *Soit A un anneau. Soient $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ des idéaux maximaux distincts et $e_1, \ldots, e_r$ des entiers. Les applications de réductions modulo $\mathfrak{q}_i^{e_i}$ induisent un isomorphisme d'anneaux*

$$A/\prod_{i=1}^n \mathfrak{q}_i^{e_i} \xrightarrow{\sim} \prod_{i=1}^n A/\mathfrak{q}_i^{e_i}.$$

Démonstration. D'après le lemme A.4.3, il reste à prouver la surjectivité de l'application. Le lemme A.4.2 implique qu'il exste $x_i \in \prod_{j \neq i} \mathfrak{q}_j^{e_j}$ tel que $x_i - 1 \in \mathfrak{q}_i^{e_i}$. Cela suffit à prouver la surjectivité. □

A.5 Algèbres de dimension finie sur un corps

Soit k un corps et soit A une k-algèbre de dimension finie sur k.

Proposition A.5.1. *L'anneau A a un nombre fini d'idéaux maximaux $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$. De plus l'application diagonale $A \to \prod_{i=1}^r A_{\mathfrak{q}_i}$ est un isomorphisme de A-algèbres et pour tout $1 \leqslant i \leqslant r$, il existe un entier $m_i \geqslant 1$ tel que $A_{\mathfrak{q}_i} \simeq A/\mathfrak{q}_i^{m_i}$.*

Démonstration. Soient $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ des idéaux maximaux distincts de A. On déduit du lemme A.4.4 que l'application $A \to \prod_{i=1}^r A/\mathfrak{q}_i$ est surjective. On en déduit que $r \leqslant \dim_k(A)$ et donc que l'ensemble des idéaux maximaux de A est fini. Soient $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ les idéaux maximaux de A. Comme A est une k-algèbre de dimension finie, un idéal de A est maximal si et seulement si il est premier. Ainsi l'intersection des idéaux maximaux de A est l'intersection des idéaux premiers de A, c'est-à-dire l'idéal des éléments nilpotents de A. Cet idéal est nécessairement engendré par un nombre fini de générateurs (c'est même un k-espace vectoriel de dimension finie). On en déduit qu'il existe $m \geqslant 1$ tel que

$$\prod_{i=1}^r \mathfrak{q}_i^m \subset (\bigcap_{i=1}^r \mathfrak{q}_i)^m = \{0\}.$$

Le lemme A.4.4 implique alors que l'application $A \to \prod_{i=1}^r A/\mathfrak{q}_i^m$ est un isomorphisme. Comme l'annulateur de $A/\mathfrak{q}_i^m$ est $\mathfrak{q}_i^m$, on en déduit que $A_{\mathfrak{q}_i} \simeq (A/\mathfrak{q}_i^m)_{\mathfrak{q}_i}$. Comme $A/\mathfrak{q}_i^m$ est local d'idéal maximal l'image de $\mathfrak{q}_i$, on a bien $(A/\mathfrak{q}_i^m)_{\mathfrak{q}_i} = A/\mathfrak{q}_i^m$, ce qui achève la démonstration. □

Si $x \in A$, on appelle *trace* de x sur k et on note $\mathrm{Tr}_{A/k}(x)$ la trace de l'endomorphisme k-linéaire $y \mapsto xy$ de A. On note $b_{A/k}$ la forme k-bilinéaire symétrique sur A définie par $b_{A/k}(x, y) \coloneqq \mathrm{Tr}_{A/k}(xy)$. L'application $x \mapsto b_{A/k}(x, -)$ définit alors un morphisme de A-modules $A \to \mathrm{Hom}_k(A, k)$ (où la structure de A-module sur $\mathrm{Hom}_k(A, k)$ est déduite de la multiplication à gauche). Ce morphisme est bijectif (resp. injectif, resp. surjectif) si et seulement si la forme $b_{A/k}$ est non dégénérée.

Proposition A.5.2. *La forme $b_{A/k}$ est non dégénérée si et seulement si A est isomorphe à un produit de corps, extensions finies séparables de k.*

Démonstration. Supposons dans un premier temps que A est un produit de corps isomorphe à un produit $k_1 \times \cdots \times k_r$ d'extensions finies et séparables de k. La forme bilinéaire $b_{A/k}$ est alors la forme $b_{k_1/k} \oplus \cdots \oplus b_{k_r/k}$ qui est non dégénérée si et seulement si toutes les formes $b_{k_i/k}$ le sont. Le résultat est alors une conséquence de la proposition 1.2.2. que les blocs sont inversibles et donc que la forme est non dégénérée.

Il reste donc à démontrer que si la forme $b_{A/k}$ est non dégénérée, alors A est isomorphe à un produit d'extensions finies de k. La proposition A.5.1 montre qu'il suffit de prouver que A ne contient pas d'élément nilpotent non nul. Soit donc $a \in A$ un élément nilpotent. Si $x \in A$, alors ax est nilpotent, de même que l'endomorphisme $y \mapsto axy$, ainsi and $b_{A/k}(a, x) = \mathrm{Tr}_{A/k}(ax) = 0$. Comme la forme $b_{A/k}$ est non dégénérée, on en conclut que $a = 0$. □

A.6 Réseaux des anneaux principaux

Soit A un anneau principal. On appelle *réseau* de A un A-module libre de type fini. Si $M \subset N$ sont deux réseaux de A de même rang n, le théorème de la base adaptée implique qu'il existe des éléments non nuls $d_1 \mid \cdots \mid d_n$, uniques à des inversibles près, tels que $N/M \simeq A/(d_1) \times \cdots \times A/(d_n)$. L'idéal engendré par le produit $d_1 \cdots d_n$ ne dépend donc que de M et N et est noté $[N : M]$.

Proposition A.6.1. *Si $M \subset N \subset P$ sont des réseaux de même rang, on a $[P : M] = [P : N][N : M]$.*

Démonstration. Il suffit de remarquer que si Q est la matrice de passage d'une base de N à une base de M (c'est une matrice à coefficients dans A), alors $[N : M] = \det(Q)$. On en déduit immédiatement le résultat. □

A.7 Cohomologie des groupes

Soit G un groupe et soit A un G-module (voir la section 5.4.1. On appelle *cocycle* (ou plus souvent 1-cocyle) une application $c : G \to A$ telle que, pour tous $\sigma, \tau \in G$, on a $c(\sigma\tau) = \sigma(c(\tau)) + c(\sigma)$. On appelle *cobord* (ou plus souvent 1-cobord) une application $b : G \to A$ telle qu'il existe $a \in A$ vérifiant $b(\sigma) = a - \sigma(a)$ pour tout $\sigma \in G$. Les cocycles et les cobords forment deux groupes abéliens noté $Z^1(G, A)$ et $B^1(G, A)$. On a de plus $B^1(G, A) \subset Z^1(G, A)$ et on note $H^1(G, A)$. Le groupe abélien $H^1(G, A)$ est appelé *premier groupe de cohomologie de G à coefficients dans A*.

Exemple A.7.1. Supposons que le groupe G est cyclique et soit γ un générateur de G. Un cocycle c de G est entièrement déterminé par sa valeur sur γ.

Annexe B

Structures topologiques

B.1 Espaces topologiques localement compacts

Un espace topologique X est dit *localement compact* s'il est séparé et si tout point de X possède un voisinage compact.

B.2 Complété d'un espace métrique

Soit (X, d) un espace métrique ($d : X \times X \to X$) est une distance sur X. Il existe un espace métrique complet $(\widehat{X}, \hat{d})$ contenant X et tel que $\hat{d}|_{X\times X} = d$ ayant la propriété universelle suivante : pour tout espace métrique Y et toute application uniformément continue $f : X \to Y$, il existe une unique application uniformément continue $\hat{f} : \widehat{X} \to Y$ prolongeant f. L'espace métrique $(\widehat{X}, \hat{d})$ est alors unique à isométrie unique près. On en choisit donc un, que l'on appelle *complété* de l'espace métrique (X, d). De plus l'espace X est dense dans $\widehat{X}$ (voir par exemple [Bou71, Ch. II §3 Thm. 3 & Prop. 12] ainsi que [Bou74, Ch. IX §2 Prop. 1]).

B.3 Groupes topologiques

Un *groupe topologique* est un groupe G muni d'une topologie pour laquelle l'application de $G \times G \to G$ définie par $(g, h) \mapsto gh^{-1}$ est continue. En particulier, si $g_0 \in G$, les applications de G dans G définies par $g \mapsto g_0 g$, $g \mapsto g_0$ et $g \mapsto g^{-1}$ sont des homéomorphismes de G.

Lemme B.3.1. *Soit G un groupe et soit $\mathcal{V}$ un ensemble de parties de G contenant l'élément neutre e_G. Supposons que*

(i) pour tous $V_1, V_2 \in \mathcal{V}$, il existe $W \in \mathcal{V}$ tel que $W \subset V_1 \cap V_2$;

(ii) pour tout $V \in \mathcal{V}$, il existe $W \in \mathcal{V}$ tel que

$$W \cdot W^{-1} \coloneqq \{g_1 g_2^{-1} \mid (g_1, g_2) \in W \times W\} \subset V;$$

(iii) pour tout $V \in \mathcal{V}$ et tout $g \in G$, il existe $W \in \mathcal{V}$ tel que $W \subset gVg^{-1}$.

Alors il existe une unique topologie sur G pour laquelle G est un groupe topologique et $\mathcal{V}$ forme une base de voisinages de e_G.

Démonstration. Soit $\mathcal{T}$ l'ensemble des parties U de G telles que

$$\forall g \in U, \quad \exists V \in \mathcal{V},\ gV \subset U.$$

On vérifie immédiatement que $\mathcal{T}$ est une topologie sur G et que $\mathcal{V}$ est une base de voisinages de e_G. Montrons que G est un groupe topologique. Si $(g_1, g_2) \in G^2$ et U est un ouvert de G contenant $g \coloneqq g_1 g_2^{-1}$, soit $V \in \mathcal{V}$ tel que $gV \subset U$. Soit $V' \in \mathcal{V}$ tel que $gV'g^{-1} \subset V$ et soit $W \in \mathcal{V}$ tel que $W \cdot W^{-1} \subset V'$. On a alors $gW(gW)^{-1} = gW \cdot W^{-1}g^{-1} \subset gV'g^{-1} \subset V$. Ainsi l'application $(g_1, g_2) \mapsto g_1 g_2^{-1}$ est continue et G est un groupe topologique. Montrons que $\mathcal{V}$ est un système de voisinages de e_G pour cette topologie. Soit $V \in \mathcal{V}$ et posons $U = \{g \in V \mid \exists W \in \mathcal{V},\, gW \subset V\}$. Montrons que U est ouvert, ce qui suffit à prouver que V est un voisinage de e_G. Si $g \in U$, il existe $W \in \mathcal{V}$ tel que $gW \subset V$. Soit alors $W_1 \in \mathcal{V}$ tel que $W_1 \cdot W_1 \subset W$. Si $h \in gW_1$, on a $hW_1 \subset gW_1 \cdots W_1 \subset gW \subset V$, donc $gW_1 \subset U$, ce qui prouve que U est ouvert. L'unicité est évidente. □

Un groupe topologique est dit *métrisable* si sa topologie est définie par une distance. C'est en particulier un espace topologique séparé.

Dans un groupe topologique métrisable G, on appelle *suite de Cauchy* une suite $(g_n)_{n\geqslant}$ telle que, pour tout voisinage V de l'élément neutre e_G, il existe $N \geqslant 0$ tel que $g_{n+k}g_n^{-1} \in V$ pour $n \geqslant N$ et $k \geqslant 0$. Un groupe topologique métrisable est dit *complet* si toute suite de Cauchy d'éléments de G converge dans G.

Proposition B.3.2. *Un groupe topologique métrisable et localement compact est complet.*

Démonstration. Voir le corollaire 1 à la proposition 4 de [Bou71, Ch. III §3]. □

Lemme B.3.3. *Soit G un groupe topologique et soit H un sous-groupe ouvert de G. Alors H est fermé dans G.*

Démonstration. Le complémentaire de H dans G est l'union des classes ensembles Hg pour $g \notin G$. Chaque Hg est l'image inverse de H par l'application continu $x \mapsto xg^{-1}$ et est donc une partie ouverte de G. Le complémentaire de H dans G est donc une partie ouverte et H est donc fermé dans G. □

Lemme B.3.4. *Soit G un groupe topologique et soit H un sous-groupe de G. Alors l'application quotient $\pi : G \to G/H$ est ouverte.*

Démonstration. Soit U un ouvert de G. Il faut prouver que $\pi(U)$ est un ouvert de G/H, c'est-à-dire que $\pi^{-1}(\pi(U))$ est un ouvert de G. Comme $\pi^{-1}(\pi(U)) = \bigcap_{h\in H} hU$, c'est immédiat. □

Lemme B.3.5. *Soit G un groupe topologique et soit $H \subset G$ un sous-groupe fermé. Alors l'espace quotient G/H est séparé.*

Démonstration. Il suffit de prouver que le graphe de la relation d'équivalence $g_1 \sim g_2 \Leftrightarrow g_2 \in g_1H$ dans $G \times G$ est fermé. Il s'agit de l'image inverse de H par l'application continue $G \times G \to G$ définie par $(g_1, g_2) \mapsto g_1^{-1}g_2$ qui est donc fermée. □

Corollaire B.3.6. *Soit G un groupe topologique localement compact et soit H un sous-groupe fermé de G. Alors l'espace quotient G/H est localement compact.*

Démonstration. D'après le lemme B.3.5, l'espace G/H est séparé. Soit $W \subset G$ un voisinage de compact de l'élément neutre e_G. D'après le lemme B.3.4, $\pi(W)$ est un voisinage de e_GH dans G/H. De plus $\pi(W)$ est compact donc e_GH possède un voisinage compact $\pi(W)$. Pour tout $g \in G$, $\pi(gW) = g\pi(W)$ est alors un voisinage compact de gH, on en déduit que G/H est localement compact. □

Lemme B.3.7. *Soit G un groupe localement compact et soit K un sous-groupe compact de G. Alors l'application quotient $G \to G/K$ est fermée. De façon équivalente, si F est une partie fermée de G, alors la partie $F \cdot K$ est fermée dans G.*

Démonstration. Soit U l'ouvert complémentaire de F dans G et soit $x \notin F \cdot K$. Pour tout $k \in K$, Fk est fermé et $x \notin Fk$, il existe donc un voisinage de l'unité $V_k \subset G$ tel que $xV_k \subset G \smallsetminus Fk$. Comme K est compact il existe un nombre fini d'éléments $k_1, \ldots, k_r$ tels que $K \subset k_1V_{k_1}^{-1} \cup \cdots k_rV_{k_r}^{-1}$. Posons $V = V_{k_1} \cap \cdots \cap V_{k_r}$, c'est un voisinage de l'unité dans G. Si $k \in k_iV_{k_i}^{-1}$, on a $xV_{k_i} \subset G \smallsetminus Fk$, ce qui implique que

$$xV = \bigcap_{i=1}^{r} xV_i \subset \bigcap_{i=1} r \bigcap_{k\in K} G \smallsetminus Fk = G \smallsetminus F \cdot K.$$

Ainsi $G \smallsetminus F \cdot K$ est ouvert dans G. □

Lemme B.3.8. *Soit G un groupe topologique. Soit $\Gamma \subset G$ un sous-groupe.*

(i) Le sous-espace Γ est discret si et seulement si il existe un voisinage V de e_G tel que $V \cap \Gamma = \{e_G\}$.

(ii) Si Γ est un sous-groupe discret de G et si G est séparé, alors Γ est fermé dans G.

(iii) Si Γ est un sous-groupe discret de G et si G est localement compact, alors l'application quotient $\pi : G \to G/H$ est un revêtement.

Démonstration. Démontrons (i). Si Γ est discret, l'ensemble $\{e_G\}$ est un ouvert de Γ pour la topologie induite de sorte qu'il existe un voisinage V de e_G dans G tel que $V \cap \Gamma = \{e_G\}$. Réciproquement supposons qu'il existe un tel voisinage V et soit $\gamma \in \Gamma$. Alors γV est un voisinage de γ dans G et $\gamma V \cap \Gamma = \gamma(V \cap \Gamma) = \{\gamma\}$. Ainsi Γ est discret, ce qui prouve (i).

Prouvons (ii). Soit $x \in G \setminus \Gamma$. Soit V un voisinage de e_G tel que $V \cap \Gamma = \{e_G\}$ et soit W un voisinage de $\{e_G\}$ dans G tel que $W \cdot W^{-1} \subset V$. Si $\gamma_1, \gamma_2 \in Wx \cap \Gamma$, on a $\gamma_1\gamma_2^{-1} \in W \cdot W^{-1} \cap \Gamma = \{e_G\}$. Ainsi il existe au plus un élément de Γ dans Wx. Comme $x \notin \Gamma$ et comme G est séparé, on peut choisir W assez petit de sorte que $Wx \cap \Gamma = \emptyset$. Ainsi $G \setminus \Gamma$ est ouvert et Γ est un sous-groupe fermé de G.

Prouvons (iii). Soit W un voisinage compact de e_G tel que $W \cdot W^{-1} \cap \Gamma = \{e_G\}$. Pour $\gamma_1, \gamma_2 \in \Gamma$, on a $W\gamma_1 \cap W\gamma_2 \neq \emptyset \Rightarrow \gamma_1 = \gamma_2$. Alors, pour $x \in G$, $\pi(xW)$ est un voisinage de $\pi(x)$ et $pi^{-1}(\pi(xW)) = \coprod_{\gamma\in\Gamma} xW\gamma$. De plus la restriction de π à $xW\gamma$ induit une bijection continue de $xW\gamma$ sur $\pi(xW)$ qui est un homéomorphisme puisque W est compact. □

B.4 Anneaux et corps topologiques

Un *anneau topologique* est un anneau $(A, +, \times)$ muni d'une topologie pour laquelle $(A, +)$ est un groupe topologique et telle que l'application de $A \times A$ dans A donnée par $(a, b) \mapsto a \times b$ est continue.

Un *corps topologique* est un anneau topologique $(A, +, \times)$ tel que A est un corps et tel que l'application de $A^\times$ dans $A^\times$ donnée par $x \mapsto x^{-1}$ est continue.

B.5 Mesures de Haar

Soit X un espace topologique localement compact. Une *mesure de Radon* (positive) sur X est une mesure μ définie sur une tribu $\mathcal{T}$ contenant la tribu borélienne et telle que :

a) pour tout compact $K \subset X$, on a $\mu(K) < +\infty$;

b) pour tout $A \in \mathcal{T}$, on a $\mu(A) = \inf\{\mu(U) \mid A \subset U,\, U \text{ open}\}$;

c) pour tout ouvert U, on a $\mu(U) = \sup\{\mu(K) \mid K \subset U,\, K \text{ compact}\}$.

Si μ est une mesure de Radon sur X, on définit une forme $\mathbb{R}$-linéaire positive sur l'espace $C_c(X, \mathbb{R})$ des fonctions continues à support compact (positives signifie ici que $\mu(f) \geqslant 0$ dès que $f \geqslant 0$ presque partout) définie par $I_\mu(f) \coloneqq \int_X f(x)\, d\mu(x)$. L'application $\mu \mapsto I_\mu$ induit une bijection entre l'ensemble des mesures de Radon sur X et l'ensemble des formes $\mathbb{R}$-linéaires positives sur $C_c(X, \mathbb{R})$ (voir [Rud75, Ch. 2]).

Le résultat suivant est immédiat.

Lemme B.5.1. *Soit X un espace topologique localement compact et $(X_n)_{n\in\mathbb{N}}$ une famile croissante d'ouverts de X telle que $X = \bigcup_{n\in\mathbb{N}} X_n$. Alors si, pour tout $n \geqslant 0$, on se donne une mesure de Radon μ_n sur X_n de sorte que $\mu_{n+1}\,|_{X_n} = \mu_n$ pour tout $n \geqslant \mathbb{N}$, il existe une unique mesure de Radon μ sur X telle que $\mu|_{X_n} = \mu_n$ pour tout $n \in \mathbb{N}$.*

Si G est un groupe topologique localement compact, une *mesure de Haar* (à gauche) sur G est une mesure de Radon qui est invariante à gauche par translation par les éléments de G, c'est-à-dire que pour tout ensemble mesureable A et tout $g \in G$, gA est mesurable et $\mu(gA) = \mu(A)$. On définit de façon analogue la notion de mesure de Haar à droite.

Théorème B.5.2. *Soit G un groupe topologique localement compact. Il existe sur G une mesure de Haar à gauche non nulle et cette mesure est unique à multiplication près par un scalaire non nul.*

Démonstration. Voir [Wei].

□

Lemme B.5.3. *Soit G un groupe abélien localement compact. Soit H un sous-groupe fermé de G et soit $\pi : G \to G/H$ le morphisme quotient. Soit dh une mesure de Haar sur H. L'application linéaire $f \mapsto \overline{f}$ de $C_c(G, \mathbb{R})$ vers $C_c(G/H, \mathbb{R})$ est surjective.*

Démonstration. Commençons par remarquer que si $f \in C_c(G, \mathbb{R})$, alors $\overline{f} \in C_c(G/H, \mathbb{R})$. C'est une conséquence du théorème de convergence dominée. Soit $h \in C_c(G/H, \mathbb{R})$. Le support de h étant compact et $\pi : G \to G/H$ ouverte (lemme B.3.4), le support de h peut être recouvert par un nombre fini d'ouverts relativement compacts U_i de la forme $\pi(V_i)$ avec $V_i \subset G$ ouvert relativement compact.

Alors $C \coloneqq \bigcup_i \overline{V_i}$ est un compact de G tel que $\pi(C)$ contient le support de h. Soit $F \in C_c(G, \mathbb{R})$ une fonction telle que $F > 0$ sur C (une telle fonction existe, on le vérifie en utilisant le fait qu'un groupe localement compact est un espace topologique *normal* par [Bou71, Ch. III §4 Prop. 13] et [Bou74, Ch. IX §4 Prop 4]). Alors la fonction f sur G définie par

$$f(g) \coloneqq \begin{cases} h(\pi(g))F(g)\overline{F}(g)^{-1} & \text{if } g \in C \\ 0 & \text{if } g \notin C \end{cases}$$

est dans $C_c(G, \mathbb{R})$ et vérifie $\overline{f} = h$. □

Proposition B.5.4. *Soit G un groupe abélien localement compact. Soit H un sous-groupe fermé de G et soit $\pi : G \to G/H$ le morphisme quotient. Soit dg une mesure de Haar sur G et soit dh une mesure de Haar sur H. Alors il existe une unique mesure de Haar $d\overline{g}$ sur G/H telle que*

$$\forall f \in C_c(G, \mathbb{R}), \quad \int_{G/H} \overline{f}(\overline{g})\, d\overline{g} = \int_G f(g)\, dg$$

où $\overline{f} \in C_c(G/H, \mathbb{R})$ est définie par la formule $\overline{f}(\overline{g}) \coloneqq \int_H f(g+h)\, dh$ pour $g \in G$ relevant $\overline{g}$.

Si H est un sous-groupe discret de G, on peut choisir pour dh la *mesure de comptage* telle que tout singleton a mesure 1. Alors $\overline{f}(\overline{g}) = \sum_{\gamma \in \Gamma} f(g+\gamma)$.

Démonstration. On définit alors une mesure de Haar sur G/H par la formule

$$\int_{G/H} h\, d\overline{g} \coloneqq \int_G f\, dg$$

où $h = \overline{f}$ pour une certaine $f \in C_c(G, \mathbb{R})$ d'après le lemme B.5.3. Pour vérifier que cette mesure est bien définie, il suffit de vérifier que $\int_G f\, dg = 0$ dès que $\overline{f} = 0$. Soit C le support de f et soit $\psi \in C_c(G, \mathbb{R})$ une fonction positive telle que $\overline{\psi}$ est constante de valeur 1 sur C. On a alors

$$\begin{aligned} 0 = \int_G \psi(g) \int_H f(g+h)\, dh\, dg &= \int_H \int_G \psi(g) f(g+h)\, dg\, dh \\ &= \int_H \int_G \psi(g-h) f(g)\, dg\, dh = \int_G \overline{\psi}(\pi(g)) f(g)\, dg = \int_G f(g)\, dg. \quad \square \end{aligned}$$

Remarque B.5.5. Supposons que $G \simeq H_1 \times H_2$, avec G, H_1 et H_2 des groupes abéliens localement compacts. Soit dg une mesure de Haar sur G et soit dh_1 une mesure de Haar sur H_1. On déduit de la proposition B.5.4 qu'il existe une unique mesure de Haar dh_2 sur H_2 telle que $dg = dh_1 \otimes dh_2$.

Soit G un groupe abélien localement compact et soit Γ un sous-groupe discret de G. Un *domaine fondamental* pour l'action de Γ sur G est une partie mesurable $D \subset G$ telle que $G = \bigcup_{\gamma\in\Gamma}(\gamma + D)$ et $D \cap (\gamma + D)$ est de mesure 0 lorsque $\gamma \neq 0$. Un domaine fondamental est dit *strict* si on a deplus $D \cap (\gamma + D) = \emptyset$ lorsque $\gamma \neq 0$.

Lemme B.5.6. *Supposons que Γ est un sous-groupe discret et dénombrable countable d'un groupe abélien localement compact G. Soit D un domaine fondamental pour l'action de Γ sur G. On a alors*

$$\forall f \in C_c(G/\Gamma, \mathbb{R}), \quad \int_{G/\Gamma} f(\overline{g})\, d\overline{g} = \int_D (f \circ \pi)(g)\, dg.$$

Démonstration. Soit $h \in C_c(G)$ telle que $f = \overline{h}$ dont l'existence est assurée par le lemme B.5.3. Alors

$$\int_{G/\Gamma} f = \int_G h = \sum_{\gamma\in\Gamma} \int_{D+\gamma} h = \int_D (\sum_{\gamma\in\Gamma} h(g-\gamma)\, dg = \int_D f(\pi(g))\, dg. \qquad \square$$

Corollaire B.5.7. *Sous les hypothèses du lemme B.5.6, on a* $\mathrm{Vol}(G/\Gamma) = \mathrm{Vol}(D)$.

Bibliographie

[BH06] Colin J. Bushnell and Guy Henniart, *The local Langlands conjecture for* GL(2), Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 335, Springer-Verlag, Berlin, 2006.

[Bou71] N. Bourbaki, *Éléments de mathématique. Topologie générale. Chapitres 1 à 4*, Hermann, Paris, 1971.

[Bou74] ———, *Éléments de mathématique. Topologie générale. Chapitres 5 à 10*, Hermann, Paris, 1974.

[Bou85] Nicolas Bourbaki, *Éléments de mathématique*, Masson, Paris, 1985, Algèbre commutative. Chapitres 5 à 7.

[CG47] Henri Cartan and Roger Godement, *Théorie de la dualité et analyse harmonique dans les groupes abéliens localement compacts*, Ann. Sci. École Norm. Sup. (3) **64** (1947), 79–99.

[Jan] G. J. Janusz, *Algebraic number fields*.

[Rud75] Walter Rudin, *Analyse réelle et complexe*, Masson et Cie, Éditeurs, Paris, 1975, Traduit de l'anglais par N. Dhombres et F. Hoffman.

[RV99] Dinakar Ramakrishnan and Robert J. Valenza, *Fourier analysis on number fields*, Graduate Texts in Mathematics, vol. 186, Springer-Verlag, New York, 1999.

[Ser68] Jean-Pierre Serre, *Corps locaux*, Publications de l'Université de Nancago, No. VIII, Hermann, Paris, 1968, Troisième édition.

[Wei] A. Weil, *L'intégration dans les groupes topologiques et ses applications*, Hermann.