Théorie Algébrique des Nombres

Louis Mallet-Burgues

3 novembre 2025

Table des matières

Introduction

Ce texte rassemble tout ce que j'ai appris au cours de ces 3 dernières années en théorie algébrique des nombres, d'abord par le cours de François Charles à l'ENS qui m'a immédiatement passioné pour les questions de géométrie des nombres, puis par la lecture du livre *Number Fields* de Markus [9] en parallèle avec le cours de Gaëtan Chenevier donné à polytechnique [3] et ensuite par mon stage à Bâle avec Philipp Habegger. C'est l'occasion pour moi de compiler en un même endroit des choses qui me sont souvent utiles, et qui j'espère pourront aussi être utiles à toutes celles et ceux qui souhaitent en apprendre plus sur le sujet. Le texte a beaucoup changé entre le début de son écriture et maintenant, des parties entières ont été refaites pour être plus générales et plus naturelles, et probablement que si je voulais le réécrire aujourd'hui, je ne raconterais pas les choses dans le même ordre.

Historiquement, la théorie algébrique des nombres est issue des travaux de Gauss, Kummer et Dedekind, et sa formulation moderne s'intéresse aux *anneaux d'entiers de corps de nombres* et plus généralement aux *anneaux de Dedekind*. Si K est un corps de nombres, c'est à dire une extension finie de $\mathbb{Q}$, son anneau des entiers $\mathcal{O}_K$ désigne l'ensemble des éléments de K qui sont des entiers algébriques, c'est à dire qui sont annulés par un polynôme unitaire à coefficients entiers. L'arithmétique d'Euclide était largement basée sur le fait que l'anneau des entiers $\mathbb{Z}$ dispose de nombreuses bonnes propriétés : il est factoriel, et même principal et euclidien. De nombreux problèmes de théorie des nombres se résolvent grâce à la factorialité de $\mathbb{Z}$, et lorsqu'on essaie de résoudre des problèmes plus difficiles comme le grand théorème de Fermat, on a besoin de manipuler des anneaux plus exotiques que $\mathbb{Z}$, qui s'obtiennent en ajoutant à $\mathbb{Z}$ un ou plusieurs *entiers algébriques*. Kummer découvre alors au milieu du 19ème siècle que ces anneaux ne sont pas toujours factoriels, mettant à défaut une potentielle preuve du grand théorème de Fermat. Il a alors une idée miraculeuse pour tout de même pouvoir faire de l'arithmétique avec de tels anneaux : factoriser les *idéaux* au lieu de factoriser les éléments de l'anneau. C'est d'ailleurs de là que vient le terme *idéal* : un idéal est, pour Kummer, un nombre idéal, c'est à dire une sorte de généralisation multiplicative des nombres. Kummer s'intéresse donc aux anneaux d'entiers de corps de nombres, pour lesquels une factorisation unique des idéaux en produit d'ideaux premiers est possible.

Dedekind formalise cette idée et introduit le *groupe des classes* d'un tel anneau, qui mesure à quel point l'anneau en question est loin d'être principal, ou factoriel car c'est équivalent pour ces anneaux dits de Dedekind. Hensel démontre ensuite, par des considérations géométriques sur le réseau formé par l'anneau des entiers d'un corps de nombres, que le groupe des classes est toujours *fini*, du moins pour l'anneau des entiers d'un corps de nombres.

Se pose alors la question de déterminer le cardinal de ce groupe, aussi appelé nombre de classes du corps de nombres K en question, une question très difficile en générale et qui fait intervenir de l'analyse complexe par le biais des fonctions ζ de Dedekind. En effet, Dirichlet donne une formule *analytique* qui relie le nombre de classes d'un corps de nombres et le résidu en $s = 1$ de sa fonction ζ. Cette formule fait intervenir des données géométriques sur le réseau des entiers, et elle permet en pratique de décrire des algorithmes de calcul du nombre de classes d'un corps de nombres, on renvoie au cours de Pascal Monin par exemple [10].

L'idée de résoudre des problèmes de nature arithmétique par des considérations géométriques sur le réseau des entiers d'un corps de nombres forme en elle même une théorie, la *géométrie des nombres*. Celle-ci permet notamment d'étudier la structure du groupe des unités d'un anneau d'entiers de corps de nombres, ou encore de majorer la taille de la p-torsion du groupe des classes, pour p un nombre premier (voir [1] et [8]).

Un autre ingrédient crucial de la théorie algébrique des nombres est l'étude de la géométrie, au sens de la géométrie algébrique, du *spectre* de l'anneau des entiers $\mathcal{O}_K$ d'un corps de nombres K et de la *ramification* des morphismes $\mathrm{Spec}\,\mathcal{O}_L \longrightarrow \mathrm{Spec}\,\mathcal{O}_K$ associés à des extensions finies L/K. L'idée est de considérer l'anneau $\mathcal{O}_K$ comme un anneau de fonctions sur un espace $\mathrm{Spec}\,\mathcal{O}_K$ qui s'apparente à une courbe lisse dans le langage moderne des schémas. Les points (fermés) de cet espace correspondent alors aux idéaux premiers non-nuls, briques de base de la factorisation des idéaux. On ne parlera pas de schémas dans ce texte mais on insitera tout de même sur l'aspect géométrique de la ramification des idéaux premiers.

Le texte est organisé de façon logique plutôt qu'historique, en allant le plus possible du général au particulier. La première partie rappelle, ou présente, les prérequis d'algèbre commutative et de théorie des corps dont on aura besoin pour la suite. Le lecteur peut bien sûr la passer et y revenir au besoin. Le langage des catégories est omniprésent dans la suite et on rappelle les principaux concepts dont on aura besoin : foncteurs, transformations naturelles, propriétés universelles, lemme de Yoneda. L'idée est d'avantage de voir cela comme une philosophie, une façon de penser, plutôt que comme une boîte à théorèmes. Ainsi, le chapitre 1 rappelle au lecteur tout ce qu'il a besoin de connaître en théorie des catégories et en algèbre commutative pour comprendre la suite, et le chapitre 2 fait un rappel complet de théorie des corps et de théorie de Galois.

La partie II est la plus longue, elle présente la théorie des anneaux de Dedekind d'un point de vue moderne en mettant l'accent sur la géométrie de l'anneau et de son spectre. Le chapitre 3 présente la notion d'anneaux de Dedekind et le théorème de factorisation des idéaux, et donne la classification des modules de type fini sur un tel anneau. Le chapitre 4 est assez indépendant du reste et présente la théorie générale des réseaux, d'un point de vue algébrique et géométrique, avec la notion d'indice d'un couple de quasi-réseaux et avec les théorèmes de Minkowski. On donne une application au problème des 4 carrés de Lagrange tirée du cours de Chenevier [3]. Le chapitre 5 étudie les extensions d'anneaux de Dedekind et la théorie de la ramification : comment un idéal premier d'un anneau de Dedekind A se factorise-t-il en produit d'idéaux premiers dans un anneau de Dedekind plus gros B ? Cette question est abordée avec des idées venant de la géométrie algébrique. Le chapitre 6 applique cette théorie au cas

sympathique des anneaux d'entiers de corps de nombres $\mathcal{O}_K$ et applique les méthodes de géométrie des nombres aux questions de finitude du groupe des classes et de la structure du groupe des unités. Le chapitre 7 étudie le cas des extensions *galoisiennes* d'anneaux de Dedekind et parle de spécialisation du groupe de Galois et de symbole d'Artin. Le chapitre 8 applique toute cette théorie aux corps cyclotomiques. Le chapitre 9 étudie la ramification supérieure et permet une démonstration d'un théorème de Kronecker et Weber absolument fondamental en théorie des nombres : toute extension finie galoisienne de $\mathbb{Q}$ de groupe de Galois abélien est contenue dans un corps cyclotomique. Enfin, le chapitre 10 explique comment Gauss donne une formule exacte pour la 2-torsion du groupe des classes (restreint) d'un corps quadratique, un des rares cas où l'on dispose d'une formule exacte de ce type.

La partie III est une introduction à la théorie analytique des nombres. Le chapitre 11 est un calcul préliminaire sur le nombre d'idéaux de petite norme d'un corps de nombres, et le chapitre 12 introduit les fonctions ζ de corps de nombres, qui permettent d'obtenir des informations statistiques sur les idéaux premiers d'un corps de nombres. On présente aussi la formule analytique du nombre de classes en suivant la présentation de Markus [9].

Enfin, la partie IV s'intéresse à la théorie locale, c'est à dire à l'étude de certains corps qui ne possèdent qu'un seul nombre premier en un certain sens. On introduit au chapitre 13 la théorie générale des corps valués, puis on étudie plus particulièrement les corps locaux au chapitre 14, c'est à dire les extensions finies des corps $\mathbb{Q}_p$ et les corps de fonctions de courbes sur un corps fini. Enfin, on fait le lien avec les corps de nombres, et plus généralement les corps globaux, au chapitre 15.

Si vous trouvez une erreur ou une imprécision dans ce texte, n'hésitez pas à m'envoyer un mail sur cette adresse :

louis.mallet-burgues AT ens.psl.eu

Bonne lecture !

Première partie

Prérequis

Chapitre 1

Algèbre commutative

> S'il est une chose en mathématiques qui me fascine plus que toute autre (et sans doute depuis toujours), ce n'est ni le "nombre" ni la "grandeur", mais bien la forme. Et parmi les mille et un visages sous lesquels la forme choisit de se révéler à nous, celui qui me fascine plus que tout autre, et continue à me fasciner, c'est la structure cachée dans les objets mathématiques.
>
> Alexandre Grothendieck,
> Récoltes et Semailles

Sauf spécification contraire, tous les anneaux seront considérés *commutatifs et unitaires*.

1.1 Catégories, foncteurs et transformations naturelles

On présente ici les notions de base de théorie des catégories qui seront utilisées ici. Le but n'est pas de faire un cours de théorie des catégories mais simplement de rappeler les notions dont on va avoir besoin. On renvoie par exemple à [7] pour les preuves des énoncés et pour (beaucoup) plus de détails.
Le choix est fait ici de ne pas s'attarder sur les difficultés de théorie des ensembles.

Définition 1.1. *Une catégorie $\mathcal{C}$ est la donnée d'une collection d'objets ainsi que pour chaque paire d'objets A, B de $\mathcal{C}$, d'un ensemble* $\mathrm{Hom}(A, B)$ *dont les éléments sont appelés morphismes ou flèches de A vers B et pour chaque triplet d'objets A, B, C de $\mathcal{C}$, d'une application appelée composition :*

$$\mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \longrightarrow \mathrm{Hom}(A, C)$$

qu'on note $(f,g) \mapsto f \circ g$ *ou pour faire plus court* fg*. On demande que cette loi soit associative au sens où, lorsque c'est bien défini, on ait :*

$$f(gh) = (fg)h$$

pour f, g *et* h *trois morphismes. On demande aussi qu'il y ait pour chaque objet* A*, un élément neutre noté* id_A *ou* 1_A *pour la composition, au sens où pour tout morphisme* f *vers* A *et tout morphisme* g *depuis* A *on ait* $\mathrm{id}_A f = f$ *et* $g\,\mathrm{id}_A = g$*. Une flèche* $A \xrightarrow{f} B$ *est un isomorphisme si elle admet un inverse* $B \xrightarrow{g} A$ *pour la composition (des deux côtés). Deux objets sont isomorphes s'il existe un isomorphisme entre les deux.*

Un foncteur entre deux catégories $F : \mathcal{C} \longrightarrow \mathcal{D}$ *est la donnée pour chaque objet* A *de* $\mathcal{C}$ *d'un objet* $F(A)$ *(ou* FA*) de* $\mathcal{D}$ *et pour chaque flèche* $A \xrightarrow{f} B$ *dans* $\mathrm{Hom}_{\mathcal{C}}(A,B)$ *d'une flèche* $F(f) \in \mathrm{Hom}_{\mathcal{D}}(FA, FB)$*. On demande les compatibilités suivantes :*

$$F(\mathrm{id}_A) = \mathrm{id}_{FA}$$

et lorsque cela a du sens :

$$F(fg) = (F(f))(F(g)).$$

Les exemples typiques de catégories sont :

— La catégorie des ensembles dont les objets sont les ensembles et les morphismes entre deux ensembles sont les applications. La composition est la composition usuelle des applications.

— La catégorie des groupes (abéliens) dont les objets sont les groupes (abéliens) et les morphismes sont les morphismes de groupes (abéliens) et la composition est comme précedemment.

— La catégorie des modules sur un anneau A dont les objets sont les A-modules et les morphismes sont les morphismes de A-modules.

— La catégorie des espaces topologiques dont les objets sont les espaces topologiques et les morphismes sont les applications continues.

Définition 1.2. *Soit* $\mathcal{C}$ *une catégorie. Un objet* I *est dit initial si pour tout objet* X *de* $\mathcal{C}$*, il existe un unique morphisme de* I *vers* X*. Dualement, un objet* F *est dit final si pour tout objet* X *de* $\mathcal{C}$*, il existe un unique morphisme de* X *vers* F*.*

Il est facile de vérifier que deux objets initiaux sont isomorphes (et qu'il existe un unique isomorphisme entre les deux) et que deux objets finaux sont isomorphes (idem). Cela permet de définir des objets de façon universelle.

Exemple 1.3. *Par exemple, si* A *est un anneau (commutatif unitaire), on peut définir* $A[X]$ *de façon universelle comme l'objet initial de la catégorie des* A*-algèbres pointées. Plus précisément, considérons la catégorie* PtAlg_A *dont les objets sont les couples* (B,b) *avec* B *une* A*-algèbre commutative et* $b \in B$ *et dont les flèches* $(B,b) \longrightarrow (C,c)$ *sont les morphismes de* A*-algèbres qui envoient* b *sur* c*.*
Alors pour toute algèbre pointée (B,b)*, il existe un unique morphisme dans la catégorie* PtAlg_A *de* $(A[X],X)$ *vers* (B,b)*. Autrement dit,* $(A[X],X)$ *est initial dans cette catégorie et est donc défini à unique isomorphisme près.*

Il est bien sûr possible de composer deux foncteurs $F : \mathcal{C} \longrightarrow D$ et $G : \mathcal{D} \longrightarrow \mathcal{E}$ en un foncteur $G \circ F : \mathcal{C} \longrightarrow \mathcal{E}$, et on a ainsi une catégorie des catégories, l'identité d'une catégorie $\mathcal{C}$ étant le foncteur qui envoie A sur A et f sur f.

Définition 1.4. *Soient $\mathcal{C}$ et $\mathcal{D}$ deux catégories et $F, G : \mathcal{C} \longrightarrow \mathcal{D}$ deux foncteurs. Une transformation naturelle de F vers G, notée $\alpha : F \implies G$ est la donnée pour tout objet A de $\mathcal{C}$ d'un morphisme $\alpha_A : FA \longrightarrow GA$ dans la catégorie $\mathcal{D}$ tel que pour tout morphisme $A \xrightarrow{f} B$, on ait un diagramme commutatif :*

$$\begin{array}{ccc} FA & \xrightarrow{F(f)} & FB \\ {\scriptstyle \alpha_A}\downarrow & & \downarrow{\scriptstyle \alpha_B} \\ GA & \xrightarrow{G(f)} & GB \end{array}$$

autrement dit $\alpha_B F(f) = G(f)\alpha_A$. On notera parfois α au lieu de α_A pour simplifier.
Un isomorphisme de foncteurs est un transformation naturelle $\alpha : F \implies G$ qui admet un inverse $\beta : G \implies F$ (nécessairement unique) au sens où $\alpha_A \beta_A = \mathrm{id}$ et $\beta_A \alpha_A = \mathrm{id}$ (on note id *pour* id_A *et* id_B *toujours pour simplifier les notations).*
Une transformation naturelle est un isomorphisme si et seulement si pour tout A, α_A est un isomorphisme. Deux foncteurs sont isomorphes s'il existe un isomorphisme entre les deux.

Le terme "naturel" dans "transformation naturelle" peut s'interpréter de la façon suivante : une transformation naturelle entre deux foncteurs est un procédé pour passer de FA à GA qui est naturel au sens où il varie de façon cohérente quand on fait varier A.
Ainsi on dira parfois que FA est isomorphe à GA naturellement en A pour dire que les foncteurs F et G sont isomorphes.

Définition 1.5. *Soient $\mathcal{C}$ et $\mathcal{D}$ deux catégories, $F : \mathcal{C} \longrightarrow \mathcal{D}$ un foncteur et $G : \mathcal{D} \longrightarrow \mathcal{C}$ un foncteur. On dit que F et G forment une équivalence de catégories entre $\mathcal{C}$ et $\mathcal{D}$ si $F \circ G$ est isomorphe au foncteur identité de $\mathcal{D}$ et $G \circ F$ est isomorphe au foncteur identité de $\mathcal{C}$.*

Deux catégories sont équivalentes s'il existe une équivalence de catégories entre les deux. Par exemple la catégorie des $\mathbb{Z}$-modules est équivalente à la catégorie des groupes abéliens. L'équivalence de catégories est la bonne notion pour dire que deux catégories sont "algébriquement les mêmes".

Théorème 1.6. *Un foncteur $F : \mathcal{C} \longrightarrow \mathcal{D}$ réalise une équivalence de catégories si et seulement si il est :*

- *Pleinement fidèle, au sens où pour tous A, B de $\mathcal{C}$ le foncteur réalise une bijection* $\mathrm{Hom}(A, B) \longrightarrow \mathrm{Hom}(FA, FB)$.
- *Essentiellement surjectif sur les objets, au sens où pour tout objet Y de $\mathcal{D}$ il existe un objet X de $\mathcal{C}$ et un isomorphisme entre FX et Y.*

Étant donnée une catégorie $\mathcal{A}$, on définit sa catégorie opposée $\mathcal{A}^{op}$ dont les objets sont les mêmes que dans $\mathcal{A}$ mais avec :

$$\mathrm{Hom}_{\mathcal{A}^{op}}(A, B) = \mathrm{Hom}_{\mathcal{A}}(B, A)$$

et en inversant la composition, c'est à dire que $f \circ_{\mathcal{A}^{op}} g = g \circ_{\mathcal{A}} f$. La donnée d'un foncteur $\mathcal{A}^{op} \longrightarrow \mathcal{B}$ équivaut à la donnée d'un foncteur $\mathcal{A} \longrightarrow \mathcal{B}^{op}$, on parle parfois de foncteur *contravariant* de $\mathcal{A}$ vers $\mathcal{B}$ car il oppose le sens des flèches. Un foncteur au sens défini plus haut est alors appelé *covariant*.

On note Set la catégorie des ensembles. Tout objet A d'une catégorie $\mathcal{C}$ induit un foncteur $\mathrm{Hom}(A, \bullet) : \mathcal{C} \longrightarrow \mathrm{Set}$ qui envoie B sur l'ensemble $\mathrm{Hom}(A, B)$ et une flèche $f : X \longrightarrow Y$ vers $f_* : \mathrm{Hom}(A, X) \longrightarrow \mathrm{Hom}(A, Y)$ qui envoie $g : A \longrightarrow X$ sur fg :

$$f_*(g) = fg.$$

De même, A induit un foncteur $\mathrm{Hom}(\bullet, A) : \mathcal{C}^{op} \longrightarrow \mathrm{Set}$ (i.e. un foncteur contravariant de $\mathcal{C}$ vers Set) défini de façon similaire, avec cette fois-ci f envoyée vers l'application de tiré en arrière par f, notée f^* telle que :

$$f^*(g) = gf.$$

Le lemme de Yoneda affirme qu'un objet est entièrement déterminé par l'un (ou l'autre) de ces deux foncteurs. De façon plus philosophique, si on sait comment un objet voit les autres objets de la catégorie (ou comment il est vu par les autres objets de la catégorie), on connait cet objet.

Lemme 1.7. *(Yoneda) Soit $\mathcal{C}$ une catégorie et $F : \mathcal{C} \longrightarrow \mathrm{Set}$ un foncteur. Soit A un objet de $\mathcal{C}$. On a une bijection (naturelle en A) entre l'ensemble $F(A)$ et l'ensemble des transformations naturelles de $\mathrm{Hom}(A, \bullet)$ vers F :*

$$\mathrm{Nat}(\mathrm{Hom}(A, \bullet), F) \cong FA.$$

La bijection en question est donnée par $\alpha \mapsto \alpha_A(\mathrm{id}_A)$.

En pratique on retient surtout le corollaire suivant obtenu en appliquant ce qui précède au foncteur $F = \mathrm{Hom}(B, \bullet)$.

Corollaire 1.8. *Soit $\mathcal{C}$ une catégorie et A, B deux objets de $\mathcal{C}$. On a une bijection :*

$$\mathrm{Hom}(B, A) \cong \mathrm{Nat}(\mathrm{Hom}(A, \bullet), \mathrm{Hom}(B, \bullet)).$$

L'intérêt du lemme de Yoneda et de son corollaire réside dans le fait que certains objets A sont décrits par des propriétés universelles, c'est à dire par leur foncteur $\mathrm{Hom}(A, \bullet)$ ou $\mathrm{Hom}(\bullet, A)$ et qu'il est alors plus facile de construire un morphisme $\mathrm{Hom}(A, X) \longrightarrow \mathrm{Hom}(B, X)$ pour tout X, et de vérifier qu'il est naturel en X, plutôt que de construire un morphisme $B \longrightarrow A$.
Par exemple, dans la catégorie des modules sur un anneau A, étant donnés M et N deux A-modules, leur produit tensoriel $M \otimes_A N$ est déterminé par la propriété universelle suivante :

$$\mathrm{Hom}(M \otimes_A N, X) \cong \mathrm{Bil}_A(M \times N, X)$$

naturellement en X (ou $\mathrm{Bil}_A(M \times N, X)$ désigne l'ensemble des applications bilinéaires de $M \times N$ vers X). Cela permet par exemple de voir que $M \otimes N \cong N \otimes M$ ou que $M \otimes (N \otimes P) \cong (M \otimes N) \otimes P$ en travaillant directement avec la propriété universelle, ou encore que

$M \otimes_A A/I \cong M/IM$ pour tout idéal I de A avec la même méthode. En pratique on peut par exemple raisonner ainsi :

$$\mathrm{Hom}(M \otimes_A A/I, X) \cong \mathrm{Bil}_A(M \times A/I, X) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(A/I, X)) \cong \mathrm{Hom}(M, X(I)) \cong \mathrm{Hom}(M/IM, X)$$

où $X(I)$ désigne la I-torsion de X, c'est à dire le sous-module des éléments de X tués par la multiplication par I. Ces isomorphismes étant naturels en X, on a donc par le lemme de Yoneda un isomorphisme :

$$M \otimes_A A/I \cong M/IM.$$

Dans cette esquisse de preuve on a aussi utilisé la propriété universelle du quotient : si N est un sous-module de M, on a :

$$\mathrm{Hom}_A(M/N, X) \cong \{f \in \mathrm{Hom}(M, X) \mid f(N) = 0\}$$

naturellement en X.

1.2 Quelques notions de théorie des modules

On rappelle des notions de théorie des modules qui seront omniprésentes dans la suite. Le but encore une fois n'est pas de faire un cours détaillé et il n'y aura pas de preuve dans cette partie. On renvoie à n'importe quel cours d'algèbre commutative pour les démonstrations omises.

Définition 1.9. *Un foncteur F entre deux catégories de modules est dit est dit additif si pour toute paire de modules dans la catégorie de départ, X et Y, l'application* $\mathrm{Hom}(X, Y) \longrightarrow \mathrm{Hom}(FX, FY)$ *est un morphisme de groupes abéliens. Un tel foncteur préserve alors les sommes directes et envoie le module nul sur le module nul. Un foncteur F est dit exact à gauche s'il préserve l'exactitude à gauche des suites, autrement dit si pour toute suite exacte $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ la suite $0 \longrightarrow FM \longrightarrow FN \longrightarrow FP$ est exacte. De façon équivalente, il est exact à gauche si pour toute suite exacte $0 \longrightarrow M \longrightarrow N \longrightarrow P$, la suite $0 \longrightarrow FM \longrightarrow FN \longrightarrow FP$ est exacte. On définit de même la notion de foncteur exact à droite. Un foncteur est exact s'il est exact à gauche et à droite.*

Le lemme de Yoneda permet de vérifier l'exactitude d'une suite.

Proposition 1.10. *(Exactitude universelle) Un morphisme $M \longrightarrow N$ est surjectif si et seulement si pour tout A-module X, le morphisme* $\mathrm{Hom}(N, X) \longrightarrow \mathrm{Hom}(M, X)$ *est injectif. Un morphisme $M \longrightarrow N$ est injectif si et seulement si pour tout A-module X, le morphisme* $\mathrm{Hom}(X, M) \longrightarrow \mathrm{Hom}(X, N)$ *est injectif.*
Une suite $M \longrightarrow N \longrightarrow P \longrightarrow 0$ est exacte si et seulement si pour tout A-module X, la suite :

$$0 \longrightarrow \mathrm{Hom}(P, X) \longrightarrow \mathrm{Hom}(N, X) \longrightarrow \mathrm{Hom}(M, X)$$

est exacte. Une suite $0 \longrightarrow M \longrightarrow N \longrightarrow P$ est exacte si et seulement si pour tout A-module X, la suite :

$$0 \longrightarrow \mathrm{Hom}(X, M) \longrightarrow \mathrm{Hom}(X, N) \longrightarrow \mathrm{Hom}(X, P)$$

est exacte.

Cela permet par exemple de démontrer l'exactitude à droite du produit tensoriel.

Proposition 1.11. *Soit M un A-module. Le foncteur $\bullet \otimes_A M$ est exact à droite.*

Démonstration. Soit $X \longrightarrow Y \longrightarrow Z \longrightarrow 0$ une suite exacte. Il s'agit de voir que la suite $X \otimes M \longrightarrow Y \otimes M \longrightarrow Z \otimes M$ est exacte, ou d'après la propostion précédente, que pour tout W, la suite :

$$0 \longrightarrow \mathrm{Bil}_A(Z \times M, W) \longrightarrow \mathrm{Bil}_A(Y \times M, W) \longrightarrow \mathrm{Bil}_A(X \times M, W)$$

est exacte. C'est alors un simple exercice. □

Définition 1.12. *Soit M un A-module. Il est de présentation finie s'il existe une suite exacte :*

$$0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0$$

avec N et L de type fini et L libre.
Il est plat si le produit tensoriel par M est exact, il est projectif si le foncteur $\mathrm{Hom}(M, \bullet)$ *est exact, et il est injectif si le foncteur* $\mathrm{Hom}(\bullet, M)$ *est exact.*

Une somme directe quelconque de modules plats (resp. projectifs) est un module plat (resp. projectif). Pour toute partie multiplicative S de A, la localisation est un foncteur exact et donc $S^{-1}A$ est un module plat. On rappelle la caractérisation suivante des modules projectifs.

Proposition 1.13. *Soit M un A-module. Les énoncés suivants sont équivalents :*

- *M est projectif.*
- *Tout morphisme surjectif vers M admet une section qui est un morphisme (un inverse à droite pour la composition).*
- *M est facteur direct d'un module libre, c'est à dire qu'il existe N tel que $M \oplus N$ soit libre. Si M est de type fini on peut aussi demander que $M \oplus N$ soit libre de type fini.*

Un module projectif de type fini est toujours de présentation finie puisque si $M \oplus N$ est libre de type fini, on a une suite exacte :

$$0 \longrightarrow N \longrightarrow M \oplus N \longrightarrow M \longrightarrow 0$$

et N est de type fini comme quotient de $M \oplus N$ qui est de type fini.

Définition 1.14. *Un anneau A est dit noéthérien si tout idéal de A est de type fini, ou de façon équivalente si toute suite croissante d'idéaux de A stationne. Un A-module M est dit noéthérien si toute suite croissante de sous-modules de M stationne.*

Un A-module noéthérien est toujours de type fini. Un théorème de Hilbert affirme que si A est noétherien, alors $A[X]$ est aussi noétherien et puisque tout quotient d'un anneau noétherien est encore noétherien, toute algèbre de type fini sur A est noéthérienne. Tout anneau principal est noétherien donc $\mathbb{Z}$ est noétherien.
Si A est noétherien, tout A-module M de type fini est noéthérien et en particulier tout sous-module de M est noéthérien donc de type fini.

Le théorème suivant est une des nombreuses versions du lemme de Nakayama. On se contentera ici de cette version pour les anneaux locaux.

Théorème 1.15. *(Nakayama) Soit A un anneau local d'idéal maximal $\mathfrak{m}$ et M un A-module de type fini.*
Si $M = \mathfrak{m}M$, alors $M = 0$. Autrement dit M est nul si et seulement si $M \otimes_A k = 0$ avec $k = A/\mathfrak{m}$ le corps résiduel.
De plus, si M est un A-module quelconque et $M = N + \mathfrak{m}N'$ avec N' de type fini, alors $M = N$.

Démonstration. Supposons $M = \mathfrak{m}M$. On se donne $x_1, \dots, x_n \in M$ des générateurs. Puisque $M = \mathfrak{m}M$, on peut écrire :

$$x_i = \sum_j m_{ij} x_j$$

avec $m_{ij} \in \mathfrak{m}$. On pose $U = (m_{ij})$: c'est une matrice $n \times n$ à coefficients dans $\mathfrak{m}$, et son polynôme caractéristique P est de la forme $X^n + a_{n-1}X^{n-1} + \cdots + a_0$ avec les a_i dans $\mathfrak{m}$. La formule de Cramer donne :

$$P(1)\,\mathrm{id} = \det(\mathrm{id} - U)\,\mathrm{id} = V \cdot (\mathrm{id} - U)$$

avec V une matrice à coefficients dans A. Au niveau des coefficients cela donne :

$$P(1)\delta_{ij} = \sum_k v_{ik}(\delta_{kj} - m_{kj})$$

et donc :

$$P(1)x_i = \sum_j P(1)\delta_{ij}x_j = \sum_{j,k} v_{ik}(\delta_{kj} - m_{kj})x_j = \sum_k (v_{ik}x_k - v_{ik}x_k) = 0.$$

Or $P(1) = 1 + \sum a_i \notin \mathfrak{m}$ donc $P(1)$ est inversible dans A et ainsi $x_i = 0$. Puisque les x_i engendrent M, on a $M = 0$.
La deuxième affirmation vient du fait que :

$$M \otimes_A k = M/\mathfrak{m}M.$$

Enfin, si $M = N + \mathfrak{m}N'$ avec N' de type fini, alors M/N est engendré par les images d'un ensemble quelconque de générateurs de N', donc il est de type fini et il vérifie clairement $\mathfrak{m}(M/N) = M/N$, donc par ce qui précède $M/N = 0$ et $M = N$. □

1.3 Spectre d'un anneau

Soit A un anneau, le spectre de A, noté $\mathrm{Spec}\,A$ est l'ensemble des idéaux premiers de A. On étudie ici cet objet de façon purement ensembliste, sans parler de géométrie. Pour I un idéal de A, on note $V(I)$ le sous-ensemble de $\mathrm{Spec}\,A$ constitué des $\mathfrak{p}$ qui contiennent I. Notons que le spectre de A est vide si et seulement si A est l'anneau nul : en effet, si A est non nul, par le théorème de Krull il possède un idéal maximal donc premier.
Les énoncés de cette partie sont parfois de simples vérifications dont la démonstration est laissée en exercice.

Remarque 1.16. En géométrie algébrique, le spectre de A est muni d'une structure très riche : c'est d'abord un espace topologique (et les $V(I)$ sont des parties fermées), qui est même muni d'un faisceau d'anneaux commutatifs. Bien que nous ne mentionnerons pas cette structure supplémentaire, il est toujours utile en algèbre commutative de penser au spectre comme à un espace géométrique, et qu'un morphisme d'anneaux $A \longrightarrow B$ induit une "transformation géométrique" $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$, comme on va le voir.

Par exemple, $\operatorname{Spec}\mathbb{Z}$ est constitué de l'ensemble des nombres premiers et de l'idéal nul. Le spectre d'un corps est un singleton.

Si $A \xrightarrow{f} B$ est un morphisme d'anneaux, et $\mathfrak{p}$ est un idéal premier de B, alors l'idéal $f^{-1}(\mathfrak{p})$ est premier car on a un morphisme injectif :

$$A/f^{-1}(\mathfrak{p}) \hookrightarrow B/\mathfrak{p}$$

et donc $A/f^{-1}(\mathfrak{p})$ est intègre. On a donc une application induite au niveau des spectres :

$$\operatorname{Spec} B \xrightarrow{f^*} \operatorname{Spec} A$$

et il est immédiat de vérifier que l'on a ainsi défini un foncteur contravariant de la catégorie des anneaux vers la catégorie des ensembles.
Voyons à présent plusieurs cas particuliers.

Proposition 1.17. *Si f est un morphisme surjectif $A \longrightarrow B$, alors* $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *est injectif, et son image est donnée par* $V(\operatorname{Ker} f)$.
Autrement dit, on a pour tout idéal de I de B, une bijection :

$$\operatorname{Spec}(B/I) \cong V(I).$$

qui envoie $\mathfrak{p}$ sur son image inverse dans B.

Démonstration. Cela découle de la bijection entre les idéaux de B/I et les idéaux de B qui contiennent I. On vérifie facilement que cette bijection se restreint en une bijection au niveau des idéaux premiers. □

Définition 1.18. *On rappelle que si $\mathfrak{q}$ est un idéal premier de A, $S_\mathfrak{q} = A \setminus \mathfrak{q}$ est une partie multiplicative de A et on peut considérer le localisé $A_\mathfrak{q} = S_\mathfrak{q}^{-1}A$. Si M est un A-module, on notera $M_\mathfrak{q} = M \otimes_A A_\mathfrak{q} = S_\mathfrak{q}^{-1}M$ le localisé de M par $S_\mathfrak{q}$. Ainsi $\mathfrak{q}_\mathfrak{q}$ est l'unique idéal maximal de l'anneau local $A_\mathfrak{q}$. On appelle corps résiduel de A en $\mathfrak{p}$ le corps :*

$$k = A_\mathfrak{q}/\mathfrak{q}_\mathfrak{q}.$$

Puisque la localisation commute au quotient, c'est aussi le corps des fractions de l'anneau intègre $A/\mathfrak{q}$:

$$k = \operatorname{Frac}(A/\mathfrak{q})$$

et ces deux définitions sont utiles.

Proposition 1.19. *Si S est une partie multiplicative de A, le morphisme de localisation $A \longrightarrow S^{-1}A$ induit une bijection :*

$$\operatorname{Spec}(S^{-1}A) \cong \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \emptyset\} \subseteq \operatorname{Spec} A.$$

En particulier pour tout $f \in A$:

$$\operatorname{Spec} A[1/f] \cong \{\mathfrak{p} \in \operatorname{Spec} A \mid f \notin \mathfrak{p}\}$$

et pour tout idéal premier $\mathfrak{q}$ de A :

$$\operatorname{Spec} A_{\mathfrak{q}} \cong \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \subseteq \mathfrak{q}\}.$$

Démonstration. Les deux derniers points découlent du premier (en effet si $f^n \in \mathfrak{p}$ pour un $n \geq 0$, alors $f \in \mathfrak{p}$ car $\mathfrak{p}$ est premier).
On laisse au lecteur le soin de vérifier que $A \longrightarrow S^{-1}A$ induit une fonction bien définie :

$$\operatorname{Spec}(S^{-1}A) \longrightarrow \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \emptyset\}$$

et que $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ en est une bijection réciproque. □

La remarque suivante pose une intuition géométrique sur le spectre d'un anneau, elle n'est pas indispensable pour la suite cependant.

Remarque 1.20. En géométrie algébrique, les éléments f de l'anneau A peuvent être interprétés comme des fonctions sur l'espace $\operatorname{Spec} A$ de la façon suivante : pour tout point $\mathfrak{p}$ de $\operatorname{Spec} A$, la valeur de f au point $\mathfrak{p}$ est l'image de f par le morphisme $A \longrightarrow k(\mathfrak{p})$ où $k(\mathfrak{p})$ est le corps résiduel au point $\mathfrak{p}$. Ainsi f est une fonction qui ne prend pas ses valeurs dans un corps fixé, mais dans un corps qui varie en fonction du point d'évaluation. Dans certains cas le corps résiduel ne varie pas (du moins en les idéaux maximaux), c'est le cas quand on considère par exemple des K-algèbres de type fini sur un corps K algébriquement clos : par le Nullstellensatz, les corps résiduels en des idéaux maximaux sont alors tous isomorphes à K, et on peut alors vraiment voir f comme une fonction de $\operatorname{Spec} A$ vers le corps K.
En général, le morphisme $\operatorname{Spec} A[1/f] \hookrightarrow \operatorname{Spec} A$ permet d'identifier $\operatorname{Spec} A[1/f]$ à un ouvert de $\operatorname{Spec} A$ qui est le lieu de non annulation de l'élément f vu comme une fonction sur l'espace $\operatorname{Spec} A$. De même, $\operatorname{Spec} A/I \hookrightarrow \operatorname{Spec} A$ identifie $\operatorname{Spec} A/I$ à un fermé de $\operatorname{Spec} A$ qui est le lieu d'annulation des éléments de I vus comme des fonctions sur $\operatorname{Spec} A$.
C'est ici que le terme *localisation* prend tout son sens : localiser, c'est considérer un certain sous-ensemble du spectre, et en particulier localiser en un idéal premier (qui correspond à un point de $\operatorname{Spec} A$), c'est considérer une sorte de voisinage infinitésimal du point en question.
Cette intuition géométrique est utile en algèbre commutative : pour vérifier qu'une propriété d'un module est vraie, il suffit parfois de la vérifier localement, c'est à dire pour chaque point de $\operatorname{Spec} A$ dans un voisinage infinitésimal, ce qui se traduit par la proposition suivante.

Proposition 1.21. *(Exactitude locale) Soit M un A-module. Les énoncés suivants sont équivalents :*

— $M = 0$.

— *Pour tout idéal premier* $\mathfrak{p}$ *de* A, *le localisé* $M_\mathfrak{p} = M \otimes_A A_\mathfrak{p}$ *est nul.*

— *Pour tout idéal maximal* $\mathfrak{m}$ *de* A, *le localisé* $M_\mathfrak{m}$ *est nul.*

Soit $M \longrightarrow N \longrightarrow P$ *une suite de trois* A*-modules. Les énoncés suivants sont équivalents :*

— *La suite* $M \longrightarrow N \longrightarrow P$ *est exacte.*

— *Pour tout idéal premier* $\mathfrak{p}$ *de* A, *la suite* $M_\mathfrak{p} \longrightarrow N_\mathfrak{p} \longrightarrow P_\mathfrak{p}$ *est exacte.*

— *Pour tout idéal maximal* $\mathfrak{m}$ *de* A, *la suite* $M_\mathfrak{m} \longrightarrow N_\mathfrak{m} \longrightarrow P_\mathfrak{m}$ *est exacte.*

Démonstration. Pour la première partie, il est clair que $(i) \implies (ii) \implies (iii)$. Supposons maintenant (iii). Soit $x \in M$, on a pour tout $\mathfrak{m}$ maximal $x/1 = 0$ dans $M_\mathfrak{m}$ donc il existe $s \notin \mathfrak{m}$ tel que $sx = 0$. Ainsi l'idéal annulateur de x n'est pas contenu dans $\mathfrak{m}$, et donc il n'est contenu dans aucun idéal maximal, ce qui par le théorème de Krull entraîne que cet idéal annulateur est A tout entier, i.e. $x = 0$.
De même, pour la seconde partie, on a $(i) \implies (ii) \implies (iii)$ car la localisation est un foncteur exact. Supposons alors (iii). Donnons des noms aux flèches :

$$M \xrightarrow{f} N \xrightarrow{g} P.$$

De la suite exacte :

$$\begin{array}{ccccc} & & & & P \\ & & \overset{gf}{\nearrow} & & \uparrow \\ M & \longrightarrow & \operatorname{Im} gf & \longrightarrow & 0 \end{array}$$

on déduit en localisant en $\mathfrak{m}$ maximal une suite exacte :

$$\begin{array}{ccccc} & & & & P_\mathfrak{m} \\ & & \overset{gf=0}{\nearrow} & & \uparrow \\ M_\mathfrak{m} & \longrightarrow & (\operatorname{Im} gf)_\mathfrak{m} & \longrightarrow & 0 \end{array}$$

où la flèche en diagonale est nulle par exactitude de la suite sur les localisés. Par surjectivité de $M_\mathfrak{m} \longrightarrow (\operatorname{Im} gf)_\mathfrak{m}$, on en déduit que l'injection $(\operatorname{Im} gf)_\mathfrak{m} \hookrightarrow P_\mathfrak{m}$ est nulle et donc $(\operatorname{Im} gf)_\mathfrak{m} = 0$, ce pour tout $\mathfrak{m}$. Par la première partie on a donc :

$$gf = 0$$

et donc $\operatorname{Im} f \subseteq \operatorname{Ker} g$ et il reste à voir la seconde inclusion. Pour cela on considère le quotient :

$$H = \operatorname{Ker} g / \operatorname{Im} f$$

et il s'agit de montrer qu'il est nul, autrement dit que pour tout $\mathfrak{m}$ maximal, $H_\mathfrak{m} = 0$. Or on a une suite exacte :

$$0 \longrightarrow \operatorname{Im} f \longrightarrow \operatorname{Ker} g \longrightarrow H \longrightarrow 0$$

qui induit une suite exacte :

$$0 \longrightarrow (\operatorname{Im} f)_\mathfrak{m} \longrightarrow (\operatorname{Ker} g)_\mathfrak{m} \longrightarrow H_\mathfrak{m} \longrightarrow 0$$

et on vérifie facilement par exactitude de la localisation que $(\operatorname{Im} f)_{\mathfrak{m}} = \operatorname{Im}(M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}})$ et $(\operatorname{Ker} g)_{\mathfrak{m}} = \operatorname{Ker}(N_{\mathfrak{m}} \longrightarrow P_{\mathfrak{m}})$ donc la flèche $(\operatorname{Im} f)_{\mathfrak{m}} \longrightarrow (\operatorname{Ker} g)_{\mathfrak{m}}$ est un isomorphisme par l'hypothèse (iii), et ainsi $H_{\mathfrak{m}} = 0$ comme souhaité. □

Comme indiqué précedemment, un morphisme d'anneaux $A \longrightarrow B$ induit une application $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ à laquelle on pense de façon géométrique : on voit $\operatorname{Spec} B$ comme "au dessus" de $\operatorname{Spec} A$, comme en topologie (en théorie des revêtements par exemple). Dans ce contexte il est souvent bon de savoir à quoi ressemble la fibre d'un point de l'espace de dessous, c'est à dire son image réciproque par l'application $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$.

$$\begin{array}{c} \operatorname{Spec} B \\ \downarrow \\ \operatorname{Spec} A \end{array}$$

Proposition 1.22. *Soit $A \xrightarrow{f} B$ un morphisme d'anneaux et $\mathfrak{p} \in \operatorname{Spec} A$ de corps résiduel k. La fibre de $\mathfrak{p}$ par $\operatorname{Spec} B \xrightarrow{f^*} \operatorname{Spec} A$ est un sous-ensemble de $\operatorname{Spec} B$ qui s'identifie à $\operatorname{Spec}(B \otimes_A k)$:*

$$(f^*)^{-1}\mathfrak{p} \cong \operatorname{Spec}(B \otimes_A k).$$

L'identification se fait avec le morphisme d'anneaux $B \longrightarrow B \otimes_A k$ qui induit une application $\operatorname{Spec}(B \otimes_A k) \longrightarrow \operatorname{Spec} B$.
En particulier $\mathfrak{p}$ est dans l'image de f^* si et seulement si l'anneau $B \otimes_A k$ est non nul.

Démonstration. Notons d'abord que :

$$B \otimes_A k = (B \otimes_A A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} k = B_{\mathfrak{p}}/\mathfrak{m}B_{\mathfrak{p}}$$

avec $\mathfrak{m} = \mathfrak{p}_{\mathfrak{p}}$ l'idéal maximal de l'anneau local $A_{\mathfrak{p}}$. De plus l'anneau $B_{\mathfrak{p}}$ est le localisé de B pour la partie multiplicative $S = f(A \setminus \mathfrak{p})$, et donc d'après les propositions 1.19 et 1.17 on a un diagramme commutatif :

$$\begin{array}{ccccc} \operatorname{Spec}(B \otimes_A k) & & & & \\ \sim\downarrow & \searrow & & & \\ V(\mathfrak{m}B_{\mathfrak{p}}) & \subseteq & \operatorname{Spec}(B_{\mathfrak{p}}) & \searrow & \\ & & \sim\downarrow & & \\ & & \{\mathfrak{q} \in \operatorname{Spec} B \mid \mathfrak{q} \cap f(A \setminus \mathfrak{p}) = \emptyset\} & \subseteq & \operatorname{Spec} B \end{array}$$

Par fonctorialité de Spec, la composée des flèches $\operatorname{Spec}(B \otimes_A k) \longrightarrow \operatorname{Spec} B_{\mathfrak{p}} \longrightarrow \operatorname{Spec} B$ est la flèche induite par la composée $B \longrightarrow B_{\mathfrak{p}} \longrightarrow B \otimes_A k$, qui est exactement la flèche canonique $B \longrightarrow B \otimes_A k$. Il reste à vérifier que l'image de $\operatorname{Spec}(B \otimes_A k)$ dans $\operatorname{Spec} B$ est bien $(f^*)^{-1}\mathfrak{p}$. Or le diagramme ci-dessus nous indique que cette image est exactement :

$$\left\{\mathfrak{q} \in \operatorname{Spec} B \mid \mathfrak{q} \cap f(A \setminus \mathfrak{p}) = \emptyset \text{ et } \mathfrak{q}_{\mathfrak{p}} \supseteq \mathfrak{p}_{\mathfrak{p}}B_{\mathfrak{p}}\right\}.$$

La première condition équivaut à $f^*\mathfrak{q} \subseteq \mathfrak{p}$ et la deuxième à $f^*\mathfrak{q} \supseteq \mathfrak{p}$, donc cet ensemble est exactement la fibre de $\mathfrak{p}$ par f^*. □

1.4 Anneaux factoriels

On rappelle la définition et les propriétés de base des anneaux factoriels.

Définition 1.23. *Soit A un anneau intègre. Un élément $x \in A$ est dit irréductible si $x \neq 0$, x n'est pas inversible, et si dès que $x = yz$, on a y ou z inversible. Notons P_A un ensemble d'irréductibles de A deux à deux non associés et tel que tout irréductible de A soit associé à un élément de P_A.*
Un anneau factoriel est un anneau intègre A tel que pour tout $x \in A \setminus \{0\}$ il existe un unique inversible u et une unique application :

$$v : P_A \longrightarrow \mathbb{N}$$

à support fini tel que :

$$x = u \prod_{p \in P_A} p^{v(p)}.$$

On note alors $v_p(x)$ l'entier $v(p)$: c'est la valuation p-adique de x. On pose aussi $v_p(0) = \infty$. Notons que la définition d'un anneau factoriel ne dépend pas du système de représentants P_A choisi.

Dans un anneau factoriel A, la relation $x \mid y$ équivaut à :

$$v_p(x) \leq v_p(y)$$

pour tout $p \in P_A$. Notons K le corps des fractions de A. On peut étendre v_p à K en posant $v_p(x/y) = v_p(x) - v_p(y)$. On vérifie alors facilement que :

$$v_p(ab) = v_p(a) + v_p(b)$$

et

$$v_p(a+b) \geq \min(v_p(a), v_p(b))$$

pour tous $a, b \in K$ et que $a \in A$ si et seulement si $v_p(a) \geq 0$ pour tout $p \in P_A$. La plupart des propriétés usuelles de l'arithmétique, comme le lemme de Gauss, sont encore vraies dans un anneau factoriel et se prouvent à l'aide des valuations p-adiques.

Proposition 1.24. *Tout anneau principal est factoriel.*

Démonstration. Soit A un anneau principal, il est en particulier intègre. On considère P_A comme avant. Rappelons que si $p \in P_A$, alors pA est un idéal maximal : en effet, si $pA \subseteq I$, avec $I = (x)$, on a $x \mid p$ donc x est inversible ou associé à p. Si x est inversible, $I = A$ et si x est associé à p, $I = pA$. De plus, $pA \neq A$ car p n'est pas inversible.
Puisque A est principal, il est noéthérien donc si $x \in A \setminus \{0\}$, il est impossible d'avoir $p^n \mid x$ pour tout n. En effet, si c'est le cas on a $(x) \subseteq (x/p) \subseteq (x/p^2) \subseteq \dots$ et cette suite doit stationner, ce qui est absurde.
Ainsi on peut définir $w_p(x)$ comme le plus grand entier $n \geq 0$ tel que $p^n \mid x$. De même, x n'a qu'un nombre fini de diviseurs dans l'ensemble P_A : sinon on pourrait écrire :

$$(x) \subseteq (x/p_1) \subseteq (x/(p_1 p_2)) \subseteq \dots$$

avec les p_i dans P_A et pour la même raison c'est impossible. Ainsi $w_\bullet(x)$ est à support fini et l'élément :

$$y = \prod_{p \in P_A} p^{w_p(x)}$$

est bien défini. Le lemme de Gauss étant valable dans un anneau principal (il repose sur le théorème de Bézout qui est vrai dans un anneau principal), on a :

$$y \mid x$$

car chaque $p^{w_p(x)}$ divise x et ils sont premiers entre eux. Posons $z = x/y$. Par construction, z n'est divisible par aucun élément de P_A. Par Krull, cela entraîne que z est inversible : si z n'est pas inversible, (z) est contenu dans un idéal maximal (m) et on vérifie facilement que m est irréductible et $m \mid z$. Ainsi on a :

$$x = z \prod_p p^{w_p(x)}$$

ce qui donne la partie "existence". Voyons l'unicité. Si $a \prod_p p^{v_p} = b \prod_p p^{w_p}$ avec $a, b \in A^\times$, alors on a par lemme de Gauss :

$$p^{v_p} \mid p^{w_p}$$

et par symétrie p^{v_p} et p^{w_p} sont associés, ce pour tout p. Ainsi $p^{v_p - w_p}$ est inversible donc $v_p = w_p$ car p n'est pas inversible.
Par intégrité on a alors $a = b$. □

Le gros avantage des anneaux factoriels par rapport aux anneaux principaux est que si A est factoriel, $A[X]$ l'est aussi, comme on va le voir à présent.

Définition 1.25. *Soit A un anneau factoriel de corps de fractions K, on fixe P_A comme avant, et soit $p \in P_A$. Pour tout $P \in K[X]$, on définit la valuation p-adique de P comme le minimum des valuations p-adiques des coefficients de P, et on la note toujours $v_p(P)$.*
Clairement $v_\bullet(P)$ est à support fini et on peut définir :

$$c(P) = \prod_{p \in P_A} p^{v_p(P)} \in K[X]$$

appelé "contenu" du polynôme P.

Lemme 1.26. *Soient $P, Q \in K[X]$, on a :*

$$v_p(PQ) = v_p(P) + v_p(Q)$$

ainsi que :

$$v_p(P+Q) \geq \min(v_p(P), v_p(Q))$$

et :

$$v_p(P) = \infty \iff P = 0.$$

De plus P est à coefficients dans A si et seulement si pour tout $p \in P_A$ on a $v_p(P) \geq 0$.
Notons que par conséquent on a $c(PQ) = c(P)c(Q)$.

Démonstration. On écrit $P = aX^k + U$ et $Q = bX^\ell + V$ avec U sans monôme de la forme X^k, V sans monôme de la forme X^ℓ, et :

$$v_p(a) = v_p(P)$$

et

$$v_p(b) = v_p(Q).$$

Ainsi :

$$PQ = abX^{k+\ell} + bX^\ell U + aX^k V + UV$$

de sorte que le coefficient devant $X^{k+\ell}$ est exactement ab et d'après les propriétés de v_p sur K, les coefficients de $bX^\ell U + aX^k V + UV$ ont tous une valuation p-adique au moins égale à celle de ab. On a donc bien $v_p(PQ) = v_p(ab) = v_p(a) + v_p(b) = v_p(P) + v_p(Q)$. Le reste est élémentaire. □

Définition 1.27. *Un polynôme $P \in A[X]$ est dit primitif si pour tout $p \in P_A$ on a $v_p(P) = 0$. En particulier tout polynôme unitaire à coefficients dans A est primitif.*

Le lemme suivant, attribué à Gauss, est fondamental en arithmétique.

Lemme 1.28. *(Gauss) Soit A un anneau factoriel et soit $P \in A[X]$ unitaire et $Q \in K[X]$ un diviseur de P dans $K[X]$ qui est aussi unitaire. Alors P est à coefficients dans A.*

Démonstration. On écrit $P = QR$ avec $R \in K[X]$. Ainsi pour tout $p \in P_A$ on a :

$$0 = v_p(P) = v_p(Q) + v_p(R)$$

et $v_p(R) \leq 0$ car R est nécessairement unitaire. Ainsi $v_p(Q) = -v_p(R) \geq 0$ donc $Q \in A[X]$. □

Le résultat suivant est très utile car il permet de ramener l'étude de l'irréductibilité dans $A[X]$ à l'étude de l'irréductibilité dans l'anneau principal $K[X]$, qui est bien plus facile.

Proposition 1.29. *Soit $P \in A[X]$ primitif. Alors P est irréductible dans l'anneau $A[X]$ si et seulement si il l'est dans l'anneau $K[X]$.*

Démonstration. Si $P = QR$ avec $Q, R \in A[X]$ non inversibles, alors on a aussi $Q, R \in K[X]$ et donc P n'est pas irréductible dans $K[X]$. Réciproquement si $P = QR$ avec $Q, R \in K[X]$ non inversibles, puisque P est primitif on a :

$$1 = c(P) = c(Q)c(R)$$

et donc :

$$P = \frac{P}{1} = \frac{QR}{c(Q)c(R)} = \frac{Q}{c(Q)}\frac{R}{c(R)}$$

et $Q/c(Q)$ est clairement à coefficients dans A et primitif (il suffit de calculer ses valuations p-adiques et de constater qu'elles sont nulles), et de même pour $R/c(R)$ donc P n'est pas irréductible dans $A[X]$.

□

On en déduit le théorème annoncé plus tôt : si A est factoriel alors $A[X]$ aussi.

Théorème 1.30. *Soit A un anneau factoriel de corps des fractions K. L'anneau $A[X]$ est factoriel et les éléments irréductibles de $A[X]$ sont d'une part les éléments irréductibles de A et d'autre part les polynômes primitifs irréductibles dans $K[X]$.*

Démonstration. Notons que les inversibles de $A[X]$ sont exactement les inversibles de A. Il est clair que les éléments irréductibles de A restent irréductibles dans $A[X]$ car leurs seuls diviseurs sont des polynômes constants. De plus, par la proposition 1.29, les polynômes primitifs irréductibles dans $K[X]$ sont irréductibles dans $A[X]$.
Réciproquement, si P est un élément irréductible de $A[X]$, ou bien il est constant auquel cas il est clairement irréductible dans A, ou bien il n'est pas constant et de l'écriture $P = c(P) \times P/c(P)$ on obtient que $c(P) = 1$ et donc que P est primitif, et irréductible dans $K[X]$ d'après la proposition 1.29.
Soit maintenant $P \in A[X]$ non nul. Puisque $K[X]$ est principal et donc factoriel, on peut écrire :

$$P = \lambda Q_1 \dots Q_r$$

avec $\lambda \in A \setminus \{0\}$ le coefficient dominant de A et les Q_i des polynômes unitaires de $K[X]$ irréductibles. On a alors $c(\lambda)c(Q_1)\dots c(Q_r) = c(P)$ et :

$$P/c(P) = \lambda/c(\lambda) \prod_i \frac{Q_i}{c(Q_i)}.$$

Les $Q_i/c(Q_i)$ sont alors dans $A[X]$, sont primitifs, et donc sont irréductibles dans $A[X]$. En multipliant par $c(P)$ de chaque côté et en utilisant le fait que A est factoriel, on obtient une décomposition de P en produit d'irréductibles de $A[X]$. Il reste à voir l'unicité de la décomposition. On fixe P_A comme avant et I un système de représentants des polynômes primitifs irréductibles à association près. On pose :

$$P_{A[X]} = P_A \cup I$$

qui est donc un système de représentants des irréductibles de $A[X]$. Supposons alors que :

$$u \prod_{p \in P_A} p^{v_p} \prod_{P \in I} P^{v_P} = v \prod_{p \in P_A} p^{w_p} \prod_{P \in I} P^{w_P}$$

avec $u, v \in A^\times$. En prenant les contenus, puisque les P sont primitifs, on obtient :

$$\prod_{p \in P_A} p^{v_p} = \prod_{p \in P_A} p^{w_p}$$

et donc $v_p = w_p$ puisque A est factoriel. On simplifie et on obtient :

$$u \prod_{P \in I} P^{v_P} = v \prod_{p \in I} P^{w_P}$$

et on conclut avec la factorialité de $K[X]$. □

Notons que la notation $v_p(P)$ définie précedemment est cohérente avec la valuation p-adique de P dans l'anneau factoriel $A[X]$.

1.5 Morphismes finis, morphismes entiers

Le but de cette partie est d'étudier des propriétés de base sur les morphismes d'anneaux qui seront omniprésentes en arithmétique.

Définition 1.31. *Soit $A \longrightarrow B$ un morphisme d'anneaux, ou de façon équivalente soit B une A-algèbre.*
Ce morphisme est dit fini si B est un A-module de type fini. On dit aussi que B est une A-algèbre finie.
Le morphisme $A \longrightarrow B$ est dit de type fini si il existe $b_1, \dots, b_n \in B$ tels que $B = A[b_1, \dots, b_n]$.
Un élément $b \in B$ est dit entier sur A s'il existe $P \in A[X]$ unitaire tel que $P(b) = 0$. On dit que B est entier sur A, ou encore que $A \longrightarrow B$ est un morphisme entier, si tout élément de B est entier sur A.

Clairement, un morphisme fini est de type fini et on va voir à présent qu'un morphisme fini est aussi entier.

Lemme 1.32. *Soit M un A-module de type fini et f un endomorphisme de M. Il existe alors $P \in A[X]$ unitaire tel que $P(f) = 0$.*

Démonstration. Puisque M est de type fini, il existe un morphisme surjectif de A-modules $A^n \longrightarrow M$. On a alors un diagramme commutatif :

$$\begin{array}{ccc} A^n & \overset{g}{\dashrightarrow} & A^n \\ \downarrow & & \downarrow \\ M & \xrightarrow[f]{} & M \end{array}$$

où l'existence d'une telle flèche g est assurée par la projectivité de A^n (ou plus simplement il suffit de relever via $A^n \longrightarrow B$ les n images des générateurs canoniques de A^n via $A^n \longrightarrow B \xrightarrow{f} B$). Par Cayley-Hamilton (en voyant g comme une matrice $n \times n$ à coefficients dans A), il existe un polynôme unitaire $P \in A[X]$ qui annule g. On a alors le diagramme commutatif suivant :

$$\begin{array}{ccc} A^n & \overset{P(g)=0}{\dashrightarrow} & A^n \\ \downarrow & & \downarrow \\ M & \xrightarrow[P(f)]{} & M \end{array}$$

et par surjectivité de $A^n \longrightarrow B$ on a donc $P(f) = 0$. □

Proposition 1.33. *Un morphisme fini est entier.*

Démonstration. Si $A \longrightarrow B$ est fini, B est un A-module de type fini donc pour tout $b \in B$, par le lemme précédent, l'endomorphisme de multiplication par b est annulé par un $P \in A[X]$ unitaire et donc $P(b) = 0$ (en appliquant la relation à l'élément 1 de B). □

Lemme 1.34. *La composition de deux morphismes finis (resp. de type fini) est un morphisme fini (resp. de type fini).*

Démonstration. Soient $A \xrightarrow{f} B \xrightarrow{g} C$ deux morphismes. Si les deux sont finis, on prend $b_1, \dots, b_m$ des générateurs de B comme A-module et $c_1, \dots, c_n$ des générateurs de C comme B-module et on vérifie facilement que les $b_i c_j$ génèrent C comme A-module. C'est exactement la même idée pour des morphismes de type fini. □

Lemme 1.35. *Soit $A \longrightarrow B$ un morphisme et $b \in B$ entier sur A. Alors $A[b]$ est fini sur A.*

Démonstration. Puisque b est entier, on a :

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

avec les a_i dans A. Il est alors immédiat de vérifier que les éléments $1, b, \dots, b^{n-1}$ engendrent $A[b]$ comme A-module grâce à la relation précédente. □

Définition 1.36. *Soit $A \longrightarrow B$ un morphisme d'anneaux. L'ensemble des éléments de B qui sont entiers sur A est appelé clôture intégrale de A dans B.*
On appelle d'ailleurs entier algébrique un nombre complexe qui est entier sur $\mathbb{Z}$, et on note souvent $\overline{\mathbb{Z}}$ la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{C}$.

Proposition 1.37. *La clôture intégrale de A dans B est un sous-anneau de B entier sur A. C'est même le sous-anneau de B entier sur A maximal, au sens où tout sous-anneau de B entier sur A est contenu dans la clôture intégrale.*

Démonstration. Soient x, y entiers sur A. Alors x est entier sur $A[y]$ donc les morphismes $A \longrightarrow A[y]$ et $A[y] \longrightarrow A[x,y]$ sont finis d'après le lemme précédent. Ainsi leur composition est un morphisme fini donc entier et donc tout élément de $A[x,y]$ est entier sur A, en particulier xy et $x - y$. De plus 0 et 1 sont clairement entiers sur A. La maximalité est claire. □

Théorème 1.38. *Un morphisme est fini si et seulement si il est entier et de type fini.*

Démonstration. Il reste à montrer que si $A \longrightarrow B$ est entier et de type fini alors il est fini. Prenons $b_1, \dots, b_n \in B$ tels que :

$$B = A[b_1, \dots, b_n].$$

Puisque b_1 est entier sur A, $A[b_1]$ est fini sur A. Ensuite b_2 est entier sur $A[b_1]$ donc $A[b_1, b_2]$ est fini sur $A[b_1]$ et donc sur A car la composition de deux morphismes fini est un morphisme fini, et ainsi de suite. □

Corollaire 1.39. *La composition de deux morphismes entiers est un morphisme entier.*

Démonstration. Soient $A \longrightarrow B$ et $B \longrightarrow C$ deux morphismes entiers et $c \in C$. Puisque c est entier sur B, il existe $P \in B[X]$ unitaire qui annule c. On considère B' le sous-anneau de B engendré par les coefficients de P. B' est un anneau entier et de type fini sur A donc fini sur A par le théorème précédent 1.38. Or c est entier sur B' donc $B'[c]$ est fini sur B' qui est fini sur A donc $B'[c]$ est fini sur A et donc entier sur A. Ainsi c est entier sur A. □

Définition 1.40. *Soit B un anneau et $A \subseteq B$ un sous-anneau. On dit que A est intégralement clos dans B si la clôture intégrale de A dans B est exactement A, autrement dit si tout élément de B entier sur A est dans A.*

Proposition 1.41. *Si A est un sous-anneau de B, la clôture intégrale de A dans B est intégralement close dans B. Autrement dit la clôture intégrale de la clôture intégrale de A est la clôture intégrale de A.*

Démonstration. Notons $\overline{A}$ cette clôture intégrale. Soit b entier sur $\overline{A}$, alors $\overline{A}[b]$ est entier sur $\overline{A}$ qui est entier sur A donc $\overline{A}[b]$ est entier sur A et b est entier sur A. □

Dans le cas des anneaux intègres, il existe une notion absolue d'anneau intégralement clos.

Définition 1.42. *Un anneau intègre A est intégralement clos s'il est intégralement clos dans K le corps des fractions de A, autrement dit si tout élément de K entier sur A est dans A.*

Voici un exemple fondamental d'anneaux intégralement clos.

Lemme 1.43. *Un anneau factoriel A est intégralement clos.*

Démonstration. Notons K le corps des fractions de A. Soit $x \in K$ tel que $x^n = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ avec $a_i \in A$. Puisque A est factoriel, on peut écrire $x = a/b$ avec a et b des éléments de A premiers entre eux. On a donc :

$$a^n = b^n a_0 + a_1 b^{n-1} a + \cdots + a_{n-1} b a^{n-1}$$

donc b divise a^n et par le lemme de Gauss, ceci entraîne que b est inversible et $x \in A$. □

Ce résultat est très utile en pratique, en voici un exemple d'application.

Corollaire 1.44. *Le nombre $\sqrt{2}$ est irrationnel, et plus généralement si $n \in \mathbb{N}$ et $\alpha \in \mathbb{Q}$, alors n^α est rationnel si et seulement si c'est un entier.*

Démonstration. Puisque $\mathbb{Z}$ est factoriel, il est intégralement clos. Or $\sqrt{2}$ est entier sur $\mathbb{Z}$ car annulé par $X^2 - 2$ et s'il était dans $\mathbb{Q}$ (qui est le corps des fractions de $\mathbb{Z}$), il serait dans $\mathbb{Z}$, ce qui n'est clairement pas le cas.
De même, n^α est entier sur $\mathbb{Z}$ car si $\alpha = p/q$, $X^q - n^p$ annule n^α et donc il est rationnel si et seulement si il est entier. □

On peut définir le polynôme minimal d'un élément entier sur A.

Définition 1.45. *Soit $A \longrightarrow B$ un morphisme d'anneaux et $b \in B$ entier sur A. On définit le polynôme minimal de b, π_b, comme le polynôme unitaire dans $A[X]$ annulant b de degré minimal. Pour que cela ait du sens il faut (et il suffit) que A ne soit pas l'anneau nul.*

Dans le cas d'un anneau factoriel, cette notion est similaire à celle de polynôme minimal d'un élément algébrique sur le corps des fractions.

Proposition 1.46. *Soit A un anneau factoriel de corps des fractions K et L/K une extension de corps. Soit $x \in L$ entier sur A. Les polynômes minimaux de x sur A et sur K sont égaux, aussi la notation π_x n'est pas ambigue, et l'idéal de $A[X]$ annulateur de x est principal, engendré par π_x.*

Démonstration. Notons P le polynôme minimal de x sur A et Q le polynôme minimal de x sur K. On considère la division euclidienne de P par Q dans l'anneau euclidien $K[X]$:

$$P = MQ + R$$

avec $\deg R < \deg Q$. Comme $P(x) = Q(x) = 0$, on a $R(x) = 0$ et par minimalité du degré cela entraîne que $R = 0$. Ainsi Q divise P et par le lemme de Gauss 1.28, puisque P et Q sont unitaires, Q est à coefficients dans A. Or $Q(x) = 0$ donc par minimalité du degré P et Q ont le même degré, et puisqu'ils sont unitaires et que l'un divise l'autre, on a bien :

$$P = Q.$$

Notons I l'idéal annulateur de x dans $A[X]$. Clairement I contient P et si $U \in I$, la division euclidienne par $Q = P$ dans $K[X]$ montre que $Q \mid U$ avec le même raisonnement qu'avant. Ainsi $P \mid U$ et $c(U/P) = c(U)/c(P) = c(U) \in A$ car P est unitaire, donc $U/P \in A[X]$, et $U \in (P)$. □

Le théorème suivant est un cas particulier d'une propriété importante des morphismes en géométrie algébrique appelée *montée* ou *going up* en anglais. Il existe aussi une propriété de descente mais nous n'en auront pas besoin ici.

Théorème 1.47. *(Lemme de montée) Soit $A \xrightarrow{f} B$ un morphisme d'anneaux entier et injectif. Alors l'application induite sur les spectres :*

$$\begin{array}{c} \operatorname{Spec} B \\ \downarrow \\ \operatorname{Spec} A \end{array}$$

est surjective. Autrement dit, pour tout idéal premier $\mathfrak{p}$ de A, il existe un idéal premier $\mathfrak{q}$ de B dit "au dessus" de A, au sens où $f^*\mathfrak{q} = \mathfrak{p}$ (ici $f^*\mathfrak{q}$ est une notation pour $f^{-1}(\mathfrak{q})$).

Démonstration. Soit $\mathfrak{p}$ un idéal premier de A. D'après la proposition 1.22, la fibre de $\mathfrak{p}$ par f^* est :

$$(f^*)^{-1}(\mathfrak{p}) = \{\mathfrak{q} \in \operatorname{Spec} B \mid f^*\mathfrak{q} = \mathfrak{p}\} \cong \operatorname{Spec}(B \otimes_A k)$$

avec k le corps résiduel de A en $\mathfrak{p}$ (voir 1.18). Il suffit donc de montrer que $\operatorname{Spec}(B \otimes_A k) \neq \emptyset$, ce qui, par le théorème de Krull équivaut à montrer que $B \otimes_A k \neq 0$. Or on a :

$$B \otimes_A k = (B \otimes_A A_\mathfrak{p}) \otimes_{A_\mathfrak{p}} k = B_\mathfrak{p} \otimes_{A_\mathfrak{p}} k$$

et si ce module est nul, alors $B_\mathfrak{p} = \mathfrak{m}B_\mathfrak{p}$ avec $\mathfrak{m}$ l'idéal maximal de l'anneau local $A_\mathfrak{p}$. Si $B_\mathfrak{p}$ était fini sur $A_\mathfrak{p}$ on pourrait directement appliquer le lemme de Nakayama et conclure que $B_\mathfrak{p} = 0$. En général, de $B_\mathfrak{p} = \mathfrak{m}B_\mathfrak{p}$, on peut écrire :

$$1 = \sum_i m_i b_i$$

avec $m_i \in \mathfrak{m}$ et $b_i \in B$ dans l'anneau $B_\mathfrak{p}$. Ainsi l'anneau $B' = A[(b_i)]$ est entier et de type fini sur A donc fini sur A, et on a encore $B'_\mathfrak{p} = \mathfrak{m}B'_\mathfrak{p}$ puisque les b_i sont dans $B'_\mathfrak{p}$, et cette fois-ci le lemme de Nakayama 1.15 s'applique et :

$$B'_\mathfrak{p} = 0.$$

Or $A \subseteq B' \subseteq B'_\mathfrak{p} \subseteq L$ donc $A = 0$ et ceci contredit l'existence même de l'idéal premier $\mathfrak{p}$ dont on est parti (c'est ici que l'injectivité de $A \longrightarrow B$ intervient). □

1.6 Dualité et modules projectifs de type fini

On fixe A un anneau et M un A-module. Le A-module *dual* de M, noté $M^\vee$ est le A-module des morphismes de M vers A :

$$M^\vee = \mathrm{Hom}_A(M, A)$$

La dualité pour les A-modules ne fonctionne pas bien en général. Les bons candidats sur lesquels elle s'applique sont les modules *projectifs de type fini*.
La proposition 1.48 et le théorème 1.50 sont des résultats intéressants mais pas indispensables pour la suite. Le lecteur pourra se contenter du théorème 1.51 et du théorème 1.53.

Proposition 1.48. *Si M est un A-module projectif de type fini, alors pour tout A-module N on a un isomorphisme canonique de A-modules :*

$$M^\vee \otimes_A N \cong \mathrm{Hom}_A(M, N)$$

qui envoie $\alpha \otimes n$ sur $m \mapsto \alpha(m)n$. De plus $M^\vee$ est encore projectif de type fini et on a un isomorphisme canonique de bidualité :

$$(M^\vee)^\vee \cong M$$

via $m \mapsto \alpha \mapsto \alpha(m)$.

Démonstration. M étant projectif de type fini, il existe M' tel que $M \oplus M' = A^k$. On a donc une suite exacte *scindée* :

$$0 \longrightarrow M \longrightarrow A^k \longrightarrow M' \longrightarrow 0$$

Le morphisme $M^\vee \otimes_A N \xrightarrow{\varphi} \mathrm{Hom}_A(M, N)$ qui envoie $\alpha \otimes n$ sur $m \mapsto \alpha(m)n$ est *naturel* en M et en N donc le diagramme suivant commute (et les lignes sont exactes et scindées) :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_A(M', N) & \longrightarrow & \mathrm{Hom}_A(A^k, N) & \longrightarrow & \mathrm{Hom}_A(M, N) & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} & & \\
0 & \longrightarrow & M'^\vee \otimes_A N & \longrightarrow & (A^k)^\vee \otimes_A N & \longrightarrow & M \otimes_A N & \longrightarrow & 0
\end{array}$$

Le morphisme du milieu est un isomorphisme (il se factorise par N^k) donc le morphisme de gauche est *injectif* et celui de droite est *surjectif*. En inversant les rôles de M et M' on obtient que φ est un isomorphisme pour M projectif de type fini.
Ensuite, voyons que le morphisme de bidualité $M \xrightarrow{\eta} (M^\vee)^\vee$ est un isomorphisme. Encore une fois, on a un diagramme commutatif à lignes exactes scindées :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M^{\vee\vee} & \longrightarrow & (A^k)^{\vee\vee} & \longrightarrow & (M')^{\vee\vee} & \longrightarrow & 0 \\ & & \eta\uparrow & & \eta\uparrow & & \eta\uparrow & & \\ 0 & \longrightarrow & M & \longrightarrow & A^k & \longrightarrow & M' & \longrightarrow & 0 \end{array}$$

et la flèche du milieu est un isomorphisme, donc on conclut comme précedemment que η est un isomorphisme dès que M est projectif de type fini. De plus, de $M \otimes M' \cong A^k$ on obtient $M^\vee \otimes M'^\vee \cong A^k$ donc $M^\vee$ est projectif de type fini. □

La remarque suivante ne sera pas utilisée dans la suite.

Remarque 1.49. Si M est projectif de type fini, on peut ainsi identifier $M^\vee \otimes M$ à $\mathrm{End}_A(M)$. Or on dispose d'un morphisme naturel en M : $M^\vee \otimes M \longrightarrow A$ qui envoie $\alpha \otimes m$ sur $\alpha(m)$. Ce morphisme, après identification, donne une forme linéaire sur $\mathrm{End}_A(M)$, natulle en M, appelée *trace*. On retrouve ainsi la notion usuelle de trace pour un A-module libre de type fini.

La dualité permet de nouvelles caractérisations pour les modules projectifs de type fini. Le théorème suivant est parfois appelé *théorème de la base duale*.

Théorème 1.50. *Soit M un A-module de type fini. Les énoncés suivants sont équivalents :*

(i) M est projectif.

(ii) Pour tout A-module N, le morphisme naturel $M^\vee \otimes N \longrightarrow \mathrm{Hom}_A(M,N)$ est un isomorphisme.

(iii) Le morphisme naturel $M^\vee \otimes M \longrightarrow \mathrm{Hom}_A(M,M)$ est surjectif.

(iv) Il existe $e_1,\dots,e_n \in M$ et $\alpha_1,\dots,\alpha_n \in M^\vee$ tels que pour tout $x \in M$:

$$x = \sum_i \alpha_i(x) e_i$$

Démonstration. La proposition 1.48 indique que (i) implique (ii), et clairement (ii) implique (iii). Ensuite (iii) implique (iv) en prenant $\sum_i \alpha_i \otimes e_i$ un antécédent de id_M. Enfin, montrons que (iv) implique (i) : on se donne $e_1,\dots,e_n$ et $\alpha_1,\dots,\alpha_n$ comme dans l'énoncé du théorème. Soit alors $X \xrightarrow{f} M \longrightarrow 0$ un morphisme surjectif. Il s'agit de construire une section pour f. Pour cela, prenons x_i un antécédent de e_i par f et posons :

$$s(m) = \sum_i \alpha_i(m) x_i$$

pour $m \in M$. Cela définit bien une section de f. □

Lorsque M n'est pas de type fini, on a tout de même la caractérisation suivante :

Théorème 1.51. *Soit M un A-module. Les énoncés suivants sont équivalents :*

(i) *M est projectif.*

(ii) *Il existe I un ensemble, $(e_i)_{i\in I}$ une famille d'éléments de M, $(\alpha_i)_{i\in I}$ une famille d'éléments de $M^\vee$ tels que pour tout $x \in M$ on ait $\alpha_i(x) = 0$ pour presque tout $i \in I$ et :*

$$x = \sum_i \alpha_i(x) e_i$$

Démonstration. Supposons M projectif, il existe alors M' tel que $M \oplus M' = A^{(I)}$ où $A^{(I)}$ désigne le A-module libre généré par l'ensemble I. Pour tout $i \in I$, on note α_i la composition de la i-ème projection canonique avec l'inclusion $M \hookrightarrow A^{(I)}$:

$$M \hookrightarrow A^{(I)} \longrightarrow A$$

Ainsi α_i est une forme linéaire sur M. On note $p : A^{(I)} \longrightarrow M$ la projection sur le facteur direct M, et on a pour tout $x \in M$:

$$x = p\left(\sum_i \alpha_i(x) f_i\right) = \sum_i \alpha_i(x) p(f_i)$$

avec (f_i) la base canonique de $A^{(I)}$ (la somme étant à support fini). On pose alors $e_i = p(f_i)$ et on a bien montré (ii).

Réciproquement, donnons nous (e_i) et (α_i) comme dans (ii) et soit $X \xrightarrow{f} M \longrightarrow 0$ un morphisme surjectif. On construit une section comme dans la preuve de 1.50 en choisissant x_i un antécédent de e_i et en posant pour tout $m \in M$:

$$s(m) = \sum_i \alpha_i(m) x_i$$

qui définit une section de f. □

Théorème 1.52. *Soit A un anneau, B une A-algèbre plate (au sens où la tensorisation par B au dessus de A est un foncteur exact) et M un A-module de présentation finie. Alors pour tout A-module N, le morphisme naturel (en M et N) :*

$$\mathrm{Hom}_A(M,N) \otimes_A B \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$$

est un isomorphisme de B-modules.

Démonstration. Appellons $\eta_{M,N}$ ce morphisme. Précisons comment il s'obtient : on a un morphisme de A-modules $\mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$ qui envoie f sur $f \otimes \mathrm{id}_B$. Ce morphisme induit, par propriété universelle d'extension des scalaires, un morphisme :

$$\eta_{M,N} : \mathrm{Hom}_A(M,N) \otimes_A B \longrightarrow \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B)$$

Pour abréger on le notera aussi η. Puisque M est de présentation finie, il existe une suite exacte de la forme :

$$A^p \longrightarrow A^q \longrightarrow M \longrightarrow 0$$

Par platitude de B on obtient les deux suites exactes suivantes :

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_A(M,N)\otimes_A B & \longrightarrow & \mathrm{Hom}_A(A^q,N)\otimes_A B & \longrightarrow & \mathrm{Hom}_A(A^p,N)\otimes_A B \\
 & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \eta} \\
0 & \longrightarrow & \mathrm{Hom}_B(M\otimes_A B, N\otimes_A B) & \longrightarrow & \mathrm{Hom}_B(A^q\otimes_A B, N\otimes_A B) & \longrightarrow & \mathrm{Hom}_B(A^p\otimes_A B, N\otimes_A B)
\end{array}$$

Les carrés de ce diagramme commutent par naturalité de η. Les deux derniers morphismes $\eta_{A^q,N}$ et $\eta_{A^p,N}$ sont des isomorphismes (en effet $\mathrm{Hom}_A(A^q,N)\otimes_A B$ s'identifie à $N^q\otimes_A B$ et $\mathrm{Hom}_B(A^q\otimes_A B, N\otimes_A B)$ aussi). On en déduit que le premier morphisme est aussi un isomorphisme. □

On rappelle enfin le résultat suivant sur les modules projectifs.

Théorème 1.53. *Soit A un anneau et M un A-module de type fini.*

- *Si A est local, alors M est projectif si et seulement si M est libre.*
- *Si A est noéthérien, alors M est projectif si et seulement si pour tout $\mathfrak{p}$ un idéal premier (ou de manière équivalente, maximal) de A, $M_\mathfrak{p}$ est libre sur l'anneau local $A_\mathfrak{p}$.*

Démonstration. Supposons A local. Si M est libre, il est projectif. Supposons maintenant M projectif et notons $\mathfrak{m}$ l'unique idéal maximal de A et $k = A/\mathfrak{m}$ le corps résiduel de A. L'espace vectoriel $V = M\otimes_A k$ est de dimension finie donc il admet une base $(\overline{e_1},\dots,\overline{e_n})$ avec $e_i\in M$, et on peut considérer l'application $\varphi : A^n \longrightarrow M$ qui correspond à la famille $(e_1,\dots,e_n)$:

$$\begin{array}{ccccccccc}
 & & & & A^n & \xrightarrow{\varphi} & M & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & k^n & \xrightarrow{\varphi\otimes id_k} & V & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

On va montrer que φ est un isomorphisme. Notons N l'image de φ. On a $N/\mathfrak{m}N = V$ car c'est un sous-espace de V qui contient les $\overline{e_i}$. Ainsi $N+\mathfrak{m}M = M$. Or M est de type fini et A est local, donc par le lemme de Nakayama on a $N = M$ et φ est surjective. M étant projectif, φ admet une section s. Notons K le noyau de φ. La suite exacte *scindée* $0\longrightarrow K\longrightarrow A^n\longrightarrow M\longrightarrow 0$ induit donc une suite exacte *scindée* :

$$0\longrightarrow K\otimes_A k\longrightarrow k^n\longrightarrow V\longrightarrow 0$$

donc $K\otimes_A k = 0$ (car $k^n\longrightarrow V$ est injective) et par le lemme de Nakayama, puisque K est de type fini comme facteur direct de A^n, on a $K = 0$ et φ est injective. M est donc libre.

À présent, supposons A noéthérien. Si M est projectif, ses localisés le sont aussi, et par ce qui précède ils sont donc libres. Supposons que pour tout $\mathfrak{p}$ maximal $M_\mathfrak{p}$ est libre. Soit $X\longrightarrow Y\longrightarrow 0$ un morphisme surjectif de A-modules. Il s'agit de montrer que le morphisme induit :

$$\mathrm{Hom}_A(M,X)\longrightarrow \mathrm{Hom}_A(M,Y)$$

est surjectif. Il suffit de vérifier que pour tout $\mathfrak{p}$ maximal, le morphisme de $A_\mathfrak{p}$-modules :

$$\mathrm{Hom}_A(M,X)_\mathfrak{p} \longrightarrow \mathrm{Hom}_A(M,Y)_\mathfrak{p}$$

est surjectif. Or A étant noéthérien, M est de présentation finie donc on a un isomorphisme naturel en X entre $\mathrm{Hom}_A(M,X)_\mathfrak{p}$ et $\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p},X_\mathfrak{p})$ (théorème 1.52). Or $\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p},X_\mathfrak{p}) \longrightarrow \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p},Y_\mathfrak{p})$ est surjectif car $M_\mathfrak{p}$ est projectif comme $A_\mathfrak{p}$-module. Grâce à l'isomorphisme naturel, le morphisme $\mathrm{Hom}_A(M,X)_\mathfrak{p} \longrightarrow \mathrm{Hom}_A(M,Y)_\mathfrak{p}$ est donc aussi surjectif.

□

1.7 Résultant et discriminant de polynômes

On fixe A un anneau commutatif. Pour tout entier $n \geq 0$, on note $A_{<n}[X]$ le A-module libre de rang n des polynômes de $A[X]$ de degré au plus $n-1$.

Définition 1.54. *Soient $P,Q \in A[X]$ deux polynômes de degrés respectifs au plus $p \geq 0$ et $q \geq 0$, avec $p+q \geq 1$. On définit leur (p,q)-résultant, ou plus simplement résultant si $p = \deg P$ et $q = \deg Q$ comme le déterminant de la matrice de l'application linéaire :*

$$\varphi : A_{<p}[X] \oplus A_{<q}[X] \longrightarrow A_{<p+q}[X]$$

qui à (U,V) associe $UQ+VP$, dans les bases canoniques
$(1,0),(X,0),\ldots,(X^{p-1},0),(0,1),(0,X),\ldots,(0,X^{q-1})$ et $1,X,\ldots,X^{p+q-1}$. Ce déterminant est noté :

$$\mathrm{Res}(P,Q) \in A$$

ou $\mathrm{Res}_{p,q}(P,Q)$. Dans le cas où $Q = P'$, on définit le discriminant d'un polynôme unitaire P de degré $p \geq 1$ comme :

$$\mathrm{Disc}(P) = (-1)^{\binom{p}{2}} \mathrm{Res}_{p,p-1}(P,P') \in A.$$

La convention de signe permettra d'avoir une définition cohérente avec le discriminant d'un corps de nombres.
Si P n'est pas unitaire, de coefficient dominant a_p on définit aussi son discriminant comme :

$$\mathrm{Disc}(P) = \frac{(-1)^{\binom{p}{2}}}{a_p} \mathrm{Res}_{p,p-1}(P,P') \in A[1/a_p].$$

Cette définition vaut même si P' n'est pas de degré $p-1$.

Remarque 1.55. L'intérêt historique du résultant est de procéder à des éliminations dans un système d'équations polynomiales à plusieurs variables.
Notons M la matrice de φ dans les bases canoniques citées plus haut, de sorte que :

$$\mathrm{Res}(P,Q) = \det(M).$$

La formule de Cramer donne :

$$MM^\sharp = M^\sharp M = \mathrm{Res}(P,Q)I$$

avec I la matrice identité et $M^\sharp$ une matrice carrée à coefficients dans A. En particulier, en appliquant cela au polynôme 1 :

$$\mathrm{Res}(P,Q) = \varphi(\psi(1))$$

avec $\psi : A_{<p+q}[X] \longrightarrow A_{<p}[X] \oplus A_{<q}[X]$ l'application linéaire représentée par $M^\sharp$.
Ainsi il existe toujours (U,V) avec $\deg U < p$ et $\deg V < q$ tels que :

$$UQ + VP = \mathrm{Res}(P,Q) \in A.$$

Si l'anneau A est intègre et si P et Q sont premiers entre eux dans $\mathrm{Frac}(A)[X]$, le théorème suivant assure que ce résultant est non nul. Ainsi, si $A = K[X_1,\dots,X_n]$, $A[X] = K[X_1,\dots,X_{n+1}]$ avec K un corps, le résultant permet d'éliminer la variable X^{n+1} puisque $\mathrm{Res}(P,Q) \in K[X_1,\dots,X_n]$.
Cela permet de donner une preuve du théorème de Bézout par exemple.

On liste ici les propriétés importantes du résultant et du discriminant que l'on utilisera.

Théorème 1.56. *Soit K un corps, Ω un corps algébriquement clos contenant K et $P,Q \in K[X]$ de degrés respectifs $p \geq 0$ et $q \geq 0$ avec $p+q \geq 1$. On écrit :*

$$P = \alpha \prod_{i=1}^{p} (X - x_i)$$

et

$$Q = \beta \prod_{j=1}^{q} (X - y_j)$$

dans $\Omega[X]$. On a alors les propriétés suivantes :

- *Les polynômes P et Q sont premiers entre eux si et seulement si $\mathrm{Res}(P,Q) \neq 0$.*
- *On a :*
$$\mathrm{Res}(P,Q) = (-1)^{pq}\,\mathrm{Res}(Q,P).$$
- *On peut exprimer le résultant de la façon suivante :*
$$\mathrm{Res}(P,Q) = \alpha^q \det(\mu_Q \mid K[X]/(P))$$
où $\mu_Q \mid K[X]/(P)$ désigne l'endomorphisme de multiplication par $\overline{Q}$ dans la K-algèbre de dimension p qu'est $K[X]/(P)$.
- *Pour tout R de degré $r \geq 0$, on a :*
$$\mathrm{Res}(P,QR) = \mathrm{Res}(P,Q)\,\mathrm{Res}(P,R)$$
- *On dispose enfin des formules explicites suivantes :*
$$\mathrm{Res}(P,Q) = \alpha^q \beta^p \prod_{i,j} (x_i - y_j) = \alpha^q \prod_i Q(x_i) = (-1)^{pq} \beta^p \prod_j P(y_j).$$

Supposons maintenant $p \geq 1$. Ce qui précède donne directement les faits suivants sur le discriminant :

— *P est séparable si et seulement si* $\mathrm{Disc}(P) \neq 0$.

— *On dispose de la formule explicite suivante :*

$$\mathrm{Disc}(P) = (-1)^{\binom{p}{2}} \alpha^{2p-2} \prod_{i \neq j} (x_i - x_j) = \alpha^{2p-2} \prod_{i<j} (x_j - x_i)^2$$

Démonstration. Par le lemme de Gauss, si P et Q sont premiers entre eux alors φ est injective car P et Q sont exactement de degrés p et q et donc $\mathrm{Res}(P,Q) \neq 0$. Si le résultant est non nul, φ est surjective et par le théorème de Bézout, puisqu'il existe U, V avec $UQ + VP = 1$, P et Q sont premiers entre eux.
La deuxième formule s'obtient par antisymétrie du déterminant.
Montrons le troisième point : on note $A = K[X]/(P)$. C'est une K-algèbre de dimension p canoniquement isomorphe comme K-espace vectoriel à $K_{<p}[X]$. On note N la matrice de μ_Q dans la base canonique $(1, X, \ldots, X^{p-1})$, et M la matrice de φ dans les bases canoniques. Les p premières colonnes de M, vues comme des polynômes de $K_{<p+q}[X]$ peuvent être remplacées par leur reste dans la division euclidienne par P sans changer le déterminant de M en faisant des combinaisons linéaires avec les q dernières colonnes. On a donc :

$$\det(M) = \begin{vmatrix} N & & & * & \\ & \alpha & * & \cdots & * \\ & 0 & \ddots & & \vdots \\ & \vdots & & \ddots & * \\ & 0 & \cdots & 0 & \alpha \end{vmatrix} = \alpha^q \det(N)$$

comme annoncé.
Le quatrième point est une conqéquence directe du troisième car la formule donnée par le troisième point est clairement multiplicative en Q et le cinquième s'obtient à partir du quatrième par récurrence (puisque le fait de changer de corps ne change pas le discriminant, on peut faire comme si on avait $K = \Omega$) avec le fait suivant :

$$\mathrm{Res}(P, X - y) = (-1)^p P(y)$$

qui est un simple calcul du déterminant :

$$\begin{vmatrix} -y & & & & a_0 \\ 1 & -y & & & a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & -y & a_{p-1} \\ & & & 1 & a_p \end{vmatrix}$$

avec $P = a_0 + \cdots + a_p X^p$ qui peut s'obtenir par exemple en développant par rapport à la dernière colonne.

Si P est séparable, alors φ est injective (on refait la preuve car ici P' n'est pas nécessairement de degré $p-1$) : si $UP'+VP=0$, avec $\deg U < p$ et $\deg V < p-1$, on a $P \mid UP'$ donc $P \mid U$ par le lemme de Gauss et donc $U=0$. Par integrité de $K[X]$ et puisque $P \neq 0$ on a donc $V=0$. Ainsi $\mathrm{Disc}(P) \neq 0$.
Si le discriminant est non nul, φ est surjective donc on peut encore conclure par le théorème de Bézout que P et P' sont premiers entre eux.
Enfin, la formule pour le discriminant vient de :

$$\mathrm{Res}(P,P') = \alpha^{p-1} \prod_i P'(x_i) = \alpha^{2p-1} \prod_i \prod_{j \neq i} (x_i - x_j)$$

car $P' = \sum_i \prod_{j \neq i} (X - x_j)$. □

Exemple 1.57. *Mentionnons le calcul du discriminant en degré* 1, 2 *et* 3. *On* a, *pour* a, b, c, d *dans* K *avec* $a \neq 0$ *:*

$$\mathrm{Disc}(aX+b) = 1$$

puis :

$$\mathrm{Disc}(aX^2+bX+c) = b^2 - 4ac$$

et :

$$\mathrm{Disc}(aX^3+bX^2+cX+d) = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2$$

dont on laisse la preuve au lecteur.

1.8 Structure du groupe des unités modulo n

Le but de cette partie est de déterminer la structure du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n \geq 1$. Par le théorème des restes chinois et puisque le groupe multiplicatif d'un produit de deux anneaux est le produit des groupes multiplicatifs, on se contente de traiter le cas où n est une puissance d'un nombre premier p.

Lemme 1.58. *Soit* p *un nombre premier,* $k \geq 1$ *et* $a, b \in \mathbb{Z}$. *Si* $a \equiv b\ [p^k]$ *alors* $a^p \equiv b^p\ [p^{k+1}]$. *De plus, si* $p \geq 3$, *si* b *est premier à* p *et si* $a \equiv b\ [p]$ *alors :*

$$v_p(a^p - b^p) = v_p(a-b) + 1.$$

Enfin, si $p = 2$, *si* b *est impair et si* $a \equiv b\ [4]$ *alors :*

$$v_2(a^p - b^p) = v_p(a-b) + 1.$$

Démonstration. On a :

$$a^p - b^p = (a-b) \sum_{i=0}^{p-1} a^i b^{p-1-i}.$$

Or $p^k \mid a-b$ et puisque $k \geq 1$, $a \equiv b\ [p]$ donc $\sum_{i=0}^{p-1} a^i b^{p-1-i} \equiv \sum_{i=0}^{p-1} a^{p-1} \equiv 0\ [p]$ et donc $p^{k+1} \mid a^p - b^p$.
Pour la deuxième affirmation, on utilise cette fois-ci le binôme de Newton :

$$a^p - b^p = (a-b+b)^p - b^p = \sum_{i=1}^{p} \binom{p}{i} (a-b)^i b^{p-i} = \sum_{i=2}^{p-1} \binom{p}{i} (a-b)^i b^{p-i} + p(a-b)b^{p-1} + (a-b)^p.$$

Notons que cette formule est bien valable pour $p = 2$, la somme étant nulle. On note $k = v_p(a-b)$: on a $k \geq 1$ par hypothèse donc par ce qui précède, $v_p(a^p - b^p) \geq k+1$ et on veut voir que sous les hypothèses faites que $a^p - b^p$ n'est pas divisible par p^{k+2}. Puisque b est premier à p, on a pour le second terme :

$$v_p(p(a-b)b^{p-1}) = k+1.$$

Pour le premier terme, les coefficients binomiaux sont divisibles par p donc le premier terme est divisible par p^{2k+1} et donc par p^{k+2}. Enfin le troisième terme est divisible par p^{kp} donc si $p \geq 3$ ou si $k \geq 2$ c'est divisible par p^{k+2} et cela permet de conclure. □

Théorème 1.59. *Soit p un nombre premier impair et $k \geq 1$. Le groupe $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ est cyclique d'ordre $\varphi(p^k) = p^{k-1}(p-1)$ tandis que pour $p = 2$ et $k \geq 2$ on a un isomorphisme :*

$$\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$$

donné par $-1 \longleftrightarrow (1,0)$ et $3 \longleftrightarrow (0,1)$ autrement dit $(-1)^a 3^b \longleftrightarrow (a,b)$.
En particulier le groupe quotient $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times / \langle -1 \rangle$ est toujours cyclique.

Démonstration. Pour p premier quelconque, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, généré par la classe d'un entier ω d'après le théorème 2.30. Notons o l'ordre de ω modulo p^k pour un $k \geq 1$ fixé. On a en particulier :

$$\omega^o \equiv 1 \ [p]$$

donc $p-1 \mid o$ car ω est d'ordre $p-1$ modulo p. Ainsi $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ contient un élément d'ordre divisible par $p-1$, donc il contient un élément d'ordre $p-1$.
Ensuite, si $p \geq 3$ et $k \geq 1$, on montre par récurrence sur k que :

$$v_p\left((p+1)^{p^{k-1}} - 1\right) = k.$$

C'est clair pour $k = 1$, et si c'est vrai pour k, alors par le lemme précédent (qui s'applique bien) on a :

$$v_p\left((p+1)^{p^k} - 1\right) = k+1$$

ce qui achève la récurrence. Ceci montre que $p+1$ est d'ordre p^{k-1} modulo p^k (en effet on a d'abord que son ordre est une puissance de p qui divise p^{k-1}, disons p^j et la formule précédente donne une contradiction si $j < k-1$).
Ainsi le groupe $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ a un élément d'ordre $p-1$ et un élément d'ordre p^{k-1}, ce qui donne un morphisme :

$$\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{k-1}\mathbb{Z} \longrightarrow \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$$

injectif car $p-1$ et p^{k-1} sont premiers entre eux. Il est surjectif car ces deux groupes ont le même cardinal, et par le théorème Chinois, le groupe de gauche est cyclique, ce qui conclut.

Pour $p = 2$ le lemme ne s'applique pas tout de suite, ce qui change légèrement la récurrence. En effet $p+1 = 3$ est d'ordre 1 dans $\mathbb{Z}/2\mathbb{Z}$, d'ordre 2 dans $\mathbb{Z}/4\mathbb{Z}$ et d'ordre 2 dans $\mathbb{Z}/8\mathbb{Z}$. Ainsi on commence la récurrence à $k = 3$ et on montre :

$$v_2\left(3^{2^{k-2}} - 1\right) = k.$$

Pour $k = 3$ c'est clair, et si c'est vrai pour un $k \geq 3$ le lemme précédent nous le donne pour $k+1$. Ainsi pour $k \geq 3$, l'élément 3 est d'ordre 2^{k-2} modulo 2^k par le même raisonnement qu'avant.
On a donc, toujours pour $k \geq 3$, un morphisme de groupes :

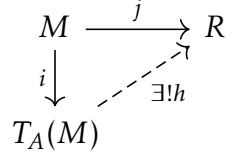
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z} \longrightarrow \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$$

qui envoie $(1,0)$ sur -1 et $(0,1)$ sur 3. Puisque ces deux groupes ont le même cardinal, il suffit de voir que ce morphisme est injectif, autrement dit que -1 n'est pas un élément de $\langle 3 \rangle$. Or le seul élément d'ordre 2 de $\langle 3 \rangle$ est $3^{2^{k-3}}$, mais la réduction modulo 8 de $3^{2^{k-3}}$ vaut 3 ou 1 donc jamais -1. □

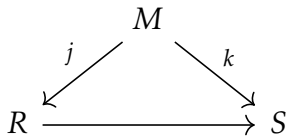
1.9 Algèbre tensorielle et algèbre extérieure

1.9.1 Algèbre tensorielle

Fixons un anneau (commutatif unitaire) A et M un A-module. On va construire une A-algèbre associative (non commutative), $T_A(M)$, qui contient naturellement M et qui est en quelque sorte l'algèbre la plus générale possible contenant M. On peut formaliser ceci avec une propriété universelle : pour toute A-algèbre associative R et tout morphisme de A-module $j : M \longrightarrow R$, il existe un unique morphisme de A-algèbres $h : T_A(M) \longrightarrow R$ tel que le diagramme suivant commute :



avec i l'inclusion de M dans $T_A(M)$.
Autrement dit, si l'on considère la catégorie Alg_M dont les objets sont les couples (R, j) avec R une A-algèbre associative et $j : M \longrightarrow R$ un morphisme de A-modules, et dont les flèches $(R, j) \longrightarrow (S, k)$ sont les morphismes d'algèbres $R \longrightarrow S$ qui font commuter le diagramme :



alors $(T_A(M), i)$ est l'objet initial de cette catégorie (voir 1.2).
En particulier, si on sait montrer qu'un tel objet initial existe, il sera unique à unique isomorphisme près.

Une troisième façon équivalente de donner la propriété universelle, plus compacte, est la suivante :

$$\mathrm{Hom}_{A-\mathrm{alg}}(T_A(M), R) \cong \mathrm{Hom}_A(M, R)$$

naturellement en R, avec R une A-algèbre.
La définition suivante montre qu'un tel objet existe et en donne une construction explicite.

Définition 1.60. *(Algèbre tensorielle) On construit $T_A(M)$ de la façon suivante :*

$$T_A(M) = \bigoplus_{n\geq 0} T_A^n(M)$$

où $T_A^n(M) = M \otimes_A \cdots \otimes_A M$ avec n facteurs. Par convention $T_A^0(M) = A$. On a alors une inclusion :

$$A = T_A^1(M) \subseteq T_A(M).$$

On construit ainsi une algèbre d'élément neutre $1 \in T_A^0(M)$ dont le produit est donné par le produit tensoriel.

On vérifie facilement la propriété universelle : si $j : M \longrightarrow R$ est un morphisme de A-modules de M vers une A-algèbre R, tout morphisme de A-algèbres $f : T_A(M) \longrightarrow R$ est entièrement déterminé par l'image des éléments de $M = T_A^1(M)$:

$$f(x_1 \otimes \cdots \otimes x_p) = f(x_1)f(x_2)\ldots f(x_p).$$

Ainsi, il existe un unique morphisme de A-algèbres $f : T_A(M) \longrightarrow R$ tel que pour tout $x \in M$, on ait $f(x) = j(x)$.
Les éléments de $T_A^n(M)$ sont appelés *tenseurs homogènes d'ordre n* : les tenseurs d'ordre 0 sont les scalaires, les tenseurs d'ordre 1 sont les éléments de M, et ainsi de suite.
L'algèbre tensorielle $T_A(M)$ est fonctorielle : si $M \xrightarrow{\varphi} N$ est un morphisme de A-modules, il induit en composant par l'inclusion canonique un morphisme de A-modules :

$$M \longrightarrow T_A(N)$$

qui induit, par propriété universelle, un morphisme de A-algèbres :

$$T_A(M) \xrightarrow{T_A(\varphi)} T_A(N)$$

qui envoie un tenseur d'ordre 1, $x \in M$, sur $\varphi(x)$.
De plus, l'algèbre tensorielle est compatible à l'extension des scalaires au sens suivant.

Proposition 1.61. *Soit B une A-algèbre commutative et M un A-module. On a un isomorphisme canonique de B-algèbres associatives :*

$$T_A(M) \otimes_A B \cong T_B(M \otimes_A B).$$

Démonstration. On peut démontrer directement que $T_A^n(M) \otimes_A B \cong T_B^n(M \otimes_A B)$. On peut aussi démontrer que ces deux objets vérifient la même propriété universelle et sont donc isomorphes, d'après le lemme de Yoneda 1.8.

En effet, si R est une B-algèbre, la donnée d'un morphisme de B-algèbres de $T_A(M)\otimes_A B$ vers R équivaut à la donnée d'un morphisme de A-algèbres de $T_A(M)$ vers R (par extension des scalaires), ce qui équivaut à la donnée d'un morphisme de A-modules de M vers R, autrement dit à la donnée d'un morphisme de B-modules de $M\otimes_A B$ vers R, c'est à dire à la donnée d'un morphisme de B-algèbres de $T_B(M\otimes_A B)$ vers R.
Notez que pour pouvoir appliquer le lemme de Yoneda, il faut aussi vérifier la naturalité en R dans toutes ces bijections, mais c'est tautologique. □

On termine notre étude des algèbres tensorielles par la remarque suivante.

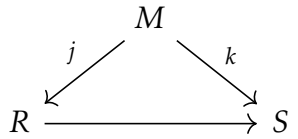
Remarque 1.62. Si M est engendré comme A-module par $x_1,\dots,x_p$, alors $T_A(M)$ est engendrée comme A-algèbre par ces mêmes éléments.

1.9.2 Algèbre extérieure

Fixons encore A un anneau (commutatif unitaire) et M un A-module. Comme ci-dessus, on va construire une A-algèbre $\Lambda_A M$ (non commutative a priori) universelle, contenant M, et qui vérifie que tout élément de M est de carré nul dans $\Lambda_A M$.
Autrement dit, si l'on considère la catégorie AlgAlt_M dont les objets sont les couples (R,j) avec R une A-algèbre associative et $j : M \longrightarrow R$ un morphisme de A-module qui vérifie :

$$\forall x \in M \; j(x)^2 = 0$$

et dont les flèches $(R,j) \longrightarrow (S,k)$ sont les morphismes d'algèbres $R \longrightarrow S$ qui font commuter le diagramme :



alors $(\Lambda_A M, i)$ est l'objet initial de cette catégorie (voir 1.2) avec $i : M \longrightarrow \Lambda_A M$ l'inclusion canonique.
De façon équivalente, on veut la propriété universelle suivante :

$$\mathrm{Hom}_{A-\mathrm{alg}}(\Lambda_A M, R) \cong \{j \in \mathrm{Hom}_A(M,R) \mid \forall x \in M \; j(x)^2 = 0\}$$

naturellement en R une A-algèbre.
Comme pour l'algèbre tensorielle, si on sait montrer qu'un tel objet existe, il sera unique à isomorphisme près.
La définition suivante montre qu'un tel objet existe et en donne une construction explicite.

Définition 1.63. *(Algèbre extérieure) On construit $\Lambda_A(M)$ de la façon suivante : on considère l'idéal bilatère I de $T_A(M)$ engendré par les $x\otimes x$ pour $x \in M$. Autrement dit, I est engendré comme A-module par les $a\otimes x\otimes x\otimes b$ pour $a,b \in T_A(M)$. On pose alors :*

$$\Lambda_A(M) = T_A(M)/I.$$

Le produit de cette algèbre associative est noté $\wedge$ et est appelé "produit extérieur". On plonge M dans $\Lambda_A(M)$ via la composée :

$$i : M \longrightarrow T_A(M) \longrightarrow \Lambda_A(M)$$

et on va voir que cette composée est injective.

Par construction, on a alors $i(x) \wedge i(x) = 0$ pour tout $x \in M$, et en oubliant le i cela s'écrit $x \wedge x = 0$.
La propriété universelle est facile à déduire de celle de $T_A(M)$.

Lemme 1.64. *(Antisymétrie du produit extérieur) Le produit $\wedge$ est antisymétrique sur les éléments de M, au sens où :*

$$x \wedge y = -y \wedge x$$

pour tous $x, y \in M$. De façon plus générale, pour tous $x_1, \ldots, x_n \in M$ et tout $\sigma \in \mathfrak{S}_n$ une permutation, on a :

$$x_{\sigma(1)} \wedge x_{\sigma(2)} \wedge \cdots \wedge x_{\sigma(n)} = \varepsilon(\sigma) x_1 \wedge x_2 \wedge \cdots \wedge x_n.$$

De plus, si $x_i = x_j$ avec $i \neq j$, on a :

$$x_1 \wedge \cdots \wedge x_n = 0.$$

Enfin, on a la loi d'anticommutativité suivante pour les éléments homogènes : si $\alpha \in \Lambda_A^p M$ et $\beta \in \Lambda_A^q M$, on a :

$$\alpha \wedge \beta = (-1)^{pq} \beta \wedge \alpha.$$

Démonstration. Soient $x, y \in M$, on a :

$$0 = (x+y) \wedge (x+y) = x \wedge x + x \wedge y + y \wedge x + y \wedge y = x \wedge y + y \wedge x$$

donc $x \wedge y = -y \wedge x$.
Le résultat général en découle car le groupe symétrique est engendré par les transpositions de la forme $(i \;\; i+1)$.
En particulier si $x_i = x_j$ avec $i < j$, on a au signe près :

$$x_1 \wedge \cdots \wedge x_n = x_1 \wedge \cdots \wedge x_i \wedge x_i \wedge \cdots \wedge \widehat{x_j} \wedge \cdots \wedge x_n = 0$$

où le chapeau désigne un terme omis, et en utilisant le fait que $x_i \wedge x_i = 0$.
Voyons la dernière formule. Par linéarité, on peut supposer :

$$\alpha = x_1 \wedge \cdots \wedge x_p$$

et :

$$\beta = y_1 \wedge \cdots \wedge y_q$$

de sorte que :

$$\alpha \wedge \beta = x_1 \wedge \cdots \wedge x_p \wedge y_1 \wedge \cdots \wedge y_q = (-1)^{pq} y_1 \wedge \cdots \wedge y_q \wedge x_1 \wedge \cdots \wedge x_p = (-1)^{pq} \beta \wedge \alpha$$

en faisant successivement avancer x_p de q places vers la droite, puis x_{p-1} de q places vers la droite, et ainsi de suite, ce qui produit un signe $(-1)^q$ exactement p fois. □

La A-algèbre $T_A(M)$ est naturellement *graduée* :

$$T_A(M) = \bigoplus_{n\geq 0} T_A^n(M)$$

et l'idéal I est compatible à cette graduation au sens suivant :

$$I = \bigoplus_{n\geq 0} (I \cap T_A^n(M)).$$

Ceci vient du fait que I est engendré par des éléments homogènes (les $x\otimes x$). Vérifions le : I est engendré comme A-module par les $u\otimes x\otimes x\otimes v$ avec $u, v \in T_A(M)$, et on peut les supposer homogènes de degrés p et q quitte à les décomposer en somme de tenseurs homogènes. On a alors :

$$u \otimes x \otimes x \otimes v \in I \cap T_A^{p+q+2}(M).$$

On peut donc graduer le quotient :

$$\Lambda_A M = \bigoplus_{n\geq 0} \frac{T_A^n(M)}{I \cap T_A^n(M)}$$

et on définit ainsi :

$$\Lambda_A^n M = \frac{T_A^n(M)}{I \cap T_A^n(M)}.$$

Puisque $I \cap T_A^0(M) = I \cap T_A^1(M) = 0$, on obtient en particulier :

$$\Lambda_A^0 M = A$$

et

$$\Lambda_A^1 M = M$$

et donc $i : M \longrightarrow \Lambda_A M$ est injectif comme promis. On peut donc considèrer que $M \subseteq \Lambda_A M$.

Définition 1.65. *Le A-module $\Lambda_A^n M$ est appelé n-ème puissance extérieure de M.*

La n-ème puissance extérieure de M vérifie une propriété universelle intéressante. On note, pour X un A-module, $\mathrm{Alt}_A^n(M, X)$ le A-module des applications n-linéaires $f : M \times \cdots \times M$ vers X qui sont alternées, au sens où $f(x_1, \ldots, x_n) = 0$ dès que deux des x_i sont égaux.

Proposition 1.66. *Soit X un A-module. On a une bijection naturelle en X :*

$$\mathrm{Hom}_A(\Lambda_A^n M, X) \cong \mathrm{Alt}_A^n(M, X)$$

qui fait correspondre à $f \in \mathrm{Hom}_A(\Lambda_A^n M, X)$ l'application n-linéaire alternée $\hat{f} : (x_1, \ldots, x_n) \mapsto f(x_1 \wedge \cdots \wedge x_n)$.

Démonstration. Il est clair que $\hat{f}$ est n-linéaire et alternée d'après le lemme 1.64. De plus, si $g \in \mathrm{Alt}_A^n(M,X)$, il existe une unique application A-linéaire :

$$\tilde{g} : M \otimes \cdots \otimes M \longrightarrow X$$

telle que $\tilde{g}(x_1 \otimes \cdots \otimes x_n) = g(x_1,\ldots,x_n)$ car g est n-linéaire, et $\tilde{g}$ se factorise par le quotient $\Lambda_A^n M = T_A^n(M)/(I \cap T_A^n(M))$ car g est alternée (et donc $\tilde{g}$ tue les éléments de la forme $u \otimes x \otimes x \otimes v$). □

L'algèbre extérieure est compatible à l'extension des scalaires.

Proposition 1.67. *Soit B une A-algèbre commutative et M un A-module. On a un isomorphisme canonique de B-algèbres associatives :*

$$\Lambda_A M \otimes_A B \cong \Lambda_B(M \otimes_A B).$$

Cet isomorphisme respecte la graduation et donne un isomorphisme canonique de A-modules pour tout n :

$$\Lambda_A^n M \otimes_A B \cong \Lambda_B^n(M \otimes_A B).$$

Cela se vérifie soit en utilisant le lemme de Yoneda 1.8 soit directement en tensorisant par B la suite exacte :

$$I \cap T_A^n(M) \longrightarrow T_A^n(M) \longrightarrow \Lambda_A^n M \longrightarrow 0.$$

Remarque 1.68. Si M est engendré comme A-module par $x_1,\ldots,x_n$, alors pour tout k, $\Lambda_A^k M$ est engendré comme A-module par les $\bigwedge_{j\in J} x_j$ pour $J \subseteq \{1,\ldots,n\}$ un ensemble de k indices. En particulier, pour $k > n$ on a :

$$\Lambda_A^k M = 0$$

et on a la somme directe :

$$\Lambda_A M = \bigoplus_{k=0}^{n} \Lambda_A^k M.$$

Démonstration. Pour $J \subseteq \{1,\ldots,n\}$, posons :

$$x_J = \bigwedge_{j\in J} x_j \in \Lambda_A^{|J|} M.$$

On sait que $T_A^k(M)$ est engendré par les $x_{i_1} \otimes \cdots \otimes x_{i_k}$ avec les i_j des indices entre 1 et n. C'est donc aussi le cas de son quotient $\Lambda_A^k M$, or on peut éliminer les doublons puisque leur produit extérieur est nul, et on peut, grâce à l'antisymétrie, remettre les indices dans l'ordre sans rien changer au signe près.
Ainsi $\Lambda_A^k M$ est engendré par les x_J pour $|J| = k$. Pour $k > n$, il n'existe pas de telle partie donc :

$$\Lambda_A^k M = 0.$$

□

Si M est un A-module libre, $\Lambda_A M$ aussi.

Proposition 1.69. *Supposons que M soit libre avec pour base $(e_i)_{i\in I}$.*
On choisit, pour tout ensemble fini $J \subseteq I$, un ordre total sur J et on pose :

$$e_J = \bigwedge_{j\in J} e_j$$

où le produit est effectué dans l'ordre choisi sur J (et $e_\emptyset = 1$).
Alors pour tout $k \geq 0$, on a :

$$\Lambda_A^k M = \bigoplus_{|J|=k} Ae_J$$

et :

$$\Lambda_A M = \bigoplus_{J} Ae_J$$

la somme portant sur les parties $J \subseteq I$ finies.
Ainsi, si M est libre de rang fini n, $\Lambda_A^k M$ est libre de rang $\binom{n}{k}$ et $\Lambda_A M$ est libre de rang 2^n.

Démonstration. La seule chose à montrer est que, pour tout $k \geq 0$, on a :

$$\Lambda_A^k M = \bigoplus_{|J|=k} Ae_J.$$

On sait déjà que les e_J avec $|J| = k$ engendrent $\Lambda_A^k M$ avec la remarque précédente, et il reste à voir que c'est une famille libre. On raisonne pour cela par dualité. Notons dx_i la i-ème forme coordonnée sur M, qui envoie e_j sur δ_{ij}.
Pour tout $J = \{j_1, \ldots, j_k\}$ dans l'ordre fixé, avec $|J| = k$ et $y_1, \ldots, y_k \in M$, on pose :

$$dx_J(y_1, \ldots, y_k) = \sum_{\sigma\in\mathfrak{S}_k} \varepsilon(\sigma) \prod_{i=1}^{k} dx_{j_i}(y_{\sigma(i)}).$$

Il s'agit d'une forme k-linéaire alternée et donc :

$$dx_J \in \mathrm{Alt}_A^k(M, A).$$

Par la propriété universelle de $\Lambda_A^k M$, il existe donc une unique application A-linéaire $\delta x_J : \Lambda_A^k M \longrightarrow A$ telle que :

$$\delta x_J(y_1 \wedge \cdots \wedge y_k) = dx_J(y_1, \ldots, y_k).$$

On a donc en particulier pour $L = \{\ell_1, \ldots, \ell_k\}$ de cardinal k dans l'ordre fixé :

$$\delta x_J(e_L) = \sum_{\sigma\in\mathfrak{S}_k} \varepsilon(\sigma) \prod_{i=1}^{k} dx_{j_i}\left(e_{\ell_{\sigma(i)}}\right) = \sum_{\sigma\in\mathfrak{S}_k} \varepsilon(\sigma) \begin{cases} 1 & \text{si } j_i = \ell_{\sigma(i)}\ \forall i \\ 0 & \text{sinon} \end{cases}$$

qui vaut 1 si $J = K$ et 0 sinon. Ainsi, si $\sum_{|J|=k} \lambda_K e_J = 0$ avec les λ_J presque tous nuls, on a en appliquant δx_J que $\lambda_J = 0$. La famille est donc libre. □

On a une formule du type binôme de Newton pour calculer la puissance extérieure d'une somme.

Proposition 1.70. *Soient M et N deux A-modules. On a un isomorphisme canonique de A-modules :*

$$\Lambda_A(M \oplus N) \cong (\Lambda_A M) \otimes_A (\Lambda_A N)$$

qui provient du morphisme $M \oplus N \longrightarrow (\Lambda_A M) \otimes_A (\Lambda_A N)$ qui envoie (m, n) sur $m \otimes 1 + 1 \otimes n$. On a de plus, pour tout $n \geq 0$:

$$\Lambda_A^n(M \oplus N) \cong \bigoplus_{p+q=n} \left(\Lambda_A^p M\right) \otimes_A \left(\Lambda_A^q N\right)$$

comme A-modules.

Attention, comme on le verra dans la preuve, pour avoir un isomorphisme de A-algèbres entre $\Lambda_A(M \oplus N)$ et $\Lambda_A M \otimes \Lambda_A N$, il faut mettre la bonne structure d'algèbre sur $\Lambda_A M \otimes \Lambda_A N$.

Démonstration. Il est possible de vérifier tout ceci à la main en construisant des morphismes, mais on va ici donner une preuve conceptuelle.
On va utiliser le lemme de Yoneda et une propriété universelle de $\Lambda_A(\bullet)$. On pourrait utiliser la propriété universelle que l'on connaît, mais ça ne marcherait pas (en effet, on aurait besoin à un moment de la preuve que la somme de deux éléments de carré nul soit de carré nul dans une algèbre associative quelconque).
On va donc utiliser une autre propriété universelle. Pour cela on considère la catégorie $\mathrm{GrdAltAlg_A}$ des A-algèbres graduées associatives et alternées : ce sont les A-algèbres graduées $R = \bigoplus_{n \geq 0} R_n$ avec $R_p R_q \subseteq R_{p+q}$, $A \cdot R_p \subseteq R_p$, $1_A \in R_0$ et pour tout $x \in R_p$ et $y \in R_q$:

$$xy = (-1)^{pq} yx$$

et pour tout $x \in R_1$, $x^2 = 0$. Notez que cette dernière condition découle de la précédente si on n'est pas en caractéristique 0. Les morphismes de cette catégorie sont les morphismes de A-algèbres qui préservent la graduation : $f : R \longrightarrow S$ doit vérifier $f(R_n) \subseteq S_n$.
D'après le lemme 1.64, l'algèbre extérieure $\Lambda_A M$ est bien un objet de cette catégorie.
De plus, on a, naturellement en R dans $\mathrm{GrdAltAlg_A}$:

$$\mathrm{Hom}_{\mathrm{GrdAltAlg_A}}(\Lambda_A M, R) \cong \mathrm{Hom}_A(M, R_1).$$

En effet, si $f : \Lambda_A M \longrightarrow R$ est un morphisme gradué, il envoie la partie d'ordre 1 sur la partie d'ordre 1 donc induit un morphisme de A-modules $g : M \longrightarrow R_1$.
Puisque $\Lambda_A M$ est engendré par les éléments de M et que f est un morphisme, f est entièrement déterminé par g.
Réciproquement, si on se donne $g : M \longrightarrow R_1$, on a en particulier $g : M \longrightarrow R$ et pour tout $x \in M$, on a $g(x)^2 = 0$, donc g induit un morphisme de A-algèbres $\Lambda_A M \longrightarrow R$ qui prolonge g et qui préserve clairement la graduation car $\Lambda_A M$ est engendré par les éléments de M.
Étudions à présent la notion de produit tensoriel dans la catégorie $\mathrm{GrdAltAlg_A}$. Si R et

S sont deux objets de $\mathrm{GrdAltAlg_A}$, on peut graduer le produit tensoriel de A-modules $R \otimes_A S$ de la façon suivante :

$$R \otimes_A S = \left(\bigoplus_n R_n \right) \otimes_A \left(\bigoplus_n S_n \right) = \bigoplus_n \left(\bigoplus_{p+q=n} R_p \otimes S_q \right)$$

par distributivité du produit tensoriel sur la somme directe. On pose ainsi :

$$(R \otimes S)_n = \bigoplus_{p+q=n} R_p \otimes S_q.$$

On munit $R \otimes_A S$ du produit suivant (grâce à la somme directe, il suffit de le définir sur les éléments homogènes) : si $x \in R_p, x' \in R_{p'}$ et $y \in R_q, y' \in R_{q'}$, on pose :

$$(x \otimes y)(x' \otimes y') = (-1)^{p'q} xx' \otimes yy'.$$

Le signe vient du fait qu'on doit inverser y et x'. On vérifie alors facilement que $R \otimes_A S$ est une A-algèbre graduée associative et alternée.
Elle est munie des deux morphismes canoniques de A-algèbres graduées $i : R \longrightarrow R \otimes_A S$ et $j : S \longrightarrow R \otimes_A S$ et elle vérifie une propriété universelle, dite du *coproduit* :

$$\mathrm{Hom}_{\mathrm{GrdAltAlg_A}}(R \otimes_A S, X) \cong \mathrm{Hom}_{\mathrm{GrdAltAlg_A}}(R, X) \times \mathrm{Hom}_{\mathrm{GrdAltAlg_A}}(S, X)$$

via $f \mapsto (f \circ i, f \circ j)$, naturellement en X. Décrivons la bijection réciproque. Si $u : R \longrightarrow X$ et $v : S \longrightarrow X$ sont des morphismes de A-algèbres graduées, on définit simplement :

$$f(x \otimes y) = u(x)v(y).$$

On laisse au lecteur le soin de vérifier les détails.
On peut enfin appliquer le lemme de Yoneda :

$$\begin{aligned}
\mathrm{Hom}_{A-\mathrm{GrdAltAlg_A}}(\Lambda_A(M \oplus N), R) &\cong \mathrm{Hom}_A(M \oplus N, R_1) \\
&\cong \mathrm{Hom}_A(M, R_1) \times \mathrm{Hom}_A(N, R_1) \\
&\cong \mathrm{Hom}_{A-\mathrm{GrdAltAlg_A}}(\Lambda_A M, R) \times \mathrm{Hom}_{A-\mathrm{GrdAltAlg_A}}(\Lambda_A N, R) \\
&\cong \mathrm{Hom}_{A-\mathrm{GrdAltAlg_A}}(\Lambda_A M \otimes_A \Lambda_A N, R)
\end{aligned}$$

d'où l'isomorphisme voulu :

$$\Lambda_A(M \oplus N) \cong (\Lambda_A M) \otimes_A (\Lambda_A N).$$

Pour le deuxième, il suffit de comparer les graduations, puisqu'on a obtenu un isomorphisme d'algèbres graduées.
Pour dire les choses de façon beaucoup plus catégorique, on a construit un *adjoint* à droite du foncteur $\Lambda_A : \mathrm{Mod}_A \longrightarrow \mathrm{GrdAltAlg_A}$ ce qui montre que Λ_A préserve les *coproduits*. □

Remarque 1.71. Il existe d'autres constructions d'algèbres universelles en partant d'un A-module M. On peut par exemple construire l'algèbre symétrique de M, $\mathrm{Sym}_A M$, obtenue comme quotient de $T_A(M)$ par l'idéal bilatère engendré par les $x \otimes y - y \otimes x$ avec $x, y \in M$. C'est l'algèbre commutative la plus générale contenant M, et de même, puisque l'idéal par lequel on quotiente est engendré par des tenseurs homogènes, c'est une algèbre graduée.
On peut aussi construire une généralisation de l'algèbre extérieure, en choisissant une forme quadratique q sur M (disons que A n'est pas de caractéristique 2) et en quotientant $T_A(M)$ par l'idéal bilatère engendré par les $x \otimes x - q(x)$ de façon à obtenir une algèbre $\mathrm{Cliff}_A(M, q)$ dans laquelle on a forcé la relation :

$$x^2 = q(x).$$

On obtient ainsi l'algèbre de *Clifford* associée à la forme quadratique q et le cas particulier $q = 0$ donne l'algèbre extérieure. Les algèbres de Clifford sont les objets de base de l'algèbre géométrique : on fixe un espace vectoriel réel V muni d'une forme quadratique q (par exemple un produit scalaire), et on considère l'algèbre de Clifford $\mathrm{Cliff}_{\mathbb{R}}(V, q)$. Par exemple, $\mathrm{Cliff}_{\mathbb{R}}(\mathbb{R}^2)$ (pour le produit scalaire usuel) est l'algèbre des quaternions.

Chapitre 2

Théorie des corps

> Lors donc qu'on aura épuisé sur le groupe d'une équation tout ce qu'il y a de décompositions propres possibles sur ce groupe, on arrive à des groupes qu'on pourra transformer, mais dont les permutations seront toujours en même nombre. Si ces groupes ont chacun un nombre premier de permutations, l'équation sera soluble par radicaux. Sinon, non.
>
> Évariste Galois

2.1 Théorie de Galois

On rappelle de façon très succinte la théorie de Galois des extensions finies de corps. Soit L/K une extension finie de corps. Un polynôme $f \in K[X]$ est dit *séparable* si ses facteurs irréductibles apparaissent avec multiplicité 1 dans f, ou de façon équivalente, si les racines de f dans un quelconque corps algébriquement clos contenant K sont simples. La séparabilité de f ne dépend pas du corps K contenant les coefficients de f choisi. Un élément $x \in L$ est séparable sur K si son polynôme minimal sur K est séparable. Enfin, l'extension L/K est séparable si tout élément de L est séparable sur K.
La question de la séparabilité ne se pose qu'en caractéristique $p > 0$ car en caractéristique 0, tout polynôme irréductible est séparable.

Proposition 2.1. *Si K est de caractéristique nulle, tout polynôme irréductible est séparable. Si K est de caractéristique $p > 0$, et si $f \in K[X]$ est irréductible, alors les énoncés suivants sont équivalents :*

— $f' = 0$.

— *Il existe $g \in K[X]$ tel que $f(X) = g(X^p)$.*

— *f n'est pas séparable.*

Démonstration. Soit f un polynôme irréductible de degré $d \geq 1$. Le polynôme f' est soit nul soit de degré strictement inférieur à d. Si $f' \neq 0$, alors f et f' sont premiers entre eux car f est irréductible et donc f est séparable. Réciproquement, si f est séparable, $f' \neq 0$.
En caractéristique nulle, il est impossible d'avoir $f' = 0$. Enfin, en caractéristique $p > 0$, on écrit $f = \sum_k a_k X^k$ de sorte que $f' = \sum_k k a_k X^{k-1}$. Ainsi $f' = 0$ si et seulement si $a_k = 0$ pour tout k non divisible par p, et ceci équivaut à la deuxième condition. □

L'exemple le plus simple d'extension non séparable est celui de l'extension $\mathbb{F}_p(T^{1/p})/\mathbb{F}_p(T)$. En effet, $T^{1/p}$ a pour polynôme minimal $X^p - T = (X - T^{1/p})^p$ qui n'est pas séparable.
Même dans l'étude des corps de nombres, considérer des corps de caractéristique p a son importance dans l'étude de la ramification. Heureusement, les corps que l'on rencontrera seront toujours parfaits.

Définition 2.2. *Un corps K est parfait si toute extension finie de K est séparable.*

Ainsi tout corps de caractéristique nulle est parfait. En caractéristique p, on rappelle la notion suivante.

Définition 2.3. *Soit K un corps de caractéristique p, avec p un nombre premier. On définit l'endomorphisme de Frobenius ainsi :*

$$F(x) = x^p$$

pour $x \in K$. C'est un morphisme d'anneau car on a :

$$F(x+y) = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = F(x) + F(y)$$

car le coefficient binomial $\binom{p}{k}$ est divisible par p si $1 \leq k \leq p-1$, et $p = 0$ dans le corps K. Notons que F est toujours injectif car c'est un morphisme de corps. Ainsi, si K est fini, il est même surjectif.

et si K est de caractéristique p, on a l'équivalence suivante.

Proposition 2.4. *K est parfait si et seulement si son Frobenius $F : x \mapsto x^p$ est surjectif. En particulier tout corps fini est parfait.*

Démonstration. Si F est surjectif et si L/K est une extension finie et $x \in L$ a pour polynôme minimal f sur K, f est irréductible, donc il est soit séparable soit de la forme $g(X^p)$, or F est surjectif donc il existe h tel que $g = h^F$ (le polynôme obtenu en mettant les coefficients de h à la puissance p) et donc :

$$f(X) = h(X)^p$$

ce qui contredit l'irréductibilité de f. Si F n'est pas surjectif, il existe $a \in K$ qui n'a pas de racine p-ème, et si z est une racine p-ème de a dans un corps algébriquement clos

contenant K, alors $X^p - a = (X - z)^p$ et ce polynôme est irréductible dans $K[X]$ car ses facteurs éventuels sont les $(X - z)^k$, et si $(X - z)^k \in K[X]$ avec $1 \leq k < p$, alors $z^k \in K$, et en prenant une relation de Bézout, puisque k et p sont premiers entre eux, on obtient $z \in K$: c'est absurde. Ainsi $K[X]/(X^p - a)$ est une extension finie de K qui n'est pas séparable. □

Le lemme suivant, que l'on doit historiquement à Dedekind, est fondamental dans la théorie des corps.

Lemme 2.5. *(Indépendance des caractères) Soit M un monoïde (noté multiplicativement) et F un corps. L'ensemble des morphismes de monoïdes de M vers le monoïde multiplicatif F forme une famille libre du F-espace vectoriel des fonction de M vers F.*

Démonstration. On montre par récurrence sur $n \geq 0$ que toute famille $f_1, \ldots, f_n$ de morphismes distincts $M \longrightarrow F$ est libre. Pour $n = 0$ c'est clair. Supposons $n \geq 1$ et que c'est vrai au rang $n-1$. On se donne $f_1, \ldots, f_n$ une telle famille et on suppose qu'elle est liée. Sans perte de généralité, quitte à renuméroter les f_i, on peut supposer que :

$$f_n = \sum_{i<n} a_i f_i$$

avec $a_i \in F$. Ainsi pour tous $x, y \in M$, on a :

$$\sum_{i<n} a_i f_i(x) f_i(y) = \sum_{i<n} a_i f_i(xy) = f_n(xy) = f_n(x) f_n(y) = \sum_{i,j<n} a_i a_j f_i(x) f_j(y)$$

et donc :

$$\sum_{i<n} a_i f_i(y) f_i = \sum_{i,j<n} a_i a_j f_j(y) f_i$$

Par hypothèse de récurrence, la famille $(f_1, \ldots, f_{n-1})$ est libre donc pour tout i et tout y :

$$a_i f_i(y) = \sum_{j<n} a_i a_j f_j(y)$$

et encore par liberté de cette famille on obtient :

$$a_i = a_i^2$$

et :

$$a_i a_j = 0$$

pour tout $j \neq i$, $j < n$. Ainsi au plus un des a_i est non nul et vaut 1. Si tous les a_i sont nuls, on a $f_n = 0$ et c'est absurde car $f_n(1) = 1$. Sinon, il existe i tel que $f_n = f_i$, ce qui est aussi absurde. □

On en déduit la proposition suivante, qui rassemble le théorème de prolongement des caractères et le théorème de l'élément primitif.

Proposition 2.6. *Soit L/K une extension finie séparable de degré d et C un corps algébriquement clos contenant L. Il existe un élément $\alpha \in L$ (séparable) tel que $L = K[\alpha]$ (théorème de l'élément primitif). De plus il existe exactement d plongements de K-algèbres de L dans C. Ces plongements forment une famille C-libre du C-espace vectoriel des fonctions de L vers C.*

Démonstration. On commence par montrer par récurrence sur $d = [L : K]$ qu'il y a toujours d plongements de K-algèbres de L vers C. Si L est engendrée par un élément $\alpha \in L$ - de ploynôme minimal π_α séparable (car L/K est séparable) - alors on a :

$$\mathrm{Hom}_{K-\mathrm{alg}}(L, C) \cong \mathrm{Hom}_{K-\mathrm{alg}}(K[X]/(\pi_\alpha), C) \cong \{x \in C \mid \pi_\alpha(x) = 0\}$$

qui est un ensemble de cardinal $d = \deg \pi_\alpha$ car π_α est séparable et C est algébriquement clos.
Sinon, il existe $x \in L \setminus K$ et de ce qui précède on a :

$$\left|\mathrm{Hom}_{K-\mathrm{alg}}(K[x], C)\right| = [K[x] : K]$$

et puisque $L/K[x]$ est finie, séparable et de degré strictement inférieur à d, on a par récurrence, pour tout plongement K-linéaire $f : K[X] \longrightarrow C$:

$$\left|\mathrm{Hom}_{K[x]-\mathrm{alg}}(L, C)\right| = [L : K[x]]$$

en voyant C comme une $K[x]$-algèbre via f. Or on a une application de restriction :

$$\varphi : \mathrm{Hom}_{K-\mathrm{alg}}(L, C) \longrightarrow \mathrm{Hom}_{K-\mathrm{alg}}(K[x], C)$$

et pour tout $f \in \mathrm{Hom}_{K-\mathrm{alg}}(K[x], C)$ la fibre $\varphi^{-1}(f)$ est exactement l'ensemble $\mathrm{Hom}_{K[x]-\mathrm{alg}}(L, C)$ en voyant C comme une $K[x]$-algèbre via f, donc cette fibre est de cardinal $[L : K[x]]$. Puisque toutes les fibres sont de même cardinal strictement positif, on obtient que φ est surjective et que :

$$\left|\mathrm{Hom}_{K-\mathrm{alg}}(L, C)\right| = [L : K[x]] \cdot \left|\mathrm{Hom}_{K-\mathrm{alg}}(K[x], C)\right| = [L : K[x]][K[x] : K] = [L : K].$$

On démontre maintenant le théorème de l'élément primitif. Si K est fini, alors L aussi et le groupe $L^\times$ est cyclique (voir 2.30), et un générateur de ce groupe est aussi un générateur de l'extension L/K. Un tel élément est séparable car L/K est séparable.
Si K est infini, supposons par l'absurde que L/K n'est pas générée par un unique élément. Soit $x \in L$. Il y a $[K[x] : K]$ plongements de K-algèbres de $K[x]$ vers C et chacun de ces plongements se prolonge en $[L : K[x]]$ plongements de K-algèbres de L vers C, or par hypothèse $[L : K[x]] \geq 2$ donc il existe deux plongements distincts $\sigma, \tau : L \longrightarrow C$ dont les restrictions à $K[x]$ sont égales. Ainsi $\sigma(x) = \tau(x)$. On peut donc écrire :

$$L = \bigcup_{\sigma \neq \tau} \mathrm{Ker}(\sigma - \tau)$$

où la réunion porte sur les σ, τ plongements de K-algèbres de L vers C distincts. Par un résultat bien connu d'algèbre linéaire, sur un corps infini, une réunion finie de sous-espaces vectoriels stricts ne donne jamais l'espace vectoriel ambient, or les $\mathrm{Ker}(\sigma - \tau)$ sont des sous-espaces stricts car $\sigma \neq \tau$: c'est absurde.
Enfin, ces plongements forment une famille libre d'après le lemme 2.5 d'indépendance des caractères. □

Une extension finie L/K est dite *normale* si tous les plongements de K-algèbres de L dans C (un corps algébriquement clos quelconque contenant L) ont la même image, ou de façon équivalente si pour tout $x \in L$, les conjugués de x (i.e. les racines dans un corps algébriquement clos contenant L du polynôme minimal de x) sont dans L. Elle est dite *galoisienne* si elle est séparable et normale. On note alors $\mathrm{Gal}(L/K)$ le groupe des automorphismes de K-algèbre de L, et on appelle ce groupe le groupe de Galois de l'extension. La très célèbre correspondance de Galois établit un lien profond entre les sous-groupes de $\mathrm{Gal}(L/K)$ et les extensions intermédiaires.

Théorème 2.7. *(Correspondance de Galois) Soit L/K une extension finie galoisienne de groupe de Galois G. Pour H un sous-groupe de G, on note L^H le sous-corps de L (contenant K) des éléments fixés par tout élément de H. Les applications :*

$$\begin{cases} \{\text{sous-groupes de } G\} \longleftrightarrow \{\text{corps } E, \text{ avec } K \subseteq E \subseteq L\} \\ H \mapsto L^H \\ \mathrm{Gal}(L/E) \hookleftarrow E \end{cases}$$

sont réciproques l'une de l'autre et sont décroissantes. De plus $H = \mathrm{Gal}(L/E)$ est distingué si et seulement si E/K est galoisienne et on a alors une suite exacte :

$$1 \longrightarrow H \longrightarrow G \xrightarrow{\text{res}} \mathrm{Gal}(E/K) \longrightarrow 1$$

où res *est le morphisme de restriction d'un élément de G au corps E, stable par cet élément. Enfin, le cardinal de G est exactement le degré de l'extension L/K.*

Démonstration. On laisse au lecteur le soin de vérifier que L/E est toujours une extension galoisienne pour $K \subseteq E \subseteq L$. La décroissance des applications en question est claire. Considérons C un corps algébriquement clos qui contient L. Puisque tous les morphismes de K-algèbres de L dans C ont la même image et que $\mathrm{id}(L) = L$, cette image est L et donc :

$$G = \mathrm{Gal}(L/K) = \mathrm{Hom}_{K-\mathrm{alg}}(L, C)$$

et donc G est d'ordre $[L : K]$ car L/K est séparable et d'après 2.6. Donnons nous E un corps intermédiaire et H un sous-groupe de G. Les inclusions suivantes sont tautologiques :

$$H \subseteq \mathrm{Gal}(L/L^H)$$

et

$$E \subseteq L^{\mathrm{Gal}(L/E)}.$$

Il reste à voir les deux autres inclusions. Par le théorème de l'élément primitif, on peut écrire $L = K[\alpha]$ et on note alors que le polynôme :

$$f(X) = \prod_{\sigma \in H} (X - \sigma\alpha)$$

est à coefficients dans le corps L^H. En effet tout élément $\varphi \in H$ induit, en agissant sur les coefficients, un automorphisme de K-algèbre de $L[X]$ et on constate que $\varphi(f) = f$

par un changement de variable. Ainsi α est algébrique de degré au plus $|H|$ sur le corps L^H et donc :

$$|H| \leq \left|\mathrm{Gal}(L/L^H)\right| = \left[L : L^H\right] \leq |H|$$

donc :

$$\mathrm{Gal}(L/L^H) = H.$$

En appliquant cela au groupe $\mathrm{Gal}(L/E)$, on obtient $\mathrm{Gal}\left(L/L^{\mathrm{Gal}(L/E)}\right) = \mathrm{Gal}(L/E)$ donc $[L : E] = \left[L : L^{\mathrm{Gal}(L/E)}\right]$ et puisqu'on a une inclusion, on en déduit :

$$E = L^{\mathrm{Gal}(L/E)}.$$

Ensuite, si $\sigma \in G$, on vérifie facilement que :

$$L^{\sigma H \sigma^{-1}} = \sigma\left(L^H\right)$$

et donc H est distingué si et seulement si L^H est stable par G, autrement dit L^H/K est galoisienne (car tout K-plongement de L^H vers C se prolonge à L d'après 2.6). Il est alors clair que la suite de l'énoncé est exacte. □

2.2 Trace, norme et discriminant

Un des contextes les plus généraux dans lequel on peut définir la notion de *trace* et de *norme* est le suivant : on considère A un anneau commutatif et B une A-algèbre commutative libre de type fini comme A-module, de rang d. On note $\mathrm{End}_A(B)$ la A-algèbre (non commutative en général) des endomorphismes A-linéaires de B.
On a alors un morphisme de A-algèbres injectif :

$$\mu : B \hookrightarrow \mathrm{End}_A(B)$$

qui envoie b sur l'endomorphisme μ_b de multiplication par b. Il est injectif car $b \cdot 1 = b$. Pour $b \in B$, on définit alors sa trace $\mathrm{Tr}_{B/A}(b)$ comme la trace de l'endomorphisme μ_b et sa norme $N_{B/A}(b)$ comme le déterminant de l'endomorphisme μ_b. Cette trace et ce déterminant sont bien définis car B est libre de type fini sur A, et on peut donc considérer la matrice de μ_b dans une certaine base et constater que sa trace et son déterminant ne dépendent pas de la base choisie.

Remarque 2.8. De plus, ces notions sont naturelles en A au sens où si $A \longrightarrow A'$ est un morphisme d'anneaux, alors $B' = B \otimes_A A'$ est une A'-algèbre libre de type fini de rang d et les diagrammes suivants commutent :

$$\begin{array}{ccc} B & \longrightarrow & B' \\ {\scriptstyle \mathrm{Tr}_{B/A}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{B'/A'}} \\ A & \longrightarrow & A' \end{array}$$

$$\begin{array}{ccc} B & \longrightarrow & B' \\ {\scriptstyle N_{B/A}}\downarrow & & \downarrow{\scriptstyle N_{B'/A'}} \\ A & \longrightarrow & A' \end{array}$$

car, si $(b_1,\dots,b_d)$ est une A-base de B, alors c'est aussi une A'-base de B' et pour tout $x \in B$, la matrice de μ_x sur B ou B' dans la base $\underline{b}$ est exactement la même.

Étant donné $b \in B$, on définit son polynôme caractérisique $\chi_b^{B/A} \in A[X]$ comme le polynôme caractéristique de l'endomorphisme μ_b, autrement dit :

$$\chi_b^{B/A}(X) = N_{B[X]/A[X]}(b - X).$$

En vertu de la remarque 2.8, pour tout $x \in A$ on a :

$$\chi_b^{B/A}(x) = N_{B/A}(b - x)$$

en utilisant le morphisme $A[X] \longrightarrow A$ qui envoie X sur x. Ainsi, par **abus de notation** on notera souvent $N_{B/A}(b-X)$ plutôt que $N_{B[X]/A[X]}(b-X)$. Notons que, d'après Cayley-Hamilton, on a :

$$\chi_b^{B/A}(b) = 0$$

puisque $\chi_b^{B/A}$ annule μ_b et que μ est un morphisme d'anneaux injectif.
L'énoncé suivant indique que le calcul du déterminant d'une matrice par blocs dont les blocs commutent peut se faire par blocs. La preuve est celle de Silvester dans [15].

Théorème 2.9. *Soient A un anneau commutatif et m,n deux entiers naturels. Soit $M \in M_{mn}(A)$ une matrice carrée de taille mn. On peut la voir comme une matrice par blocs :*

$$M = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \dots & \alpha_{mm} \end{pmatrix}$$

avec $\alpha_{ij} \in M_n(A)$.
On suppose que les α_{ij} commutent deux à deux et on considère B une sous A-algèbre commutative de $M_n(A)$ contenant les α_{ij}. On peut ainsi voir M comme une matrice $\hat{M} \in M_m(B)$.
On a alors la formule suivante :

$$\det M = \det(\det \hat{M})$$

où $\det \hat{M} \in B \subseteq M_n(A)$.

Démonstration. On le prouve par récurrence sur m. Pour $m = 0$, c'est clair. On suppose $m \geq 1$ et que c'est vrai au rang $m-1$.
On décompose $\hat{M}$ de la façon suivante :

$$\hat{M} = \begin{pmatrix} \hat{M}' & \hat{C} \\ \hat{L} & \gamma \end{pmatrix}$$

avec $\gamma \in B$, $\hat{M}' \in M_{m-1}(B)$, $\hat{C} \in M_{1,m-1}(B)$ une colonne et $\hat{L} \in M_{m-1,1}(B)$ une ligne.
Pour des raisons techniques (de division par zéro) on a besoin d'ajouter une variable formelle et de travailler dans $A[X]$. On considère alors la matrice suivante :

$$\hat{M}_X = \begin{pmatrix} \hat{M}' & \hat{C} \\ \hat{L} & \gamma + X \end{pmatrix} \in M_{1,m-1}(B[X])$$

Dans toute cette preuve, la notation $\hat{\bullet}$ signifie qu'on regarde la même matrice mais qu'on la considère par blocs, c'est à dire comme une matrice à coefficients dans B et non dans A.
On a l'identité suivante :

$$\hat{M}_X \cdot \begin{pmatrix} (\gamma+X)\mathrm{I}_{m-1} & 0 \\ -\hat{L} & 1_B \end{pmatrix} = \begin{pmatrix} \hat{U}_X & \hat{C} \\ 0 & \gamma+X \end{pmatrix}$$

avec $\hat{U}_X = (\gamma+X)\hat{M}' - \hat{C}\hat{L} \in M_{m-1}(B)$.
D'une part, en prenant le déterminant à coefficients dans $A[X]$, on a :

$$\det M_X \cdot \det(\gamma+X)^{m-1} = \det(U_X)\det(\gamma+X) \in A[X]$$

et d'autre part en prenant le déterminant à coefficients dans $B[X]$:

$$\det \hat{M}_X \cdot (\gamma+X)^{m-1} = \det \hat{U}_X \cdot (\gamma+X) \in B[X]$$

puis en reprenant le déterminant à coefficients dans $A[X]$:

$$\det(\det \hat{M}_X) \cdot \det(\gamma+X)^{m-1} = \det(\det \hat{U}_X)\det(\gamma+X) \in A[X].$$

On soustrait alors les deux égalités pour obtenir, dans $A[X]$:

$$\det(\gamma+X)^{m-1}\left(\det(\det \hat{M}_X) - \det M_X\right) = \det(\gamma+X)\left(\det(\det \hat{U}_X) - \det U_X\right) = 0$$

par hypothèse de récurrence appliquée à U_X. Or $\det(\gamma+X)^{m-1}$ est un polynôme unitaire donc ce n'est pas un diviseur de 0 dans $A[X]$ (d'où l'intérêt d'ajouter cette variable formelle) et on obtient donc :

$$\det\left(\det \hat{M}_X\right) = \det M_X.$$

On évalue en $X = 0$, ce qui revient à considérer le morphisme d'anneaux $A[X] \longrightarrow A$ et son tensorisé par B, $B[X] \longrightarrow B$ qui envoient tous les deux X sur 0 et à utiliser le fait que le déterminant est naturel (la formule de Laplace du déterminant se comporte bien lorsqu'on change d'anneau). On obtient donc :

$$\det(\det \hat{M}) = \det M$$

comme souhaité. □

De ce théorème de calcul matriciel par blocs on déduit un énoncé de transitivité de la norme, de la trace et du polynôme caractéristique.

Théorème 2.10. *Soient A un anneau commutatif, B une A-algèbre commutative libre rang d et V un B-module libre de rang n. Soit $f \in \mathrm{End}_B(V)$. On note f_B l'endomorphisme B-linéaire f et f_A l'endomorphisme A-linéaire f. On a les égalités suivantes :*

$$\mathrm{Tr}_{B/A}(\mathrm{Tr}(f_B)) = \mathrm{Tr}(f_A) \in A$$

puis :

$$N_{B/A}(\det(f_B)) = \det(f_A) \in A$$

et :

$$N_{B/A}(\chi_{f_B}) = \chi_{f_A} \in A[X]$$

avec le même abus de notation que précedemment.
En particulier, si C est une B-algèbre commutative libre de rang t et $x \in C$, on a :

$$\mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(x)) = \mathrm{Tr}_{C/A}(x)$$

puis :

$$N_{B/A}(N_{C/B}(x)) = N_{C/A}(x)$$

et :

$$N_{B/A}\left(\chi_x^{C/B}\right) = \chi_x^{C/A}.$$

Démonstration. On fixe $\underline{b}$ une A-base de B et $\underline{v}$ une B-base de V de sorte que les $b_i v_j$ forment une A-base de V. Notons $M \in M_{dn}(A)$ la matrice de f_A dans cette base et constatons que, via le morphisme injectif :

$$\mu : B \hookrightarrow \mathrm{End}_A(B) \cong M_d(A)$$

on peut identifier B à la sous-algèbre commutative $\mu(B)$ de $M_d(A)$. En décomposant V comme $\bigoplus_{j=1}^n Bv_j$, on peut voir M comme une matrice par blocs $\hat{M} \in M_n(\mu(B))$, qui est exactement la matrice de f_B. Or, par le théorème 2.9 on a :

$$\det(\det \hat{M}) = \det M$$

autrement dit :

$$\det(\mu(\det f_B)) = \det f_A.$$

Par définition de la norme on obtient :

$$N_{B/A}(\det f_B) = \det f_A$$

comme souhaité.
En appliquant cette identité à $A[X]$ et $B[X]$ ainsi qu'à l'élément $f - X\,\mathrm{id} \in \mathrm{End}_{B[X]}(V[X])$, on obtient l'identité sur les polynômes caractéristiques. L'identité sur la trace vient du fait que :

$$\mathrm{Tr}(\mathrm{Tr}(\hat{M})) = \mathrm{Tr}(M)$$

ce qui est très facile à voir.
Les énoncés restant s'en déduisent en considérant l'endomorphisme de multiplication par c de C. □

On définit maintenant le discriminant d'une famille de d éléments de B, une A-algèbre commutative libre de rang d.

Définition 2.11. *Soient $x_1, \ldots, x_d \in B$. On définit le discriminant de la famille $(x_1, \ldots, x_d)$ comme le déterminant de la matrice symétrique $(\mathrm{Tr}_{B/A}(x_i x_j))_{i,j}$. On le note :*

$$D_{B/A}(x_1, \ldots, x_d) \in A.$$

Encore une fois, cette quantité est naturelle en A en un sens similaire à la remarque 2.8. Notons que $D_{B/A}$ peut aussi se voir comme une forme quadratique sur le A-module libre de rang 1 qu'est $\Lambda_A^d B$. En effet, c'est la forme quadratique associée à la forme bilinéaire symétrique (bien définie) suivante :

$$(x_1 \wedge \cdots \wedge x_d, y_1 \wedge \cdots \wedge y_d) \mapsto \det(\mathrm{Tr}_{B/A}(x_i y_j)).$$

En particulier le discriminant ne dépend pas de l'ordre de la famille (x_i). Ainsi si u est un endomorphisme A-linéaire de B, on a :

$$u(x_1 \wedge \cdots \wedge x_d) = \det(u) x_1 \wedge \cdots \wedge x_d$$

et donc :

$$D_{B/A}(u(x_1), \ldots, u(x_d)) = (\det(u))^2 D_{B/A}(u(x_1), \ldots, u(x_d)).$$

Dans le cas particulier où l'endomorphisme est donné par la multiplication par un $b \in B$, on obtient naturellement :

$$D_{B/A}(bx_1, \ldots, bx_d) = N_{B/A}(b)^2 D_{B/A}(x_1, \ldots, x_d).$$

On s'intéresse à présent au cas particulier des extensions finies *séparables* de corps. Si L/K est une telle extension, de degré d, L est une K-algèbre commutative libre de type fini et donc ce qui précède s'applique. On fixe C un corps algébriquement clos contenant K.
Dans ces conditions, la trace, la norme et le polynôme caractéristique peuvent se calculer à partir des plongements K-linéaires de L dans C.

Proposition 2.12. *On a les égalités suivantes pour $x \in L$:*

$$\mathrm{Tr}_{L/K}(x) = \sum_\sigma \sigma(x)$$

puis :

$$N_{L/K}(x) = \prod_\sigma \sigma(x)$$

et :

$$\chi_x(X) = \prod_\sigma (X - \sigma x)$$

où σ parcourt l'ensemble des d plongements K-linéaires de L dans C.
Ainsi les racines de χ_x sont les conjugués de x avec multiplicité.

Démonstration. Par le théorème de l'élément primitif, on peut écrire $L = K[\alpha] = K[X]/\pi$ avec $\alpha \in L$ et π le polynôme minimal de α sur K, irréductible et séparable. On numérote $\sigma_1, \ldots, \sigma_d$ les K-plongements de L dans C et $\alpha_i = \sigma_i(\alpha)$.
On a alors le diagramme commutatif suivant :

$$\begin{array}{ccc}
L \otimes_K C & \xrightarrow{\mu_x \otimes \mathrm{id}} & L \otimes_K C \\
\sim \downarrow & & \downarrow \sim \\
C[X]/\pi & \xrightarrow[\mu_Q]{} & C[X]/\pi \\
\varepsilon \downarrow & & \downarrow \varepsilon \\
C^d & \xrightarrow[A]{} & C^d
\end{array}$$

en écrivant $x = Q(\alpha)$ avec $Q \in K[X]$, avec μ_Q la multiplication par Q et ε l'isomorphisme donné par le théorème chinois qui envoie P sur $(P(\alpha_i))_i$.
La matrice A est la matrice de multiplication par $(Q(\alpha_i))_i$ et donc elle est diagonale avec comme i-ème coefficient sur la diagonale :

$$Q(\alpha_i) = Q(\sigma_i \alpha) = \sigma_i Q(\alpha) = \sigma_i(x)$$

et donc :

$$\chi_A = \prod_i (X - \sigma_i(x))$$

et c'est aussi le polynôme caractéristique de μ_x. Les égalités pour la trace et le déterminant s'en déduisent en considérant les coefficients du polynôme caractéristique. □

Proposition 2.13. *Pour une extension finie séparable L/K, la forme bilinéaire :*

$$b(x, y) = \mathrm{Tr}_{L/K}(xy)$$

est non dégénérée. C'est d'ailleurs une caractérisation des extensions séparables, mais on n'utilisera pas ce fait ici.

Démonstration. Soit $x \in L$ tel que pour tout $y \in L$ on ait :

$$b(x, y) = 0$$

autrement dit :

$$0 = \sum_\sigma \sigma(x) \cdot \sigma$$

ce qui entraîne, par le lemme d'indépendance linéaire des caractères 2.5 que tous les conjugués de x sont nuls et donc $x = 0$. □

On dispose aussi d'une formule pour le discriminant en fonction des plongements.

Proposition 2.14. *Soient $x_1, \ldots, x_d \in L$. On numérote les K-plongements de L dans C : $\sigma_1, \ldots, \sigma_d$. On a alors la formule suivante :*

$$\mathrm{Disc}(x_1, \ldots, x_d) = \det\left((\sigma_i(x_j))_{i,j}\right)^2.$$

Démonstration. Notons $M = (\sigma_i(x_j))_{i,j}$ et $B = (b(x_i, x_j))$. On a :

$$b(x_i, x_j) = \sum_k \sigma_k(x_i x_j) = \sum_k M_{k,i} M_{k,j}$$

donc $B = M^\top M$ et $\det(B) = \det(M)^2$ comme voulu. □

Corollaire 2.15. *Soit α un générateur de L/K. On note π_α son polynôme minimal. On a alors :*

$$D_{L/K}(1, \alpha, \alpha^2, \ldots, \alpha^{d-1}) = (-1)^{\binom{d}{2}} N_{L/K}(\pi'_\alpha(\alpha)) = (-1)^{\binom{d}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j)$$

avec α_i les conjugués de α dans une clotûre algébrique de L.
Cette quantité est d'ailleurs égale au discriminant du polynôme unitaire π_α définie en 1.54. Ceci justifie que ces deux notions aient le même nom.

Démonstration. On note :

$$\pi_\alpha = \prod_i (X - \alpha_i)$$

avec $\alpha_1 = \alpha$. Ainsi :

$$\pi'_\alpha = \sum_i \prod_{j \neq i} (X - \alpha_j)$$

et :

$$N_{L/K}(\pi'_\alpha(\alpha)) = N_{L/K}\left(\prod_{j=2}^{d} \alpha - \alpha_j\right) = \prod_{i \neq j} (\alpha_i - \alpha_j).$$

De plus, en utilisant la formule 2.14, le discriminant de la famille $(1, \alpha, \ldots, \alpha^{d-1})$ est le carré d'un déterminant de Vandermonde :

$$D_{L/K}(1, \alpha, \ldots, \alpha^{d-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\binom{d}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j)$$

comme souhaité. □

Enfin, mentionnons la propriété de transitivité suivante pour le discriminant dans le cas particulier des extensions finies séparables. La preuve donnée ici est celle de Joseph Rabinoff (voir [13]).

Théorème 2.16. *Soit $M/L/K$ une tour d'extensions finies séparables, avec $d = [L : K]$ et $m = [M : L]$. Soient $x_1, \ldots, x_d \in L$ et soient $y_1, \ldots, y_m \in M$. On a :*

$$D_{M/K}\left((x_i y_j)_{i,j}\right) = N_{L/K}\left(D_{M/L}(y_1, \ldots, y_m)\right) D_{L/K}(x_1, \ldots, x_d)^m.$$

Démonstration. On se donne C un corps algébriquement clos contenant K. On note $\sigma_1, \ldots, \sigma_d$ les K-plongements de L dans C et pour chaque i, on note $\tau_{i1}, \ldots, \tau_{im}$ les K-plongements de M dans C qui prolongent σ_i. Ainsi les τ_{ij} sont les K-plongements de M dans C d'après 2.6.
On considère $S \in M_d(C)$ la matrice $S_{ij} = \sigma_i(x_j)$, ainsi que $A \in M_{dm}(C)$ la matrice :

$$A_{(i,j),(k,\ell)} = \tau_{ij}(x_k y_\ell).$$

Enfin, pour tout t on considère la matrice $T^{(t)} \in M_m(C)$ définie par :

$$T^{(t)}_{ij} = \tau_{ti}(y_j).$$

On observe alors que :

$$A_{(i,j),(k,\ell)} = \tau_{ij}(x_k)\tau_{ij}(y_\ell) = \sigma_i(x_k)\tau_{ij}(y_\ell) = S_{ik} T^{(i)}_{j\ell}$$

ce qui permet d'écrire A comme une matrice par blocs de taille m :

$$A = \begin{pmatrix} S_{11}T^{(1)} & \ldots & S_{1d}T^{(1)} \\ \vdots & \ddots & \vdots \\ S_{d1}T^{(d)} & \ldots & S_{dd}T^{(d)} \end{pmatrix} = \begin{pmatrix} T^{(1)} & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & T^{(d)} \end{pmatrix} \cdot \begin{pmatrix} S_{11}I_m & \ldots & S_{1d}I_m \\ \vdots & \ddots & \vdots \\ S_{d1}I_m & \ldots & S_{dd}I_m \end{pmatrix}.$$

La deuxième matrice qui apparaît dans ce produit a des blocs qui commutent deux à deux, donc par la théorème 2.9, on a :

$$\det\begin{pmatrix} S_{11}I_m & \cdots & S_{1d}I_m \\ \vdots & \ddots & \vdots \\ S_{d1}I_m & \cdots & S_{dd}I_m \end{pmatrix} = \det(\det(S)I_m) = \det(S)^m.$$

On obtient :

$$\det(A) = \left(\prod_t \det\left(T^{(t)}\right)\right)\det(S)^m.$$

Or, d'après la formule du discriminant via les plongements 2.14 on a :

$$\det(A)^2 = D_{M/K}\left((x_i y_j)_{i,j}\right)$$

puis

$$\det(S)^2 = D_{L/K}((x_i)_i)$$

et pour tout t :

$$\det\left(T^{(t)}\right)^2 = \sigma_t\left(D_{M/L}((y_j)_j)\right)$$

en voyant C comme un corps algébriquement clos contenant L via le plongement σ_t. On en déduit la formule suivante :

$$D_{M/K}\left((x_i y_j)_{i,j}\right) = \left(\prod_t \sigma_t\left(D_{M/L}((y_j)_j)\right)\right) D_{L/K}((x_i)_i)^m = N_{L/K}\left(D_{M/L}((y_j)_j)\right) D_{L/K}((x_i)_i)^m$$

d'après la proposition 2.12. □

2.3 Treillis des sous-extensions, intersection et compositum

Soit L/K une extension quelconque de corps. L'ensemble $\mathcal{E}$ des extensions intermédiaires E/K avec $E \subseteq L$ est ordonné par l'inclusion.

Proposition 2.17. *L'ensemble ordonné $\mathcal{E}$ est un treillis : chaque paire d'éléments E, F possède une borne inférieure, en l'ocurrence l'intersection $E \cap F$ et une borne supérieure, appelée compositum de E et F et notée EF.*
Concrètement, EF est le sous-corps de L engendré par E et F.
De plus, EF et $E \cap F$ ne dépendent pas de L et K : on peut les remplacer par $L' \supseteq L$ et $K' \subseteq K$ sans changer EF et $E \cap F$.

Démonstration. On note EF le sous-corps de L engendré par E et F. Soit U un élément de $\mathcal{E}$. On a clairement :

$$(U \subseteq E) \text{ et } (U \subseteq F) \iff U \subseteq E \cap F$$

et :

$$(U \supseteq E) \text{ et } (U \supseteq F) \iff U \supseteq K(E,F) \iff U \supseteq EF$$

ce qui conclut. L'indépendance vis à vis de L et K est claire par construction. □

Remarque 2.18. En général, le compositum EF n'est pas l'ensemble des $\sum e_i f_i$ avec $e_i \in E$ et $f_i \in F$ bien que la notation puisse le suggérer. Cependant, comme le montre la proposition suivante, c'est le cas lorsque E et F sont des extensions finies de K.

Proposition 2.19. *Soient E et F des extensions finies de K. Le compositum EF est alors une extension finie de K et c'est aussi le sous-anneau de L engendré par E et F, ou encore :*

$$EF = \left\{ \sum_i e_i f_i \mid (e_i) \in E^n, (f_i) \in F^n, n \geq 0 \right\}.$$

Démonstration. Prenons $(f_1, \ldots, f_\ell)$ une K-base de F. On a :

$$EF = E(f_1, \ldots, f_\ell) = E[f_1, \ldots, f_\ell]$$

car les f_i sont algébriques sur K donc sur E, et donc EF est une extension finie de K (car engendrée par un nombre fini d'éléments algébriques).
Il est clair que $E[f_1, \ldots, f_\ell]$ est le sous-anneau de L engendré par E et F. □

Dans le cas où l'extension L/K est finie et galoisienne, la correspondance de Galois permet d'obtenir le groupe de Galois de L/EF et de $L/E \cap F$.

Proposition 2.20. *Supposons L/K galoisienne et finie de groupe de Galois G. Pour tous $E, F \in \mathcal{E}$, on a :*

$$\mathrm{Gal}(L/EF) = \mathrm{Gal}(L/E) \cap \mathrm{Gal}(L/F)$$

et :

$$\mathrm{Gal}(L/E \cap F) = \langle \mathrm{Gal}(L/E), \mathrm{Gal}(L/F) \rangle.$$

De façon équivalente, si U et V sont deux sous-groupes de G, on a :

$$L^{U \cap V} = L^U L^V$$

et :

$$L^{\langle U, V \rangle} = L^U \cap L^V.$$

Démonstration. Cela vient du fait que la correspondance de Galois induit un anti-isomorphisme d'ensemble ordonnés entre le treillis des sous-groupes de G et le treillis $\mathcal{E}$. Ainsi la borne supérieure est envoyée sur la borne inférieure et inversement. □

En général, même si $E \cap F = K$, le degré de l'extension EF/K n'est pas toujours égal au produit des degrés $[E : K]$ et $[F : K]$ (voir 2.25) pour un contre-exemple. Cependant c'est toujours vrai si les extensions E/K et F/K sont galoisiennes.
Notons que si E et F sont des extensions finies de K, d'après 2.19, le morphisme canonique $E \otimes_K F \longrightarrow EF$ est surjectif donc on a toujours :

$$[EF : K] \leq [E : K] \times [F : K].$$

Définition 2.21. *Soient E, F deux sous-corps d'un corps Ω. On suppose E et F de degré fini sur leur intersection $E \cap F$.*
On dit alors que E et F sont complémentaires (dans l'extension $EF/E \cap F$) si :

$$[EF : E \cap F] = [E : E \cap F] \times [F : E \cap F].$$

Grâce au morphisme surjectif $E \otimes_{E\cap F} F \longrightarrow EF$, cette condition équivaut à l'injectivité de ce morphisme, ou encore à ce que

$$E \otimes_{E\cap F} F$$

soit un corps.

Dans le cas où E et F sont contenus dans une extension galoisienne finie d'un sous-corps de $E \cap F$, on dispose d'une autre caractérisation.

Proposition 2.22. *Soit L/K une extension finie galoisienne et E, F deux sous-corps de L contenant K. Les énoncés suivants sont équivalents :*

- *E et F sont complémentaires.*
- *L'ensemble* $\mathrm{Gal}(L/E)\mathrm{Gal}(L/F)$ *est un sous-groupe de* $\mathrm{Gal}(L/K)$.
- *On a :* $\mathrm{Gal}(L/E)\mathrm{Gal}(L/F) = \mathrm{Gal}(L/E \cap F)$.

Démonstration. Notons $G = \mathrm{Gal}(L/K)$, $U = \mathrm{Gal}(L/E)$ et $V = \mathrm{Gal}(L/F)$. D'après la correspondance de Galois Et plus particulièrement d'après 2.20 on a :

$$U \cap V = \mathrm{Gal}(L/EF)$$

et

$$\langle U, V \rangle = \mathrm{Gal}(L, E \cap F).$$

On a la formule suivante bien connue en théorie des groupes :

$$|UV| = \frac{|U| \cdot |V|}{|U \cap V|}.$$

Or UV est un groupe si et seulement si $UV = \langle U, V \rangle$, autrement dit les points 2 et 3 sont équivalents, et cela équivaut encore à $|UV| = |\langle U, V \rangle|$, autrement dit :

$$\frac{[L : E] \cdot [L : F]}{[L : EF]} = \frac{|U| \cdot |V|}{|U \cap V|} = [L : E \cap F]$$

ce qui se réécrit :

$$[EF : E \cap F] = [E : E \cap F] \times [F : E \cap F].$$

□

En particulier, cela se produit si l'un des deux groupes $\mathrm{Gal}(L/E)$ et $\mathrm{Gal}(L/F)$ est distingué comme le montre le lemme suivant.

Lemme 2.23. *Soit G un groupe et H, K deux sous-groupes de G. On suppose que H est distingué dans G. Alors HK est un sous-groupe de G.*

Démonstration. Soient $h \in H$ et $k \in K$. On a :

$$hk = k(k^{-1}hk) \in KH$$

car H est distingué dans G. Ainsi $HK \subseteq KH$ et de même l'autre inclusion est vraie, donc :

$$HK = KH.$$

Ainsi $HKHK \subseteq HKKH \subseteq HKH \subseteq KHH \subseteq KH \subseteq HK$ donc HK est stable par produit, et $(HK)^{-1} \subseteq K^{-1}H^{-1} \subseteq KH \subseteq HK$ donc HK est stable par inverse, et clairement $1 \in HK$. □

Cela donne lieu au théorème suivant.

Théorème 2.24. *Soit Ω un corps et E, F deux sous-corps de Ω. On suppose que les extensions $E/E \cap F$ et $F/E \cap F$ sont finies et séparables. Dans ce cas $EF/E \cap F$ est finie et séparable et on a les propriétés suivantes :*

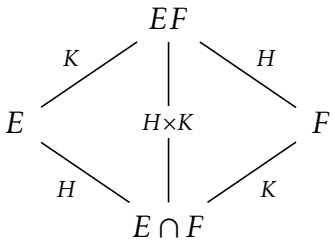
— *Si $E/E \cap F$ est galoisienne, alors E et F sont complémentaires, EF/F est galoisienne et la restriction induit un isomorphisme :*

$$\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/E \cap F).$$

— *Si $F/E \cap F$ est galoisienne, alors E et F sont complémentaires, EF/E est galoisienne et la restriction induit un isomorphisme :*

$$\mathrm{Gal}(EF/E) \cong \mathrm{Gal}(F/E \cap F).$$

— *Si $E/E \cap F$ et $F/E \cap F$ sont galoisiennes de groupes H et K, alors $EF/E \cap F$ est galoisienne de groupe $H \times K$ et on a les groupes de Galois suivants :*



Démonstration. Posons $L = EF$ et $K = E \cap F$ afin de conserver les notations précédentes. On choisit $\overline{\Omega}$ un corps algébriquement clos contenant Ω. D'après 2.19, l'extension L/K est finie. De plus, par le théorème de l'élément primitif on peut écrire $E = K[\alpha]$ avec α séparable sur K de sorte que $L = F[\alpha]$ est séparable sur F (le polynôme minimal de α sur F est séparable car il divise celui sur K), et comme F/K est séparable, L/K est séparable.
Il existe $M \supseteq L$ une extension finie galoisienne de K : en effet, par le théorème de l'élément primitif on peut écrire L comme le corps de rupture d'un polynôme séparable sur K et il suffit alors de prendre le corps de décomposition d'un tel polynôme.
Les points (i) et (ii) sont complétement symétriques, voyons le premier. Si E/K est galoisienne, E est le corps de décomposition d'un polynôme à coefficients dans K, et

L est le corps de décomposition sur F de ce même polynôme, donc c'est une extension galoisienne de F. Ensuite, le groupe $\mathrm{Gal}(M/E)$ est distingué dans $\mathrm{Gal}(M/K)$ car M/K est E/K est galoisienne. D'après le lemme 2.23, l'ensemble $\mathrm{Gal}(M/E)\mathrm{Gal}(M/F)$ est donc un sous-groupe de $\mathrm{Gal}(M/E)$ et par la proposition 2.22, on en déduit que E et F sont complémentaires. On peut donc identifier L à $E \otimes_K F$, de sorte que :

$$\mathrm{Gal}(EF/F) = \mathrm{Hom}_F(EF, \overline{\Omega}) = \mathrm{Hom}_F(E \otimes_K F, \overline{\Omega}) \cong \mathrm{Hom}_K(E, \overline{\Omega}) = \mathrm{Gal}(E/K)$$

comme voulu.
Voyons maintenant le point (iii). Dans ce cas, par ce qui précède, E et F sont complémentaires et comme L/E et E/K sont galoisiennes, L/K est galoisienne, et on note G son groupe de Galois. D'après la proposition 2.22, on a :

$$G = \mathrm{Gal}(L/E)\mathrm{Gal}(L/F)$$

et si $\sigma \in \mathrm{Gal}(L/E)$ et $\tau \in \mathrm{Gal}(L/F)$, le commutateur $[\sigma, \tau]$ agit trivialement sur E (car σ agit trivialement sur E et τ stabilise E) et il agit trivialement sur F pour la même raison, donc ce commutateur agit trivialement sur L et :

$$[\sigma, \tau] = \mathrm{id}_L .$$

Ainsi les sous-groupes $\mathrm{Gal}(L/E)$ et $\mathrm{Gal}(L/F)$ commutent, et leur intersection est triviale donc c'est un produit direct interne :

$$G \cong \mathrm{Gal}(L/E) \times \mathrm{Gal}(L/F).$$

On a donc $H = \mathrm{Gal}(E/K) = G/\mathrm{Gal}(L/E) \cong \mathrm{Gal}(L/F)$ et $K \cong \mathrm{Gal}(L/E)$ donc :

$$G \cong H \times K.$$

□

Remarque 2.25. Voici un exemple où E et F ne sont pas complémentaires dans le cas où les extensions E/K et F/K ne sont pas normales. Prenons $K = \mathbb{Q}$, et L une extension galoisienne de $\mathbb{Q}$ de groupe de Galois $G = \mathfrak{S}_5$.
Une telle extension existe : choisissons $P \in \mathbb{Q}[X]$ irréductible de degré 5 avec trois racines réelles et deux racines complexes conjuguées (par exemple $P = X^5 - 3X^3 + 1$) et prenons pour L le corps de décomposition de P sur $\mathbb{Q}$. Notons G le groupe de Galois de l'extension galoisienne $L/\mathbb{Q}$.
Puisque P est de degré 5, en considérant le sous-corps engendré par une quelconque des racines de P, on a que le cardinal de G est divisible par 5. Par le lemme de Cauchy il contient donc un élément d'ordre 5. Or via l'action de G sur les racines de P on peut considérer G comme un sous-groupe de $\mathfrak{S}_5$, et un élément d'ordre 5 est nécessairement un 5-cycle. De plus la conjugaison complexe échange les deux racines complexes en fixant les autres, donc G contient aussi une transposition. Un sous-groupe de $\mathfrak{S}_5$ qui contient un 5-cycle et une transposition est $\mathfrak{S}_5$ (on le laisse en exercice).
Une fois une telle extension $L/\mathbb{Q}$ fixée de groupe de Galois $G = \mathfrak{S}_5$, on considère U un sous-groupe engendré par une transposition et V un sous-groupe engendré par un 5-cycle (dans notre exemple on peut prendre U le sous-groupe engendré par la

conjugaison complexe).
On a alors $U \cap V = \{1\}$ et $\langle U, V \rangle = G$.
On a donc $L^U \cap L^V = \mathbb{Q}$ et $L^U L^V = L$ (dans notre exemple on aurait $L^U = \mathbb{R} \cap L$). Or UV est de cardinal 10 donc ce n'est pas G. Par la caractérisation 2.22, E et F ne sont pas complémentaires.

2.4 Extensions cycliques

Définition 2.26. *Une extension de corps L/K est dite cyclique si elle est finie et galoisienne de groupe de Galois cyclique.*

Théorème 2.27. *(Kummer) Soit L/K une extension de corps, et $n \geq 1$ un entier. On suppose que K possède n racines n-èmes de l'unité distinctes. Alors L/K est galoisienne de groupe de Galois cyclique d'ordre n si et seulement si il existe $\alpha \in L$ qui engendre l'extension L/K tel que $\alpha^n \in K$ avec n minimal pour cette propriété. Dans ce cas, le groupe de Galois s'identifie canoniquement au groupe $\mathbb{U}_n(K)$ des racines n-èmes de l'unité dans K.*

Démonstration. D'abord, supposons $L = K[\alpha]$ avec $\alpha^n \in K$ et n minimal pour cette propriété. On a la factorisation suivante dans $L[X]$:

$$X^n - \alpha^n = \prod_{\omega \in \mathbb{U}_n(K)} (X - \omega\alpha)$$

qui est un polynôme annulateur de α à coefficients dans K scindé à racines simples dans L par hypothèse sur K. Ainsi l'extension L/K est galoisienne, on note G son groupe de Galois. Le groupe G agit fidèlement sur les $\omega\alpha$ par multiplication par un élément de $\mathbb{U}_n(K)$: si $\sigma \in G$, on a $\sigma(\omega\alpha) = \omega\sigma(\alpha) = \omega\alpha\frac{\sigma(\alpha)}{\alpha}$ et $\sigma(\alpha)/\alpha$ est un élément de $\mathbb{U}_n(K)$. On a donc un morphisme injectif :

$$j : G \hookrightarrow \mathbb{U}_n(K)$$

dont l'image est un sous-groupe $\mathbb{U}_d(K)$ avec $d \mid n$. Par injectivité de ce morphisme, tout élément de G est donc d'ordre divisant d, et en particulier, pour tout $\sigma \in G$:

$$\sigma(\alpha^d) = \sigma(\alpha)^d = (j(\sigma)\alpha)^d = j(\sigma)^d \alpha^d = \alpha^d$$

donc $\alpha^d \in L^G = K$. Par minimalité de n, on a donc $d = n$ et un isomorphisme canonique :

$$G \cong \mathbb{U}_n(K)$$

qui est cyclique d'ordre n par hypothèse sur K.

Réciproquement, supposons L/K galoisienne de groupe de Galois cyclique d'ordre n et prenons σ un générateur de $G = \mathrm{Gal}(L/K)$. On a $\sigma^n = \mathrm{id}$ et $X^n - 1$ est scindé à racines simples sur K donc σ est diagonalisable comme endomorphisme K-linéaire de L. Le spectre de σ est un sous-groupe de $\mathbb{U}_n(K)$ car si $\sigma(x) = \lambda x$ et $\sigma(y) = \mu(y)$, alors $\sigma(x/y) = \lambda/\mu \cdot x/y$ et $\sigma(1) = 1$. Ce sous-groupe est un certain $\mathbb{U}_d(K)$ avec $d \mid n$, et donc

$\sigma^d = \mathrm{id}$ puisque σ est diagonalisable, et ainsi $d = n$. Le spectre de σ est donc exactement $\mathbb{U}_n(K)$ et en particulier il existe un vecteur propre α pour une valeur propre ζ racine primitive n-ème de l'unité (i.e. ζ engendre le groupe $\mathbb{U}_n(K)$). On a :

$$\sigma(\alpha) = \zeta\alpha$$

donc

$$\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n$$

donc α^n est fixé par le générateur σ de G, donc par G et ainsi $\alpha^n \in K$. Le même argument qu'avant montre que n est minimal pour cette propriété. Par la première partie du théorème, l'extension $K(\alpha)/K$ est donc galoisienne de groupe de Galois cyclique d'ordre n, donc $L = K(\alpha)$. □

Théorème 2.28. *(Hilbert 90) Soit L/K une extension cyclique de degré $n \geq 1$ et σ un générateur de $G = \mathrm{Gal}(L/K)$. Un élément $a \in L$ est de norme 1 sur K si et seulement si il existe $x \in L^\times$ tel que $a = \sigma(x)/x$. Autrement dit on a une suite exacte :*

$$1 \longrightarrow K^\times \longrightarrow L^\times \xrightarrow{\sigma/\mathrm{id}} L^\times \xrightarrow{N_{L/K}} K^\times$$

Démonstration. Soit $a \in L^\times$ de norme 1 sur K. On considère l'application K-linéaire suivante :

$$\varphi : \begin{cases} L \longrightarrow L \\ x \mapsto a\sigma(x) \end{cases}$$

Le problème revient à montrer que 1 est valeur propre de φ : en effet, si x est fixé par φ, alors $1/x$ est envoyé sur a par σ/id.
Par le théorème de l'élément primitif, on peut écrire $L = K(\alpha)$, avec $\alpha \in L$ de polynôme minimal sur K :

$$\pi_\alpha = \prod_{g \in G}(X - g\alpha) = (X - \alpha)(X - \sigma\alpha)\dots(X - \sigma^{n-1}\alpha).$$

On étend les scalaires en considérant $\hat{\varphi} = \varphi \otimes_K \mathrm{id}_L$. Par le théorème chinois, on a un isomorphisme :

$$\eta : L \otimes_K L = L[X]/(\pi_\alpha) \longrightarrow L^n$$

donné par $P(X) \mapsto (P(\alpha), P(\sigma\alpha), \dots, P(\sigma^{n-1}\alpha))$. Par cet isomorphisme, φ s'identifie à l'application ψ suivante :

$$\begin{array}{ccc} L \otimes_K L & \xrightarrow{\hat{\varphi}} & L \otimes_K L \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta} \\ L^n & \xrightarrow[\psi]{} & L^n \end{array}$$

On a, pour tout $P \in K[X]$ et tout $\lambda \in L$:

$$\psi(P(\alpha), P(\sigma\alpha), \dots, P(\sigma^{n-1}\alpha)) = \eta \circ \hat{\varphi}(P(\alpha) \otimes 1) = \eta(a\sigma(P(\alpha)) \otimes 1)$$

et il existe alors $Q \in K[X]$ tel que $a\sigma(P(\alpha)) = Q(\alpha)$, de sorte que :

$$\begin{aligned}\psi(P(\alpha), P(\sigma\alpha), \dots, P(\sigma^{n-1}\alpha)) &= (Q(\alpha), Q(\sigma\alpha), \dots, Q(\sigma^{n-1}(\alpha))) \\ &= (Q(\alpha), \sigma Q(\alpha), \dots, \sigma^{n-1} Q(\alpha)) \\ &= (aP(\sigma\alpha), \sigma(a)P(\sigma^2\alpha), \dots, \sigma^{n-1}(a)P(\sigma^n\alpha))\end{aligned}$$

et donc pour tout $(x_1, \dots, x_n) \in L^n$:

$$\psi(x_1, \dots, x_n) = (ax_2, \sigma(a)x_3, \dots, \sigma^{n-2}(a)x_n, \sigma^{n-1}(a)x_1)$$

et donc le polynôme caractéristique de ψ est donné par :

$$\det(T\,\mathrm{id} - \psi) = T^n - \sigma^{n-1}(a)(-1)^{n-1}\prod_{i=0}^{n-2}(-\sigma^i(a)) = T^n - \prod_{g\in G} ga = T^n - N_{L/K}(a) = T^n - 1$$

donc 1 est valeur propre de ψ, donc de $\hat{\varphi}$ et donc de φ. □

On mentionne ici une application simple de ce résultat.

Proposition 2.29. *Soit K un corps fini de cardinal $q = p^k$ avec $p \geq 3$ et $C(K) = \{(x, y) \in K^2 \mid x^2 + y^2 = 1\}$. Il s'agit du groupe des K-points du cercle d'équation $x^2 + y^2 = 1$, et la loi de groupe est donnée par $(x, y) \cdot (x', y') = (xx' - yy', xy' + x'y)$. Alors on a :*

$$|C(K)| = \begin{cases} q - 1 & \text{si } p \equiv 1\ [4] \text{ ou } p^2 \mid q \\ q + 1 & \text{sinon} \end{cases}$$

Démonstration. Il y a deux cas à traiter selon si $X^2 + 1$ est scindé ou non dans K.
S'il n'est pas scindé, l'extension $K(i)/K$ est cyclique d'ordre 2 avec $i^2 = -1$. Par le théorème 90 de Hilbert (2.28) on a donc une suite exacte :

$$1 \longrightarrow K^\times \longrightarrow K(i)^\times \xrightarrow{\sigma/\mathrm{id}} K(i)^\times \xrightarrow{N_{K(i)/K}} K^\times$$

avec $\sigma(x + iy) = x - iy$. Or $C(K)$ s'identifie au noyau de la norme en identifiant K^2 et $K(i)$, et donc :

$$|C(K)| = \frac{|K(i)^\times|}{|K^\times|} = \frac{q^2 - 1}{q - 1} = q + 1.$$

Ensuite, si $X^2 + 1$ est scindé dans K, notons j et $-j$ ses deux racines dans K. On a alors un isomorphisme de groupes :

$$C(K) \longrightarrow K^\times$$

donné par $(x, y) \mapsto x + jy$, dont la réciproque est :

$$z \mapsto \left(\frac{z + z^{-1}}{2}, \frac{z - z^{-1}}{2j}\right)$$

Enfin, si $p \equiv 1\ [4]$, la première loi complémentaire de la réciprocité quadratique donne que $X^2 + 1$ est scindé dans K, et si $p \equiv 3\ [4]$, il est scindé dans K si et seulement si K contient $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2 + 1)$, d'où le résultat. □

2.5 Corps finis

On rappelle ici les propriétés de base des corps finis. Pour tout corps K, on a un unique morphisme d'anneau $\mathbb{Z} \longrightarrow K$ et son noyau est un idéal maximal de $\mathbb{Z}$, engendré par un élément positif appelé la *caractéristique* de K : c'est soit 0, auquel cas $\mathbb{Q}$ s'injecte dans K, soit un nombre premier p, auquel cas le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ s'injecte dans K.
Pour un corps fini K, la caractéristique est toujours un nombre premier p et ainsi K est une extension finie de $\mathbb{F}_p$. Son cardinal est donc une puissance de p.
Le théorème suivant donne la structure des sous-groupes finis du corps multiplicatif d'un corps.

Théorème 2.30. *Soit K un corps. Les sous-groupes finis du groupe multiplicatif $K^\times$ sont cycliques et ce sont exactement les groupes $\mathbb{U}_n(K)$ des racines n-èmes de l'unité dans K. En particulier, si K est fini, alors $K^\times$ est un groupe cyclique.*

Démonstration. Soit G un sous-groupe fini de $K^\times$ de cardinal $n \geq 1$. Par le théorème de Lagrange on a :

$$G \subseteq \mathbb{U}_n(K)$$

Or $|\mathbb{U}_n(K)| \leq n$ car le polynôme $X^n - 1$ a au plus n racines dans K. Donc :

$$G = \mathbb{U}_n(K)$$

et il reste à voir que G est cyclique. Puisque c'est un groupe fini abélien, il existe un élément $\omega \in G$ d'ordre d l'exposant de G, c'est à dire le ppcm des ordres des éléments de G. Ainsi l'ordre de tout élément de G divise d, et donc :

$$G \subseteq \mathbb{U}_d(K)$$

et ainsi :

$$|G| \leq |\mathbb{U}_d(K)| \leq d$$

donc $n = d$ et ω engendre G. □

Proposition 2.31. *Pour tout entier q de la forme p^r avec p un nombre premier et $r \geq 1$, il existe, à isomorphisme près, un unique corps fini de cardinal q. Un tel corps est noté $\mathbb{F}_q$.*

Démonstration. On considère $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$ et on définit l'endomorphisme de *Frobenius* suivant :

$$\varphi_q(x) = x^q$$

sur $\overline{\mathbb{F}_p}$. C'est bien un endomorphisme d'anneau car $\varphi_q = \varphi_p \circ \cdots \circ \varphi_p$ et φ_p en est un (voir 2.3). Notons F le sous-corps des points fixes de φ_q et voyons que $|F| = q$.
Pour cela, on observe que, pour $x \in \overline{\mathbb{F}_p} \setminus \{0\}$:

$$x \in F \iff x^q = x \iff x^{q-1} = 1$$

de sorte que $F = \mathbb{U}_{q-1}(\overline{\mathbb{F}_p}) \cup \{0\}$. Ainsi F est de cardinal au plus q (un polynôme de degré q a au plus q racines dans un corps), et il est exactement de cardinal q car le polynôme :

$$X^{q-1} - 1$$

est scindé à racines simples dans $\overline{\mathbb{F}_p}$ car ce corps est algébriquement clos et car $X^{q-1}-1$ est séparable (il est premier à sa dérivée).
On a donc montré l'existence d'un corps de cardinal q. Pour l'unicité, donnons-nous K un corps de cardinal q. Le groupe multiplicatif $K^\times$ est cyclique engendré par un certain α, de sorte que :

$$K = \mathbb{F}_p[\alpha]$$

et $\alpha^{q-1} = 1$. De plus α est séparable sur $\mathbb{F}_p$ car annulé par $X^{q-1}-1$ et donc il existe un plongement :

$$K \longrightarrow \overline{\mathbb{F}_p}$$

donné en envoyant α sur une racine du polynôme minimal de α. On peut donc supposer que K est contenu dans $\overline{\mathbb{F}_p}$, et on a alors, puisque $K^\times$ est cyclique :

$$K^\times = F^\times = \mathbb{U}_{q-1}(\overline{\mathbb{F}_p})$$

donc $K = F$. □

Puisque tout corps fini est parfait, une extension de corps finis est toujours séparée. Le théorème suivant montre qu'une telle extension est tojours galoisienne de groupe de Galois cyclique.

Théorème 2.32. *Soit L/K une extension de corps finis. On note $q = |K|$. Alors l'extension L/K est galoisienne et son groupe de Galois est cyclique : il est engendré par la Frobenius $x \mapsto x^q$.*

Démonstration. Le nombre q est une puissance d'un certain nombre premier p. L'extension est normale car $\overline{\mathbb{F}_p}$ ne contient qu'un seul corps de cardinal q d'après la preuve de 2.31. De plus, le Frobenius φ_q est bien un élément de $\mathrm{Gal}(L/K)$ car tout élément de $K^\times$ est une racine $q-1$-ème de l'unité, donc est fixé par φ_q. Ensuite, on a vu dans la preuve de 2.31 que le corps fixé par φ_q est exactement K donc :

$$K = L^{\langle \varphi_q \rangle}$$

en notant $\langle \varphi_q \rangle$ le sous-groupe de $\mathrm{Gal}(L/K)$ engendré par φ_q. Par correspondance de Galois, on a donc :

$$\mathrm{Gal}(L/K) = \langle \varphi_q \rangle.$$

□

Proposition 2.33. *Soit q une puissance de nombre premier p et $r, s \geq 1$. Le corps $\mathbb{F}_{q^r}$ se plonge dans le corps $\mathbb{F}_{q^s}$ si et seulement si $r \mid s$.*

Démonstration. Quitte à tout plonger dans $\overline{\mathbb{F}_p}$, il suffit de montrer que :

$$\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^s} \iff r \mid s$$

car $\overline{\mathbb{F}_p}$ ne contient qu'une seule copie de chaque $\mathbb{F}_\ell$ avec ℓ puissance de p.
Or on a :

$$\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^s} \iff \mathbb{U}_{q^r-1}(\overline{\mathbb{F}_p}) \subseteq \mathbb{U}_{q^s-1}(\overline{\mathbb{F}_p}) \iff q^r - 1 \mid q^s - 1 \iff r \mid s.$$

En effet, si $s = rk + d$ avec $0 \leq d < r$, alors :

$$q^s \equiv q^d \ [p^r - 1]$$

donc $q^r - 1 \mid q^s - 1$ si et seulement si $q^r - 1 \mid q^d - 1$, ce qui équivaut à avoir $d = 0$. □

Remarque 2.34. En pratique, on construit les corps $\mathbb{F}_q$ comme corps de décomposition de polynômes irréductibles sur $\mathbb{F}_p$. Si $I_{q,d}$ désigne l'ensemble des polynômes irréductibles unitaires à coefficients dans $\mathbb{F}_q$ de degré d, on a la factorisation suivante, pour tout $n \geq 1$:

$$X^{q^n} - X = \prod_{x \in \mathbb{F}_{q^n}} (X - x) = \prod_{d \mid n} \prod_{P \in I_{q,d}} P$$

en regroupant les x selon leur polynôme minimal sur $\mathbb{F}_q$ et en utilisant la proposition précédente. On en déduit, en prenant les degrés :

$$q^n = \sum_{d \mid n} \left| I_{q,d} \right| d$$

dont on tire une formule pour le nombre de polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$ par inversion de Möbius :

$$\left| I_{q,n} \right| = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{\frac{n}{d}}.$$

Si L/K est une extension de corps finis, elle est séparable donc la trace $\mathrm{Tr}_{L/K}$ est une forme linéaire non nulle donc surjective $L \longrightarrow K$. La proposition suivante montre que la norme aussi est surjective.

Proposition 2.35. *Soit L/K une extension de corps finis. On note $q = |K|$ et $d = [L : K]$. Pour tout $x \in L$ on a :*

$$N_{L/K}(x) = x^{\frac{q^d - 1}{q - 1}}$$

et le morphisme norme $L^\times \longrightarrow K^\times$ est surjectif.

Démonstration. On fixe α un générateur du groupe cyclique $L^\times$, et on a, puisque l'extension est galoisienne de groupe de Galois engendré par $x \mapsto x^q$:

$$N_{L/K}(\alpha) = \prod_{g \in \mathrm{Gal}(L/K)} g\alpha = \prod_{i=0}^{d-1} \alpha^{q^i} = \alpha^{1 + q + \cdots + q^{d-1}} = \alpha^{\frac{q^d - 1}{q - 1}}.$$

La formule s'étend à tout $L^\times$ et à tout L, et le morphisme norme est surjectif car l'image de α est une racine de l'unité d'ordre $q - 1$, donc engendre $K^\times$. □

Deuxième partie

Théorie algébrique des nombres dans une extension d'anneaux de Dedekind

Chapitre 3

Anneaux de Dedekind

> Les nombres sont des créations libres de l'esprit humain ; ils servent à mieux saisir et à distinguer plus nettement les différences entre les choses.
>
> Richard Dedekind, Essays on the theory of numbers (1901)

3.1 Idéaux fractionnaires

On fixe A un anneau *intègre* de corps des fractions K. La notion d'idéal fractionnaire permet de généraliser la notion de nombres usuels. Cette intuition provient de Dedekind qui parle de *nombres idéaux*.

Définition 3.1. *Un idéal fractionnaire de A est un sous-A-module de K de la forme $J = \alpha I$ avec I un idéal de A et $\alpha \in K$. Il est principal s'il est de la forme $J = \alpha(x)$ avec $x \in A$, ou de manière équivalente s'il est monogène comme A-module.*

Remarque 3.2. Un idéal fractionnaire est un idéal de A si et seulement si il est contenu dans A. Le produit de deux idéaux fractionnaires (principaux) est un idéal fractionnaire (principal).

On note $\mathcal{F}(A)$ l'ensemble des idéaux fractionnaires de A. C'est un monoïde commutatif pour le produit des idéaux fractionnaires, de neutre A. On note également $\mathrm{Princ}(A)$ le sous-monoïde de $\mathcal{F}(A)$ formé des idéaux principaux *non nuls* de A.

Définition 3.3. *Un idéal fractionnaire J est dit inversible s'il est inversible dans $\mathcal{F}(A)$, c'est à dire s'il existe $K \in \mathcal{F}(A)$ tel que $JK = A$. L'ensemble des idéaux fractionnaires inversibles est le groupe des inversibles de $\mathcal{F}(A)$, noté $\mathcal{F}(A)^\times$.*

Lemme 3.4. *Tout idéal fractionnaire principal non nul est inversible. Autrement dit,* $\mathrm{Princ}(A)$ *est un sous-groupe de $\mathcal{F}(A)^\times$.*

Démonstration. On a $(Ax)(Ax^{-1}) = A$ pour $x \neq 0$. □

Définition 3.5. *Le quotient $\mathcal{F}(A)^\times/\mathrm{Princ}(A)$ est appelé groupe des classes de l'anneau intègre A. On le note* $\mathrm{Cl}(A)$.

On donne à présent une caractérisation plus agréable des idéaux fractionnaires inversibles à l'aide du théorème 1.50. Pour cela, si J est un idéal fractionnaire de A (inversible ou non), on définit son *quasi-inverse* J^{-1} ainsi :

$$J^{-1} = \{x \in K \mid xJ \subseteq A\}$$

On fera attention au fait que J^{-1} est un sous A-module de K mais n'est pas un idéal fractionnaire en général, par exemple le quasi-inverse de (0) est K.

Théorème 3.6. *Soit J un idéal fractionnaire de A non nul. Les énoncés suivants sont équivalents :*

(i) J *est inversible.*

(ii) J *est un A-module projectif.*

(iii) J *est un A-module projectif de type fini.*

(iv) Il existe $e_1, \dots, e_n \in J$ et $\alpha_1, \dots, \alpha_n \in J^{-1}$ vérifiant :

$$1 = \sum_i \alpha_i e_i$$

(v) $JJ^{-1} \supseteq A$

(vi) $JJ^{-1} = A$

Dans ce cas, J^{-1} est un idéal fractionnaire de A et c'est l'inverse de J dans le groupe $\mathcal{F}(A)^\times$.

Démonstration. Supposons J inversible et notons K son inverse dans $\mathcal{F}(A)^\times$. On a $JK = A$ donc $K \subseteq J^{-1}$ et $A \subseteq JK \subseteq JJ^{-1}$. Ainsi (i) implique (v), puis (v) implique (vi) car on a toujours $JJ^{-1} \subseteq A$. Ensuite (vi) entraîne (iv).
Voyons que (iv) implique (iii) : on écrit $1 = \sum_i \alpha_i e_i$ avec $e_i \in J$ et $\alpha_i \in J^{-1}$. La multiplication par α_i, notée μ_i, est une forme linéaire sur J, et on a, pour tout $x \in J$:

$$x = \sum_i \alpha_i x e_i = \sum_i \mu_i(x) e_i$$

donc J est de type fini (car engendré par les e_i) et projectif par le théorème 1.51. Ensuite (iii) implique (ii).

Supposons alors (ii). Par le théorème 1.51 il existe $(\alpha_i)_i$ une famille (éventuellement infinie) de forme linéaires sur J et $(e_i)_i$ une famille d'éléments de M tels que pour tout $x \in J$ on ait :

$$x = \sum_i \alpha_i(x) e_i$$

Puisque $J \neq 0$, on dispose d'un $b \in J \setminus \{0\}$. On a :

$$b = \sum_i \alpha_i(b) e_i$$

donc

$$1 = \sum_i \frac{\alpha_i(b)}{b} e_i$$

Ensuite, montrons que $\alpha_i(b)/b \in J^{-1}$: pour tout $x \in J$, on a :

$$\frac{\alpha_i(b)}{b} x = \frac{\alpha_i(x)}{b} b = \alpha_i(x) \in A$$

On a utilisé le résultat intermédiaire suivant : $\alpha_i(b)x = \alpha_i(x)b$. Pour l'obtenir, J étant un idéal fractionnaire, il existe $s \in A \setminus \{0\}$ tel que $sJ \subseteq A$, et donc :

$$\alpha_i(b)x = \alpha_i(b)\frac{sx}{s} = \frac{\alpha_i(sxb)}{s} = \frac{\alpha_i(x)sb}{s} = \alpha_i(x)b$$

par A-linéarité de α_i. On a donc montré que (ii) implique (iv). Clairement (iv) implique (vi), et (vi) implique (i) car si $JJ^{-1} = A$, alors en prenant $b \in J \setminus \{0\}$ on a $bJ^{-1} \subseteq A$ donc J^{-1} est un idéal fractionnaire. □

3.2 Anneaux de valuation

Définition 3.7. *Un anneau de valuation est un anneau intègre A dont la relation de divisibilité est totale : pour tous $a, b \in A$, ou bien $a \mid b$ ou $b \mid a$.*

On peut également utiliser les caractérisations suivantes :

Proposition 3.8. *Soit A un anneau intègre de corps des fractions K. Les énoncés suivants sont équivalents :*

(i) A est un anneau de valuation.

(ii) Les idéaux de A sont totalement ordonnés par l'inclusion.

(iii) Pour tout $x \in K \setminus \{0\}$ on a $x \in A$ ou $1/x \in A$.

Démonstration. Il est clair que (ii) implique (i) grâce aux idéaux principaux, et (i) entraîne (iii) ne pose aucun problème. Enfin, si (iii) est vrai, soient I et J deux idéaux vérifiant $I \not\subseteq J$: on prend $a \in I \setminus J$ et on a, pour tout $x \in J \setminus \{0\}$, $x/a \in A$ ou $a/x \in A$. Dans le premier cas on obtient $x \in I$ et le second cas entraîne $a \in I$, ce qui est exclu. Ainsi on a $J \subseteq I$ et on a montré (ii). □

Proposition 3.9. *Un anneau de valuation est local.*

Démonstration. Les idéaux d'un anneau de valuation sont totalement ordonnés par l'inclusion donc il n'y a qu'un seul idéal maximal (car un tel anneau est non nul, étant intègre). □

3.3 Anneaux de valuation discrète

Définition 3.10. *Soit K un corps. Une valuation discrète sur K est une application $\nu : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ vérifiant pour tous $x, y \in K$:*

(i) $\nu(x) = \infty \iff x = 0$

(ii) $\nu(xy) = \nu(x) + \nu(y)$

(iii) $\nu(x+y) \geq \min(\nu(x), \nu(y))$

(iv) ν *est surjective.*

L'ensemble des éléments de K de valuation positive ou nulle est alors un sous-anneau de K, appelé anneau de valuation discrète associé à (K, ν). En effet, $\nu(1) = 0$ car $\nu(1 \times 1) = \nu(1) + \nu(1)$.
On appelle anneau de valuation discrète un anneau intègre qui est l'anneau de valuation discrète associé à un corps muni d'une valuation discrète.

Lemme 3.11. *Soient K, ν et A comme ci-dessus. Un élément $x \in A$ est inversible si et seulement si $\nu(x) = 0$, et on a, pour $x \neq 0$:*

$$\nu(1/x) = -\nu(x)$$

Enfin, K est le corps des fractions de A et A est un anneau de valuation.

Démonstration. Le second point est immédiat.
Si x est inversible, alors $\nu(x^{-1}) = -\nu(x) \geq 0$ et $\nu(x) \geq 0$ donc $\nu(x) = 0$. Si $\nu(x) = 0$, alors $\nu(x^{-1}) = 0$ donc $x^{-1} \in A$ et x est inversible.
Soit $x \in K \setminus A$. On a $\nu(x) < 0$ donc $\nu(x^{-1}) > 0$ donc $x^{-1} \in A$, ce qui montre que A est un anneau de valuation et que K est le corps des fractions de A. □

Exemple 3.12. *Un exemple typique est le corps $\mathbb{Q}$ muni de la valuation p-adique avec p un nombre premier. L'anneau de valuation associé est alors $\mathbb{Z}_{(p)}$, le localisé de $\mathbb{Z}$ en l'idéal premier (p). Un autre exemple est le corps des fractions rationnelles sur un corps k, $k(X)$, avec pour valuation l'ordre d'annulation en 0 (négatif si 0 est un pôle).*

Remarque 3.13. Un anneau de valuation discrète est en particulier un anneau de valuation, et la relation de divisibilité s'y vérifie facilement : on a $a \mid b$ si et seulement si $\nu(a) \leq \nu(b)$.

Définition 3.14. *Soient K, ν et A comme avant. Un élément de A de valuation égale à 1 est appelé une uniformisante de A. Il en existe car ν est supposée surjective. Elle est de plus unique à un coefficient inversible près.*

On peut réécrire l'arithmétique de A en fonction d'une uniformisante.

Proposition 3.15. *Soient K, ν et A comme avant et π une uniformisante de A. Alors (π) est l'unique idéal maximal de A, les idéaux non nuls de A sont les (π^k), en particulier A est principal donc factoriel, le seul élément irréductible de A est π et pour tout $x \in A$, la valuation $\nu(x)$ est aussi la valuation π-adique de x.*

Démonstration. Soit I un idéal non nul de A et $x \in I$ de valuation minimale $d \geq 0$. Alors x et π^d ont même valuation donc sont associés et $I = (\pi^d)$ par minimalité de d. Tout le reste en découle directement. □

Les anneaux à valuation discrète possèdent donc une arithmétique très élémentaire. On introduit la définition suivante sur les anneaux :

Définition 3.16. *Un anneau A est dit de dimension de Krull au plus* 1 *si tous ses idéaux premiers non nuls sont maximaux.*

Remarque 3.17. La notion de *dimension de Krull* provient de la géométrie algébrique, mais il n'est pas nécessaire de comprendre cette notion dans sa généralité pour lire ce cours.

On peut caractériser les anneaux de valuation discrète de plusieurs façons :

Théorème 3.18. *Soit A un anneau intègre qui n'est pas un corps. Les énoncés suivants sont équivalents :*

(i) *A est un anneau à valuation discrète.*

(ii) *A est principal et local.*

(iii) *A est factoriel avec exactement un élément irréductible à association près.*

(iv) *A est noéthérien et local avec un idéal maximal principal.*

(v) *A est noéthérien, local, intégralement clos et de dimension de Krull au plus* 1.

Démonstration. On a déjà vu que (i) entraîne (ii) et (iii). Réciproquement, (ii) entraîne (i) en considérant (π) l'idéal maximal et en prenant comme valuation sur K la valuation π-adique, ce qui est possible car A n'est pas un corps. De même, on montre $(iii) \implies (i)$ en considérant la valuation π-adique pour π un irréductible de A. Les points (i), (ii) et (iii) sont donc équivalents.
Ensuite on a clairement $(ii) \implies (iv)$. Réciproquement, supposons que (iv) est vrai et soit I un idéal non nul de A. On prend (π) l'unique idéal maximal de A. A étant noéthérien, I est de type fini, de la forme $(x_1, \dots, x_n)$ avec $x_i \neq 0$, et sans perte de généralité on peut supposer que x_1 est de valuation π-adique minimale parmi les x_i. Ainsi x_1 divise tous les x_i car tout élément de valuation π-adique nulle n'est pas dans l'unique idéal maximal donc est inversible. On a donc $I = (x_1)$ et A est principal. Ainsi (i), (ii), (iii) et (iv) sont équivalents.

Supposons $(i), \dots, (iv)$ et montrons (v). A est déjà noéthérien et local. Il est de dimension de Krull au plus 1 car ses idéaux non nuls sont les (π^k) et seul (π) est premier, et il est aussi maximal. L'anneau A étant factoriel, il est intégralement clos par le lemme 1.43.

Enfin, supposons (v) et montrons (iv). On note $\mathfrak{m}$ l'idéal maximal de A. On veut montrer qu'il est principal. On a $\mathfrak{m}/\mathfrak{m}^2 \neq 0$ par le lemme de Nakayama car $\mathfrak{m}$ est de type fini. On prend $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$ et on va montrer que $\mathfrak{m} = (\pi)$. On a déjà $(\pi) \subseteq \mathfrak{m}$, et :

$$\sqrt{(\pi)} = \mathfrak{m}$$

car $\sqrt{(\pi)}$ est l'intersection des idéaux premiers contenant π, or A est de dimension de Krull au plus 1 donc il n'y a que $\mathfrak{m}$ dans cette intersection.
Puisque $\mathfrak{m}$ est de type fini, il existe donc $\ell \geq 1$ minimal tel que $\mathfrak{m}^\ell \subseteq (\pi)$. Si $\ell = 1$ on a gagné. Sinon, il existe $\alpha \in \mathfrak{m}^{\ell-1} \setminus (\pi)$. On va montrer que $\beta = \alpha/\pi$ est *entier sur A*, c'est à dire annulé par un polynôme unitaire à coefficients dans A.
On a $\beta\mathfrak{m} \subseteq A$ par construction (en effet $\beta\mathfrak{m} = (\alpha/\pi)\mathfrak{m} \subseteq (\pi)/\pi \subseteq A$). De plus $\beta\mathfrak{m} \neq A$, sans quoi on peut écrire $1 = \beta m$ avec $m \in \mathfrak{m}$ et donc $\pi = \alpha m \in \mathfrak{m}^2$ car $\ell \geq 2$, et c'est absurde. Ainsi $\beta\mathfrak{m} \subseteq \mathfrak{m}$ car $\mathfrak{m}$ est le seul idéal maximal de A. On dispose donc d'un endomorphisme μ_β du A-module $\mathfrak{m}$ de multiplication par β. Mais le A-module $\mathfrak{m}$ est de type fini. Par le théorème de Cayley-Hamilton, l'endomorphisme μ_β est donc annulé par P un polynôme unitaire à coefficients dans A et donc β est entier sur A (on utilise ici l'intégrité de A et le fait que $\mathfrak{m} \neq 0$ pour passer de $P(\mu_\beta) = 0$ à $P(\beta) = 0$). Puisque A est intégralement clos, on a alors $\beta \in A$ et donc $\alpha \in (\pi)$, ce qui est absurde. □

Remarque 3.19. Un anneau de valuation (qui n'est pas un corps) est un anneau de valuation discrète si et seulement si il est noéthérien.

Théorème 3.20. *Soit A un anneau à valuation discrète d'idéal maximal $\mathfrak{m} = (\pi)$ et de corps résiduel $\kappa = A/\mathfrak{m}$. Alors pour tous $n \geq 0$, le quotient $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ est un κ-espace vectoriel de dimension 1. Par convention, $\mathfrak{m}^0 = A$.*
De plus, chaque $1 + \mathfrak{m}^n$ (pour $n \geq 1$) est un sous-groupe de $A^\times$ et on a un isomorphisme de groupes :

$$A^\times/(1 + \mathfrak{m}) \cong \kappa^\times$$

et pour tout $n \geq 1$ des isomorphismes de groupes :

$$\frac{1 + \mathfrak{m}^n}{1 + \mathfrak{m}^{n+1}} \cong \kappa$$

Démonstration. L'idéal $\mathfrak{m}$ agit trivialement sur $\mathfrak{m}^n/\mathfrak{m}^{n+1}$, ce qui en fait un κ-espace vectoriel. Ensuite on a un isomorphisme de A-modules :

$$A \longrightarrow \mathfrak{m}^n$$

qui envoie 1 sur π^n. En tensorisant par κ cela donne un isomorphisme de κ-espaces vectoriels :

$$\kappa \longrightarrow \mathfrak{m}^n \otimes_A \kappa = \mathfrak{m}^n/\mathfrak{m}^{n+1}.$$

Il est facile de vérifier que les $1 + \mathfrak{m}^n$ avec $n \geq 1$ sont des sous-groupes de $A^\times$ (car tout élément hors de $\mathfrak{m}$ est inversible). On a ensuite une première suite exacte :

$$1 \longrightarrow 1 + \mathfrak{m} \longrightarrow A^\times \longrightarrow \kappa^\times \longrightarrow 1$$

induite par le quotient $A \longrightarrow \kappa$. Cette suite donne le premier isomorphisme.
Ensuite, on a une bijection ensembliste :

$$A \longrightarrow 1 + \mathfrak{m}^n$$

qui envoie λ sur $1 + \lambda\pi^n$. Par cette bijection, la relation d'équivalence sur A associée au quotient par $\mathfrak{m}$ correspond à la relation d'équivalence sur $1 + \mathfrak{m}^n$ associée au quotient par $1 + \mathfrak{m}^{n+1}$. On obtient donc une bijection :

$$\kappa \longrightarrow \frac{1 + \mathfrak{m}^n}{1 + \mathfrak{m}^{n+1}}$$

et un calcul direct montre que c'est un morphisme de groupes. □

3.4 Anneaux de Dedekind

Les anneaux de Dedekind sont une vaste généralisation des anneaux principaux. Ils permettent une arithmétique riche au niveau des idéaux, avec un théorème de factorisation unique d'un idéal en produit d'idéaux premiers. Ils apparaissent naturellement en théorie des nombres comme anneaux d'entiers de corps de nombres. On verra plusieurs caractérisations équivalentes d'un anneau de Dedekind, mais la définition avec laquelle on commencera à les étudier est la suivante :

Définition 3.21. *Un anneau de Dedekind est un anneau intègre dont tout idéal non nul est inversible.*

Pour un anneau de Dedekind A, le groupe des classes $\mathrm{Cl}(A)$ mesure le *défaut de principalité* de l'anneau A : A est principal si et seulement si $\mathrm{Cl}(A)$ est le groupe trivial.

Remarque 3.22. Dans la définition, on peut demander aussi bien que tout idéal non nul soit inversible ou que tout idéal fractionnaire non nul soit inversible, c'est équivalent car si $J = xI$ avec $x \in K\backslash\{0\}$ et I un idéal inversible, alors J est inversible d'inverse $x^{-1}I^{-1}$.
Un anneau *principal (et intègre)* est toujours un anneau de Dedekind car tout idéal principal non nul est inversible.

L'objectif de ce paragraphe est de donner une caractérisation beaucoup plus facile à vérifier pour les anneaux de Dedekind. Pour cela, on va d'abord traduire le fait que A soit un anneau de Dedekind sur les localisés de A. Ce type d'étude est courant en géométrie algébrique : on étudie une propriété globale et on se demande si elle peut provenir d'informations locales. D'abord, voici quelques rappels sur des propriétés de localisation :

Proposition 3.23. *Soit A un anneau et S une partie multiplicative de A. Si A est noéthérien, alors $S^{-1}A$ aussi.*

Démonstration. Soit $I_1 \subseteq I_2 \subseteq \dots$ une suite croissante d'idéaux de $S^{-1}A$, on note $f : A \longrightarrow S^{-1}A$ le morphisme de localisation. La suite des images inverses f^*I_k est croissante donc stationnaire car A est noéthérien. Or $S^{-1}f^*I_k = I_k$ donc la suite des I_k stationne aussi en appliquant S^{-1}. □

Proposition 3.24. *Soit A un anneau intègre et S une partie multiplicative de A ne contenant pas 0. Si A est intégralement clos, alors $S^{-1}A$ aussi. De plus, A est intégralement clos si et seulement si tous les $A_{\mathfrak{m}}$ le sont, avec $\mathfrak{m}$ idéal maximal de A.*

Démonstration. Supposons A intégralement clos et soit $x \in K$ (le corps des fractions de A et $S^{-1}A$ car S ne contient pas 0) vérifiant :

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

avec $a_i \in S^{-1}A$. Il existe $s \in S$ tel que $sa_i \in A$ pour tout i, et donc :

$$(sx)^n = s^n a_0 + s^{n-1}a_1(sx) + \cdots + sa_{n-1}(sx)^{n-1}$$

donc sx est entier sur A et $sx \in A$. Ainsi $x \in S^{-1}A$ comme voulu.
Supposons maintenant tous les $A_{\mathfrak{m}}$ intégralement clos et montrons que A l'est : soit $x \in K$ vérifiant :

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

avec $a_i \in A$. Cette égalité est aussi valable dans chaque $A_{\mathfrak{m}}$ donc x est entier sur $A_{\mathfrak{m}}$ et $x \in A_{\mathfrak{m}}$. Or l'intersection des $A_{\mathfrak{m}}$ est égale à A pour un anneau intègre (prendre l'idéal J formé par les $\lambda \in A$ tels que $\lambda x \in A$: si $J \neq A$, J est contenu dans un idéal maximal $\mathfrak{m}$ et donc $x \notin A_{\mathfrak{m}}$) donc $x \in A$. □

On peut caractériser les anneaux de valuation discrète comme des anneaux de Dedekind locaux :

Proposition 3.25. *Soit A un anneau intègre qui n'est pas un corps. Alors A est un anneau de valuation discrète si et seulement si c'est un anneau de Dedekind local.*

Démonstration. Supposons que A est un anneau de valuation discrète. A est alors principal donc de Dedekind et local, d'après le théorème 3.18. Si A est un anneau de Dedekind local, A est noéthérien car tout idéal non nul de A est inversible donc de type fini par le théorème 3.6. Notons $\mathfrak{m}$ l'unique idéal maximal de A. Par le théorème 3.18 il suffit de montrer que $\mathfrak{m}$ est principal. Par le lemme de Nakayama (ici $\mathfrak{m}$ est de type fini), il existe $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$. On a donc $(\pi) \subseteq \mathfrak{m}$ et ainsi $\pi\mathfrak{m}^{-1} \subseteq A$. Deux cas sont possibles : soit $\pi\mathfrak{m}^{-1} = A$ auquel cas, A étant de Dedekind, on a $(\pi) = \mathfrak{m}$ et $\mathfrak{m}$ est principal, soit $\pi\mathfrak{m}^{-1}$ est un idéal strict de A et est donc contenu dans l'unique idéal maximal $\mathfrak{m}$, c'est à dire que $\pi \in \mathfrak{m}^2$: c'est absurde. □

Lemme 3.26. *Si A est un anneau de Dedekind et $\mathfrak{p}$ est un idéal premier non nul de A, alors $A_{\mathfrak{p}}$ est un anneau de valuation discrète.*

Démonstration. Par la proposition 3.25, il suffit de montrer que $A_{\mathfrak{p}}$ est encore un anneau de Dedekind. Il est intègre, et si I est un idéal non nul de $A_{\mathfrak{p}}$, son tiré en arrière $I \cap A$ est non nul car son localisé est I et donc inversible, i.e. projectif sur A. Ainsi I est projectif sur $A_{\mathfrak{p}}$ en localisant, donc inversible par le théorème 3.6.
On peut aussi raisonner directement sans utiliser les modules projectifs. □

On donne deux autres caractérisations des anneaux de Dedekind.

Théorème 3.27. *Soit A un anneau intègre qui n'est pas un corps. Les énoncés suivants sont équivalents :*

(i) A est un anneau de Dedekind.

(ii) A est noéthérien, intégralement clos et de dimension de Krull au plus 1.

(iii) A est noéthérien et pour tout idéal maximal (ou de manière équivalente pour tout idéal premier non nul) $\mathfrak{m}$, $A_{\mathfrak{m}}$ est un anneau de valuation discrète.

Remarque 3.28. La caractérisation (ii) est souvent la plus agréable à vérifier. La caractérisation (iii) est *locale* et permet surtout le passage de (i) à (ii).

Démonstration. Si (i) est vrai, alors A est noéthérien car tout idéal non nul est inversible donc de type fini par le théorème 3.6 et pour tout idéal premier non nul $\mathfrak{p}$, le lemme 3.26 assure que $A_\mathfrak{p}$ est un anneau de valuation discrète. Ainsi (i) implique la version de (iii) avec les idéaux premiers non nuls qui elle même implique la version de (iii) avec les idéaux maximaux. La version de (iii) avec les idéaux maximaux entraîne à son tour (i) : dans ce cas tout idéal non nul de A est localement projectif et de type fini, or A est noéthérien donc tout idéal non nul de A est projectif par le théorème 1.53, donc inversible. Ainsi (i) et (iii) sont équivalents.
Si (ii) est vrai, alors pour tout $\mathfrak{p}$ premier, $A_\mathfrak{p}$ est intégralement clos par la proposition 3.24, noéthérien par la proposition 3.23, local, et de dimension de Krull au plus 1 car A est de dimension de Krull au plus 1 (et les idéaux premiers de $A_\mathfrak{p}$ correspondent bijectivement aux idéaux premiers de A contenus dans $\mathfrak{p}$). Par le théorème 3.18 , $A_\mathfrak{p}$ est donc un anneau de valuation discrète et (iii) est vrai.
Réciproquement, si (iii) est vrai, A est intégralement clos car il l'est localement (proposition 3.24), il reste à voir qu'il est de dimension de Krull au plus 1 : soit $\mathfrak{p}$ un idéal premier non nul de A. Il existe $\mathfrak{m}$ maximal contenant $\mathfrak{p}$ et $\mathfrak{p}_\mathfrak{m}$ est un idéal premier non nul de $A_\mathfrak{m}$ donc maximal, or $A_\mathfrak{m}$ est local donc $\mathfrak{p}_\mathfrak{m} = \mathfrak{m}_\mathfrak{m}$ et $\mathfrak{p} = \mathfrak{m}$ en tirant en arrière par le morphisme de localisation $A \longrightarrow A_\mathfrak{m}$. □

Lemme 3.29. *Soient $\mathfrak{p}, \mathfrak{p}'$ deux premiers distincts de A. Alors :*

$$\mathfrak{p}_{\mathfrak{p}'} = A_{\mathfrak{p}'}$$

Démonstration. On raisonne par contraposée. Si $\mathfrak{p}_{\mathfrak{p}'}$ est un idéal strict de l'anneau local $A_{\mathfrak{p}'}$, alors il est contenu dans l'unique idéal maximal $\mathfrak{p}'_{\mathfrak{p}'}$.
En prenant l'intersection avec A on obtient alors :

$$\mathfrak{p} \subseteq \mathfrak{p}_{\mathfrak{p}'} \cap A \subseteq \mathfrak{p}'_{\mathfrak{p}'} \cap A = \mathfrak{p}'$$

donc par maximalité $\mathfrak{p} = \mathfrak{p}'$. □

3.5 Factorisation d'un idéal

On va montrer que les idéaux non nuls d'un anneau de Dedekind se factorisent en produit d'ideaux premiers non nuls avec unicité de la factorisation.

Remarque 3.30. Par analogie avec l'arithmétique des anneaux principaux, si I et J sont deux idéaux (fractionnaires) d'un anneau A, on notera $I \mid J$ pour $I \supseteq J$. Si $x \in A$, on notera aussi $x \mid J$ pour $(x) \mid J$ et $I \mid x$ pour $I \mid (x)$. Ce choix est compatible avec la notation $x \mid y$ pour deux éléments de A puisque x divise y si et seulement si $(x) \supseteq (y)$.

Proposition 3.31. *Soit A un anneau de Dedekind. Tout idéal non nul de A est produit d'idéaux maximaux.*

Démonstration. On peut supposer que A n'est pas un corps. S'il existe un idéal non nul qui n'est pas produit d'idéaux maximaux, il en existe un maximal *parmi les idéaux qui ne sont pas produits d'idéaux maximaux* car A est noéthérien. Notons I un tel idéal.

Observons que $I \neq A$ car A est le produit vide. Ainsi I est contenu dans un idéal maximal $\mathfrak{m}$, or A est un anneau de Dedekind donc l'idéal $\mathfrak{m}$ est inversible (car A n'est pas un corps) et $\mathfrak{m}^{-1}I$ est un idéal de A qui contient I car $\mathfrak{m}^{-1}$ contient A. Or $\mathfrak{m}^{-1}I$ n'est pas produit d'idéaux maximaux (sinon I le serait) donc $\mathfrak{m}^{-1}I = I$ par maximalité de I parmi les idéaux qui ne sont pas produits d'idéaux maximaux. Ainsi en simplifiant par I dans le groupe des idéaux fractionnaires on obtient $\mathfrak{m}^{-1} = A$ donc $\mathfrak{m} = A$, ce qui est absurde. □

De manière temporaire, un anneau intègre dans lequel tout idéal non nul est produit d'idéaux *premiers* sera appelé un *anneau à factorisation d'idéaux*. On verra qu'en fait cette notion est équivalente à la notion d'anneau de Dedekind.

Définition 3.32. *Un anneau à factorisation d'idéaux est un anneau intègre dans lequel tout idéal non nul est produit d'idéaux premiers.*

On peut reformuler la proposition 3.31 de la façon suivante : un anneau de Dedekind est un anneau à factorisation d'idéaux.

Lemme 3.33. *(de Gauss) Soit A un anneau, $\mathfrak{p}$ un idéal premier et I, J deux idéaux. Si $\mathfrak{p} \mid IJ$, alors $\mathfrak{p} \mid I$ ou $\mathfrak{p} \mid J$.*

Démonstration. On raisonne par contraposée : si $\mathfrak{p} \nmid I$ et $\mathfrak{p} \nmid J$ alors il existe $x \in I \setminus \mathfrak{p}$ et $y \in J \setminus \mathfrak{p}$. On a donc $xy \in IJ \setminus \mathfrak{p}$ car $\mathfrak{p}$ est un idéal premier, et donc $\mathfrak{p} \nmid IJ$.

□

Proposition 3.34. *Soit A un anneau intègre. Un idéal I admet au plus une décomposition en facteurs premiers inversibles à l'ordre des facteurs près.*

Remarque 3.35. On parle bien de décomposition en facteurs premiers *inversibles*, on ne dit pas encore qu'il y a unicité d'une décomposition en facteurs premiers. Cependant, si le lecteur ne se soucie pas de l'équivalence entre anneau de Dedekind et anneau à factorisation d'idéaux (qui ne servira pas dans la suite), cela n'a pas d'importance puisque dans un anneau de Dedekind les idéaux premiers non nuls sont toujours inversibles.

Démonstration. Soit I un idéal non nul, et supposons que :

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}} = \prod_{\mathfrak{p}} \mathfrak{p}^{w_\mathfrak{p}}$$

où les deux produits portent sur les idéaux premiers *inversibles* de A (car I est non nul) et sont à support fini, au sens où $v_\mathfrak{p} = 0$ pour presque tout $\mathfrak{p}$ et $w_\mathfrak{p} = 0$ pour presque tout $\mathfrak{p}$. En simplifiant dans le groupe des idéaux fractionnaires inversibles, on peut supposer que pour tout $\mathfrak{p}$, ou bien $v_\mathfrak{p} = 0$ ou bien $w_\mathfrak{p} = 0$.
Il s'agit donc montrer que $v_\mathfrak{p} = w_\mathfrak{p} = 0$ pour tout $\mathfrak{p}$. Si ce n'est pas le cas, on peut supposer sans perte de généralité qu'il existe $\mathfrak{p}$ tel que $w_\mathfrak{p} > 0$, avec $\mathfrak{p}$ minimal pour l'inclusion parmi les $\mathfrak{q}$ qui vérifient $v_\mathfrak{q} \neq w_\mathfrak{q}$. Ainsi $\mathfrak{p} \mid \prod_\mathfrak{q} \mathfrak{q}^{v_\mathfrak{q}}$ donc par le lemme de Gauss 3.33 $\mathfrak{p}$ divise l'un des facteurs premiers et aucun n'est égal à $\mathfrak{p}$ puisque $v_\mathfrak{p} = 0$. Donc il existe $\mathfrak{q}$ premier différent de $\mathfrak{p}$ tel que $\mathfrak{p} \mid \mathfrak{q}$ et $v_\mathfrak{q} > 0$. Ceci contredit la minimalité pour l'inclusion dans le choix de $\mathfrak{p}$. □

Remarque 3.36. On a déjà établi le résultat important : dans un anneau de Dedekind, il existe une factorisation des idéaux non nuls en facteurs premiers avec unicité des facteurs (en vertu de la remarque 3.35. Cela permet de définir une *valuation* $\mathfrak{p}$*-adique* pour I un idéal non nul et $\mathfrak{p}$ un idéal premier non nul. On la notera souvent $v_\mathfrak{p}(I)$. Elle peut naturellement être étendue aux idéaux fractionnaires de A par la formule $v_\mathfrak{p}(x^{-1}I) = v_\mathfrak{p}(I) - v_\mathfrak{p}((x))$ dont on laisse au lecteur le soin de vérifier qu'elle n'est pas ambigüe. On a naturellement $v_\mathfrak{p}(IJ) = v_\mathfrak{p}(I)+v_\mathfrak{p}(J)$. Par convention, on pose aussi $v_\mathfrak{p}(0) = \infty$.

Dans ce qui suit, on s'assure qu'un anneau à factorisation d'idéaux est en fait un anneau de Dedekind. Ce n'est pas indispensable pour la suite.

Lemme 3.37. *Soit A un anneau à factorisation d'idéaux et $\mathfrak{p}$ un idéal premier inversible. Alors $\mathfrak{p}$ est un idéal maximal.*

Démonstration. Soit $a \in A \setminus \mathfrak{p}$. On veut montrer que $A = \mathfrak{p} + (a)$ (pour montrer que $\mathfrak{p}$ est maximal).
On décompose $\mathfrak{p}+(a)$ et $\mathfrak{p}+(a^2)$ en produit d'idéaux premiers non nuls : $\mathfrak{p}+(a) = \mathfrak{p}_1 \dots \mathfrak{p}_k$ et $\mathfrak{p} + (a^2) = \mathfrak{q}_1 \dots \mathfrak{q}_\ell$. On a donc $\mathfrak{p}_i \mid \mathfrak{p}$ et $\mathfrak{q}_j \mid \mathfrak{p}$ pour tous i, j. On va maintenant réduire cela dans l'anneau *intègre* $A/\mathfrak{p}$:

$$(\overline{a}) = (\mathfrak{p}_1/\mathfrak{p}) \dots (\mathfrak{p}_k/\mathfrak{p})$$

et $(\overline{a})$ est un idéal fractionnaire inversible de $A/\mathfrak{p}$ car $a \notin \mathfrak{p}$. Ainsi les $\mathfrak{p}_i/\mathfrak{p}$ sont inversibles et premiers (noter que $\mathfrak{p}_i$ contient $\mathfrak{p}$). De même les $\mathfrak{q}_j/\mathfrak{p}$ sont inversibles et premiers car $(\overline{a}^2)$ est inversible. On a donc :

$$(\overline{a}^2) = (\mathfrak{p}_1/\mathfrak{p})^2 \dots (\mathfrak{p}_k/\mathfrak{p})^2 = (\mathfrak{q}_1/\mathfrak{p}) \dots (\mathfrak{q}_\ell/\mathfrak{p})$$

qui sont deux écritures de l'idéal non nul $(\overline{a}^2)$ en produit d'idéaux premiers *inversibles*. Or il y a unicité d'une telle écriture donc $\ell = 2k$ et chaque $\mathfrak{p}_i$ apparaît exactement deux fois parmi les $\mathfrak{q}_j$ car il y a une correspondance bijective entre les idéaux premiers de $A/\mathfrak{p}$ et les idéaux premiers de A contenant $\mathfrak{p}$. Ainsi :

$$(\mathfrak{p} + (a))^2 = (\mathfrak{p}_1 \dots \mathfrak{p}_k)^2 = \mathfrak{q}_1 \dots \mathfrak{q}_\ell = \mathfrak{p} + (a^2)$$

Ainsi $\mathfrak{p} \subseteq (\mathfrak{p} + (a))^2 \subseteq \mathfrak{p}^2 + (a)$. Voyons enfin que :

$$\mathfrak{p} = \mathfrak{p}(\mathfrak{p} + (a))$$

L'inclusion de droite à gauche est claire. Dans l'autre sens, soit $x \in \mathfrak{p}$, on peut écrire $x = \lambda a + y$ avec $\lambda \in A, y \in \mathfrak{p}^2$. Ainsi $\lambda a \in \mathfrak{p}$, or $a \notin \mathfrak{p}$ et $\mathfrak{p}$ est premier donc $\lambda \in \mathfrak{p}$ et $x \in \mathfrak{p}(\mathfrak{p} + (a))$. Or on a supposé $\mathfrak{p}$ *inversible*, donc :

$$A = \mathfrak{p} + (a)$$

ce qui conclut pour la maximalité de $\mathfrak{p}$. □

Théorème 3.38. *Soit A un anneau. A est un anneau de Dedekind si et seulement si A est un anneau à factorisation d'idéaux.*

Démonstration. Il reste à prouver le sens indirect. Soit donc A un anneau à factorisation d'idéaux. Il suffit de montrer que tout idéal premier non nul est inversible car un produit d'inversibles est encore inversible. Soit donc $\mathfrak{p}$ un idéal premier non nul. Il existe $a \in \mathfrak{p} \setminus \{0\}$, et (a) se décompose en produit d'idéaux premiers non nuls :

$$(a) = \mathfrak{p}_1 \dots \mathfrak{p}_k$$

Or (a) est inversible donc les $\mathfrak{p}_i$ aussi. De plus $\mathfrak{p} \mid (a)$ donc par le lemme de Gauss 3.33, $\mathfrak{p}$ divise l'un des $\mathfrak{p}_i$. Mais $\mathfrak{p}_i$ étant inversible, il est maximal d'après le lemme 3.37. Donc $\mathfrak{p} = \mathfrak{p}_i$ et $\mathfrak{p}_i$ est inversible. □

3.6 Arithmétique des idéaux

On mentionne ici quelques résultats supplémentaires sur la factorisation des idéaux dans un anneau de Dedekind.

Proposition 3.39. *Soit A un anneau de Dedekind. Tout idéal fractionnaire non nul se factorise aussi en produit d'idéaux premiers non nuls (avec des puissances négatives éventuellement), et il y a unicité d'une telle décomposition. Avec les notations de valuation $\mathfrak{p}$-adiques, on a les propriétés suivantes pour I et J deux idéaux fractionnaires non nuls et $\mathfrak{p}$ un idéal premier non nul :*

- $v_\mathfrak{p}(IJ) = v_\mathfrak{p}(I) + v_\mathfrak{p}(J)$
- $v_\mathfrak{p}(I^{-1}) = -v_\mathfrak{p}(I)$
- $I \subseteq A \iff \forall \mathfrak{p}\ v_\mathfrak{p}(I) \geq 0$

Ensuite, si I et J sont deux idéaux non nuls de A, on a :

- $v_\mathfrak{p}(I + J) = \min(v_\mathfrak{p}(I), v_\mathfrak{p}(J))$
- $v_\mathfrak{p}(I \cap J) = \max(v_\mathfrak{p}(I), v_\mathfrak{p}(J))$
- $v_\mathfrak{p}(\sqrt{I}) = \begin{cases} 1 & si\ \mathfrak{p} \mid I \\ 0 & sinon \end{cases}$
- $I \mid J \iff \forall \mathfrak{p}\ v_\mathfrak{p}(I) \leq v_\mathfrak{p}(J)$

La démonstration ne pose pas de problème et est laissée au lecteur. Pour l'intersection et la somme, on pourra s'inspirer de l'énoncé analogue en arithmétique sur le pgcd et sur le ppcm, c'est à dire utiliser les propriétés universelles de $I + J$ et de $I \cap J$. On peut d'ailleurs généraliser ces formules pour des sommes et intersections infinies.

Notation 3.40. *On définit aussi la valuation $\mathfrak{p}$-adique d'un élément $x \in K \setminus \{0\}$ comme la valuation $\mathfrak{p}$-adique de l'idéal fractionnaire qu'il engendre :*

$$v_\mathfrak{p}(x) = v_\mathfrak{p}(xA)$$

Remarque 3.41. Une manière de reformuler le principe de factorisation des idéaux fractionnaires dans un anneau de Dedekind est de dire que l'on a un isomorphisme canonique :

$$\mathcal{F}(A)^\times \cong \bigoplus_\mathfrak{p} \mathbb{Z}\mathfrak{p}$$

autrement dit $\mathcal{F}(A)^\times$ est un groupe abélien libre dont une base est donnée par les premiers de A.
En général, le groupe des idéaux fractionnaires principaux n'est pas égal à $\mathcal{F}(A)^\times$, ce qui se traduit par le fait que, étant donné une famille d'entiers presque nulle $(v_\mathfrak{p}) \in \bigoplus_\mathfrak{p} \mathbb{Z}\mathfrak{p}$, il n'existe pas en général d'élément de A ayant exactement ces valuations $\mathfrak{p}$-adiques là (contrairement aux anneaux factoriels). La proposition suivante affirme cependant que l'on peut toujours trouver un élément dont on spécifie un nombre fini de valuations $\mathfrak{p}$-adiques.
C'est un premier résultat qui indique que le groupe des idéaux principaux est "suffisament grand", ou de façon équivalente que le groupe des classes $\mathrm{Cl}(A)$ est "suffisament petit".

Théorème 3.42. *(Spécification Finie) Soit P un ensemble fini de premiers de A et $v : P \longrightarrow \mathbb{Z}$ une application. Alors il existe $x \in K \setminus \{0\}$ tel que pour tout $\mathfrak{p} \in P$ on ait :*

$$v_\mathfrak{p}(x) = v(\mathfrak{p})$$

et pour tout $\mathfrak{p} \notin P$ on ait :

$$v_\mathfrak{p}(x) \geq 0.$$

En particulier, pour tout idéal fractionnaire non nul I, et toute application $v : P \longrightarrow \mathbb{Z}$ comme précedemment, il existe J un idéal fractionnaire de A équivalent à I dans le groupe des classes tel que :

$$v_\mathfrak{p}(J) = v(\mathfrak{p})$$

pour tout $\mathfrak{p} \in P$ et $v_\mathfrak{p}(J) \geq v_\mathfrak{p}(I)$ pour $\mathfrak{p} \notin P$.

Démonstration. On traite d'abord le cas où v est à valeurs *positives*, et on cherche alors un élément dans $A \setminus \{0\}$. Pour tout $\mathfrak{p} \in P$, on a une inclusion :

$$\mathfrak{p}^{v(\mathfrak{p})+1} \subsetneq \mathfrak{p}^{v(\mathfrak{p})}$$

qui est stricte par unicité de la décomposition en facteurs premiers. Il existe donc un élément $x_\mathfrak{p} \in A$ tel que :

$$v_\mathfrak{p}(x) = v(\mathfrak{p})$$

ce qui prouve la proposition dans le cas où P n'aurait qu'un seul élément. On utilise à présent le théorème chinois pour contrôler toutes les valuations $\mathfrak{p}$-adiques avec $\mathfrak{p} \in P$: puisque les $\mathfrak{p}^{v(\mathfrak{p})+1}$ sont deux à deux premiers entre eux et en nombre fini, il existe $x \in A$ tel que pour tout $\mathfrak{p} \in P$:

$$x \equiv x_\mathfrak{p} \ [\mathfrak{p}^{v(\mathfrak{p})+1}]$$

Et x convient alors.
Ensuite, pour le cas général, on peut toujours écrire $v = v_1 - v_2$ avec v_1, v_2 à valeurs positives. Par ce qui précède, il existe x_1, x_2 de valuations spécifiées par v_1 et v_2, et $y = x_1/x_2$ est alors un élément de $K^\times$ pour lequel :

$$v_\mathfrak{p}(y) = v(\mathfrak{p})$$

pour tout $\mathfrak{p} \in P$. Pour avoir la deuxième condition, on considère l'ensemble fini $P' = \{\mathfrak{p} \mid v_\mathfrak{p}(y) < 0\} \cup P$. Par ce qui précède, il existe $z \in A \setminus \{0\}$ tel que pour tout $\mathfrak{p} \in P$, on ait $v_\mathfrak{p}(z) = 0$ et pour tout $\mathfrak{p} \in P' \setminus P$ on ait :

$$v_\mathfrak{p}(z) = -v_\mathfrak{p}(y) > 0$$

et on pose $x = yz$ qui convient alors.
La conséquence sur les idéaux s'en déduit directement en considérant $J = xI$. □

Ce résultat est fondamental et a plusieurs corollaires intéressants sur la structure des idéaux d'un anneau de Dedekind, qui montrent qu'un tel anneau est assez proche d'être principal.

Corollaire 3.43. *Tout idéal fractionnaire de A est engendré par deux éléments. De façon plus précise, pour tout idéal fractionnaire I de A et tout élément non nul $a \in I$, il existe $b \in I$ tel que $I = aA + bA$.*
Ainsi un anneau de Dedekind est vraiment proche d'être principal en un sens.

Démonstration. Soit I un idéal non nul de A (on se ramène facilement à ce cas) et soit $a \in I$ non nul. On a $I \mid a$ et l'ensemble :

$$P = \{\mathfrak{p} \text{ premier} \mid \mathfrak{p} \mid a\}$$

est *fini*. Par le théorème de spécification finie 3.42, il existe donc $b \in A \setminus \{0\}$ tel que pour tout $\mathfrak{p} \in P$:

$$v_\mathfrak{p}(b) = v_\mathfrak{p}(I) \geq 0$$

et on a alors :

$$I = aA + bA$$

car pour tout $\mathfrak{p}$:

$$v_\mathfrak{p}(I) = \min(v_\mathfrak{p}(a), v_\mathfrak{p}(b))$$

comme voulu. □

Corollaire 3.44. *Un anneau de Dedekind est principal si et seulement si il est factoriel.*
De plus, un anneau de Dedekind semi-local (i.e. avec un nombre fini de premiers) est principal.

Démonstration. La deuxième affirmation est claire par le théorème de spécification finie 3.42 : il n'y a qu'un nombre fini de valuations à spécifier.
Soit maintenant A un anneau de Dedekind factoriel. Alors pour tout élément irréductible x de A, le quotient A/xA est intègre donc xA est un idéal premier non nul de A donc maximal.
Soit $\mathfrak{p}$ un premier de A. Prenons $a \in \mathfrak{p} \setminus \{0\}$. Puisque a se factorise en produit d'irréductibles et que $\mathfrak{p}$ est un idéal premier, $\mathfrak{p}$ contient un élément irréductible x. Or xA est un idéal maximal contenu dans $\mathfrak{p}$ donc $\mathfrak{p} = xA$. Tous les premiers de A sont donc principaux et par principe de factorisation tous les idéaux de A sont principaux. □

On verra plus tard que les anneaux de Dedekind qui apparaissent en théorie des nombres ont un groupe de classe fini (6.22). Ces anneaux sont alors localement principaux au sens suivant.

Proposition 3.45. *Soit A un anneau de Dedekind qui a un groupe des classes de type fini. Alors pour tout premier $\mathfrak{p}$ il existe $f \notin \mathfrak{p}$ tel que $A[1/f]$ est principal.*

Remarque 3.46. En termes géométriques, cela signifie que l'on peut recouvrir $\operatorname{Spec} A$ par des ouverts standards $D(f_i)$ qui sont des spectres d'anneaux principaux.

Démonstration. Puisque le groupe des classes de A est de type fini, il existe $I_1, \dots, I_k$ des idéaux non nuls contenus dans A dont les classes génèrent $\mathrm{Cl}(A)$.
On peut supposer que chaque I_j est premier avec $\mathfrak{p}$: en effet, par le théorème de spécification finie 3.42, on trouve un idéal fractionnaire J_j équivalent à I_j dans le groupe des classes tel que $v_\mathfrak{p}(J_j) = 0$.
Ensuite, en considérant les premiers $\mathfrak{q}$ tels que $v_\mathfrak{q}(I_j) \neq 0$ pour un certain j, on trouve $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ des premiers distincts de A différents de $\mathfrak{p}$ et dont les classes engendrent le groupe des classes de A :

$$\mathrm{Cl}(A) = \langle [\mathfrak{q}_1], \dots, [\mathfrak{q}_r] \rangle.$$

Il existe alors f tel que :

$$f \in \bigcap_i \mathfrak{q}_i \setminus \mathfrak{p} = \prod_i \mathfrak{q}_i \setminus \mathfrak{p}$$

car $\mathfrak{p}$ ne divise pas le produit des $\mathfrak{q}_i$.
Il reste à voir que $A[1/f]$ est principal. Soit donc $I[1/f]$ un idéal non nul de $A[1/f]$, avec I un idéal non nul de A. Dans le groupe de classes de A, on peut écrire :

$$[I] = \prod_i [\mathfrak{q}_i^{n_i}]$$

avec $n_i \in \mathbb{Z}$ et donc il existe $g \in A$ tel que :

$$I = g \prod_i \mathfrak{q}_i^{n_i}$$

et donc il suffit de montrer que $\mathfrak{q}_i[1/f]$ est principal. Or $f \in \mathfrak{q}_i$ donc $\mathfrak{q}_i[1/f] = A[1/f]$ car f est inversible dans $A[1/f]$. □

Proposition 3.47. *Soit A un anneau de Dedekind de corps des fractions K et $\mathfrak{p}$ un premier de A. Alors on a :*

$$A_\mathfrak{p} = \{x \in K \mid v_\mathfrak{p}(x) \geq 0\}.$$

En particulier on a :

$$A = \bigcap_\mathfrak{p} A_\mathfrak{p}.$$

Démonstration. L'inclusion de gauche à droite est claire car un élément de $A_\mathfrak{p}$ s'écrit a/b avec $b \notin \mathfrak{p}$ donc $v_\mathfrak{p}(b) = 0$.
Soit maintenant $x \in K^\times$ tel que $v_\mathfrak{p}(x) \geq 0$. L'idéal xA s'écrit alors :

$$xA = I \cdot J^{-1}$$

avec I et J des idéaux fractionnaires non nuls contenus dans A et $\mathfrak{p} \nmid J$ (il suffit de décomposer xA en facteurs premiers et de mettre dans I les facteurs apparaissant avec

une puissance positive et dans J^{-1} ceux apparaissant avec une puissance négative). On a donc $xJ = I$, or $J \not\subseteq \mathfrak{p}$ donc il existe $j \in J \setminus \mathfrak{p}$, et ainsi $i = xj \in I$ et :

$$x = \frac{i}{j} \in A_{\mathfrak{p}}.$$

□

3.7 Modules de type fini sur un anneau de Dedekind

On fixe A un anneau de Dedekind de corps des fractions K. On cherche à classifier les modules de type fini sur A. On commence par le résultat suivant.

Théorème 3.48. *Un A-module de type fini est projectif si et seulement si il est sans torsion.*

Démonstration. Soit M un A-module de type fini. Si M est sans torsion, alors pour tout idéal premier $\mathfrak{p}$, $M_{\mathfrak{p}}$ n'a pas de torsion et est de type fini comme $A_{\mathfrak{p}}$-module, or $A_{\mathfrak{p}}$ est principal donc $M_{\mathfrak{p}}$ est libre. Par 1.53, M est donc projectif.
Si M est projectif, il est facteur direct d'un module libre donc est sans torsion. □

La stratégie de la classification est alors la suivante. Soit M un A-module de type fini. On a naturellement une suite exacte :

$$0 \longrightarrow M_{\text{tors}} \longrightarrow M \longrightarrow P \longrightarrow 0$$

avec M_{tors} le module de torsion de M, c'est à dire l'ensemble des $x \in M$ pour lesquels il existe $a \in A \setminus \{0\}$ tel que $ax = 0$, et P sans torsion de type fini. Par le théorème 3.48, P est projectif et donc cette suite est scindée.
Ainsi M est somme directe d'un module projectif de type fini et d'un module de torsion de type fini (dont le produit tensoriel avec K est nul). Il suffit donc de classifier ces deux types de modules.
Notons de plus que les foncteurs $M \mapsto M_{\text{tors}}$ et $M \mapsto M/M_{\text{tors}}$ préservent les sommes directes finies, et donc si $M = N \oplus P$ avec N de torsion et P sans torsion, on a $M_{\text{tors}} = N$ et $M/M_{\text{tors}} = P$.

3.7.1 Classification des modules projectifs de type fini sur un anneau de Dedekind

A est toujours un anneau de Dedekind de corps des fractions K.
On a besoin d'un premier lemme d'arithmétique sur les anneaux de Dedekind.

Lemme 3.49. *Soit I un idéal non nul de A et soit $\omega \in \mathrm{Cl}(A)$. Il existe un représentant $J \subseteq A$ de ω tel que :*

$$I + J = A.$$

Démonstration. C'est une application directe du théorème de spécification finie 3.42 : choisissons d'abord $J_0 \subseteq A$ un représentant quelconque de ω.

On trouve alors J un représentant de la même classe ω tel que pour tout $\mathfrak{p} \mid I$, on ait $v_\mathfrak{p}(J) = 0$ et pour tout autre $\mathfrak{p}$, $v_\mathfrak{p}(J) \geq v_\mathfrak{p}(J_0)$. Ainsi $J \subseteq A$ et on a par construction :

$$I + J = A.$$

par un calcul de pgcd. □

On mentionne ensuite un résultat surprenant dû à Steinitz.

Lemme 3.50. *(Steinitz) Soient I, J deux idéaux fractionnaires non nuls de A. On a un isomorphisme (non canonique) :*

$$I \oplus J \cong IJ \oplus A.$$

Démonstration. On peut supposer I et J contenus dans A car pour tout $x \in K^\times$, les idéaux fractionnaires I et xI sont isomorphes comme A-modules. Par le lemme 3.49, on peut aussi supposer $I + J = A$ sans changer la classe d'isomorphisme de J. On a alors une suite exacte :

$$0 \longrightarrow I \cap J = IJ \longrightarrow I \oplus J \longrightarrow I + J = A \longrightarrow 0$$

qui par projectivité de $I + J$ se scinde pour donner un isomorphisme :

$$I \oplus J \cong IJ \oplus A.$$

□

Théorème 3.51. *(Classification des modules projectifs de type fini) Soit M un A-module projectif de type fini.*
M est alors somme directe d'un nombre fini n d'idéaux non nuls de A, avec n le rang de M, c'est à dire la dimension du K-espace vectoriel $M \otimes_A K$.
De plus, si $n \geq 1$, il existe I un idéal non nul de A dont la classe est uniquement déterminée dans le groupe des classes $\mathrm{Cl}(A)$ tel que :

$$M \cong I \oplus A^{n-1}$$

et deux modules $I \oplus A^{n-1}$ et $J \oplus A^{m-1}$ sont isomorphes si et seulement si $m = n$ et I et J ont la même classe.
En particulier, si A est principal, on retrouve la classification des modules projectifs de type fini sur un anneau principal : ce sont les modules libres.
On en déduit ainsi que pour tout $n \geq 1$, les classes d'isomorphisme de A-modules projectifs de rang n sont en bijection avec le groupe des classes $\mathrm{Cl}(A)$ via l'application :

$$I_1 \oplus \cdots \oplus I_n \mapsto \left[\prod_i I_i\right].$$

Démonstration. Puisque M est projectif de type fini, il est facteur direct d'un certain A^n. On va montrer par récurrence sur n que tout sous-module de type fini d'un A-module libre de rang n est une somme directe d'idéaux de A. C'est clair au rang 0. Supposons que c'est vrai au rang n, et prenons F un A-module libre de rang $n+1$, que

l'on écrit $F = G \oplus A$ avec G libre de rang n. Soit M un sous-module de type fini de F. On a une suite exacte :

$$0 \longrightarrow I \longrightarrow M \longrightarrow \pi_G(M) \longrightarrow 0$$

induite par $0 \longrightarrow A \longrightarrow G \oplus A \longrightarrow G \longrightarrow 0$ avec I un idéal de A.
Mais $\pi_G(M)$ est sans torsion et de type fini (A est noéthérien) donc projectif et ainsi la suite est scindée. Or par hypothèse de récurrence $\pi_G(M) \subseteq G$ est une somme directe d'idéaux de A et donc M aussi.
Soient maintenant $I_1, \dots, I_n$ des idéaux non nuls de A. Le module $M = \bigoplus_i I_i$ est bien sûr projectif de type fini et on a :

$$M \otimes_A K \cong \bigoplus_i I_i \otimes_A K \cong K^n$$

car si I est un idéal non nul de A, on a $IK = K$ puisque I est non nul donc $I \otimes_A K \longrightarrow K$ est surjective et elle est injective car K est plat sur A et $I \hookrightarrow A$ est injective.
Ainsi n correspond bien au rang de M. Ensuite, en appliquant plusieurs fois le lemme de Steinitz 3.50 :

$$M \cong \prod_i I_i \oplus A^{n-1}$$

comme voulu. Il reste à montrer que si $I \oplus A^{n-1}$ et $J \oplus A^{m-1}$ sont isomorphes, alors $m = n$ (cela s'obtient en tensorisant par K) et I et J ont la même classe. En ajoutant I^{-1} de chaque côté et avec le lemme de Steinitz, on se ramène à montrer que si $A^{n-1} \oplus I$ est isomorphe à A^n, alors I est principal.
Si $A^{n-1} \oplus I \cong A^n$, alors les n-èmes puissances extérieures sont des A-modules isomorphes :

$$\Lambda_A^n \left(A^{n-1} \oplus I \right) \cong \Lambda_A^n A^n \cong A$$

On applique maintenant 1.70 :

$$\Lambda_A^n \left(A^{n-1} \oplus I \right) = \bigoplus_{p+q=n} \Lambda_A^p \left(A^{n-1} \right) \otimes \Lambda_A^q I.$$

Or I est engendré par deux éléments d'après 3.43, disons $I = Ax + Ay$, et donc pour $q > 2$, on a d'après 1.68 :

$$\Lambda_A^q I = 0$$

car ce A-module est engendré par les produits extérieurs de q éléments x ou y. On a donc :

$$A \cong \Lambda_A^n A^{n-1} \oplus \left(\Lambda_A^{n-1} A^{n-1} \otimes I \right) \oplus \left(\Lambda_A^{n-2} A^{n-1} \otimes \Lambda_A^2 I \right) \cong I \oplus \left(\Lambda_A^2 I \right)^{n-1}$$

En quotientant par le sous-groupe de torsion (ce qui préserve les sommes directes finies), on obtient :

$$A \cong I \oplus 0 \cong I$$

car $\Lambda_A^2 I$ est de torsion puisque la puissance extérieure commute à l'extension de scalaires (voir 1.67) :

$$\Lambda_A^2 I \otimes_A K = \Lambda_K^2 (I \otimes_A K) = \Lambda_K^2 K = 0.$$

□

On en déduit directement le corollaire suivant.

Corollaire 3.52. *Si le groupe des classes de A est trivial, tout module projectif de type fini sur A est libre. La réciproque est vraie.*

Pour finir cette partie sur les modules projectifs de type fini, on mentionne le résultat suivant qui donne une condition nécessaire et suffisante pour l'existence de supplémentaires pour des sous-modules d'un module projectif de type fini.

Proposition 3.53. *(Condition pour l'existence d'un supplémentaire) Soit M un A-module projectif de type fini et N un sous-module de M. Les propositions suivantes sont équivalentes :*

(i) Il existe P un sous-module de M tel que $M = N \oplus P$.

(ii) On a $KN \cap M = N$ dans l'espace vectoriel $M \otimes_A K$.

(iii) Le quotient M/N est projectif.

Démonstration. D'abord, on a clairement $(i) \implies (iii)$ car un facteur direct d'un projectif est projectif, et $(iii) \implies (i)$ car une suite exacte dont le dernier terme est projectif est scindée.
Ensuite, on a les équivalences suivantes :

$$\begin{aligned} M/N \text{ projectif} &\iff M/N \text{ sans torsion} \\ &\iff \forall x \in M\ \forall \lambda \in A \setminus \{0\}\ \lambda x \in N \implies x \in N \\ &\iff \bigcup_{\lambda \in A\setminus\{0\}} N/\lambda \cap M \subseteq N \\ &\iff KN \cap M = N \end{aligned}$$

□

3.7.2 Classification des modules de torsion de type fini sur un anneau de Dedekind

A est toujours un anneau de Dedekind de corps des fractions K. On rappelle qu'un A-module M est de torsion si l'un des énoncés suivants (équivalents) est vérifié :

— On a $M \otimes_A K = 0$.

— Pour tout $x \in M$, il existe $\lambda \in A \setminus \{0\}$ tel que $\lambda x = 0$.

— On a $M_{\text{tors}} = M$.

On a un théorème de classification pour ces modules analogue au cas des modules de torsion de type fini sur un anneau principal. Pour cela, on a besoin du lemme suivant, qui est une conséquence du théorème de spécification finie 3.42.

Lemme 3.54. *Soient $\mathfrak{p} \neq \mathfrak{q}$ deux premiers distincts de A. On a alors un isomorphisme canonique de A-modules :*

$$A_{\mathfrak{p}} \otimes_A A_{\mathfrak{q}} \cong K.$$

Démonstration. Puisque $\mathfrak{p}$ et $\mathfrak{q}$ sont distincts et par le théorème de 3.42, il existe $\pi \in A \setminus \{0\}$ tel que :

$$v_{\mathfrak{p}}(\pi) = 1$$

et :

$$v_{\mathfrak{q}}(\pi) = 0$$

de sorte que π est une uniformisante de l'anneau de valuation discrète $A_{\mathfrak{p}}$ et π est inversible dans $A_{\mathfrak{q}}$. Par conséquent π est inversible dans $A_{\mathfrak{p}} \otimes_A A_{\mathfrak{q}}$ et par conséquent tout élément non nul de $A_{\mathfrak{p}}$ est inversible dans $A_{\mathfrak{p}} \otimes_A A\mathfrak{q}$ puisqu'un tel élément s'écrit $u\pi^n$ avec u inversible dans $A_{\mathfrak{p}}$. □

Théorème 3.55. *(Classification des modules de torsion de type fini) Soit M un A-module de torsion de type fini. Il existe une unique suite finie d'idéaux non nuls de A différents de A qui se divisent dans cet ordre :*

$$I_1 \mid I_2 \mid \cdots \mid I_n$$

telle qu'on ait un isomorphisme :

$$M \cong \bigoplus_i A/I_i.$$

On peut donner une autre décomposition qui utilise les premiers de A : il existe une unique famille à support fini $(v_{\mathfrak{p},k})$ indexée par les premiers de A et les entiers $k \geq 1$ telle qu'on ait un isomorphisme :

$$M \cong \bigoplus_{\mathfrak{p},k\geq 1} \left(A/\mathfrak{p}^k\right)^{v_{\mathfrak{p},k}}.$$

Démonstration. On commence par montrer le second point. Pour tout premier $\mathfrak{p}$, l'anneau $A_{\mathfrak{p}}$ est un anneau principal dont le seul idéal premier est $\mathfrak{p}_{\mathfrak{p}}$. Puisque $M_{\mathfrak{p}}$ est de torsion et de type fini sur $A_{\mathfrak{p}}$, le théorème de classification des modules de type fini de torsion sur un anneau principal donne un isomorphisme :

$$M_{\mathfrak{p}} \cong \bigoplus_{k\geq 1} (A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}^k)^{v_{\mathfrak{p},k}}$$

et les $v_{\mathfrak{p},k}$ sont uniquement déterminés. Ensuite, pour tout $x \in M$, puisque M est de torsion, il existe $\lambda \in A \setminus \{0\}$ tel que $\lambda x = 0$. En particulier, pour tout premier $\mathfrak{p}$ qui ne divise pas λ, l'image de x dans $M_{\mathfrak{p}}$ est nulle. Donc pour tous les premiers sauf un nombre fini, x est envoyé sur 0 dans $M_{\mathfrak{p}}$. Or M est de type fini donc en appliquant cette remarque à un nombre fini de générateurs, on obtient que :

$$M_{\mathfrak{p}} = 0$$

sauf pour un nombre fini de premiers $\mathfrak{p}$. En particulier on a un morphisme bien défini :

$$M \longrightarrow \bigoplus_{\mathfrak{p}} M_{\mathfrak{p}}$$

qui est un isomorphisme car pour tout premier $\mathfrak{p}$ la localisation de ce morphisme est l'identité de $M_{\mathfrak{p}}$, puisque si $\mathfrak{q} \neq \mathfrak{p}$, on a d'après le lemme 3.54 :

$$(M_{\mathfrak{p}})_{\mathfrak{q}} = M \otimes_A A_{\mathfrak{p}} \otimes_A A_{\mathfrak{q}} = M \otimes_A K = 0$$

et on a donc un isomorphisme :

$$M \cong \bigoplus_{\mathfrak{p},k\geq 1} \left(A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}^k\right)^{v_{\mathfrak{p},k}}$$

et il reste à constater que $A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}^k = (A/\mathfrak{p}^k)_\mathfrak{p} = A/\mathfrak{p}^k$ car pour tout $s \in A\setminus\mathfrak{p}$, on a $sA+\mathfrak{p}^k = A$ et donc s est inversible modulo $\mathfrak{p}^k$. Ceci achève la preuve du second point. Le premier s'en déduit grâce au théorème chinois, c'est la même preuve que dans le cas d'un anneau principal. □

3.7.3 Classification des modules de type fini sur un anneau de Dedekind

En réunissant les deux théorèmes 3.51 et 3.55, on obtient le théorème de classification suivant.

Théorème 3.56. *(Classification des modules de type fini sur un anneau de Dedekind) Soit A un anneau de Dedekind de corps des fractions K et M un A-module de type fini. Si M est de torsion, le théorème 3.55 donne la structure de M. Si M n'est pas de torsion :*

$$A^{n-1} \oplus I \oplus A/I_1 \oplus \cdots \oplus A/I_n$$

avec $n = \dim_K M \otimes_A K$, $I, I_1, \ldots, I_n$ des idéaux de A non nuls, avec $I_1 \mid \cdots \mid I_n$ uniquement déterminés, et $[I]$ uniquement déterminée dans le groupe des classes de A.

3.7.4 Application à la simplification des quotients

Soit A un anneau de Dedekind de corps de fractions K, et I un idéal non nul de A. Sous certaines hypothèses, on cherche à montrer que les A-modules IM/IN et M/N sont isomorphes (non canoniquement) avec $N \subseteq M$ des A-modules.
Le cas des anneaux principaux, ou plus généralement le cas où I est principal, est très simple.
On commence par deux cas particuliers importants.

Lemme 3.57. *Soit $I = (\lambda)$ un idéal principal non nul de A, et $N \subseteq M$ deux A-modules sans torsion. On a alors un isomorphisme :*

$$M/N \cong IM/IN$$

donné par la multiplication par λ.

Démonstration. Il suffit de contempler ce diagramme, où la multiplication par λ est injective car M est sans torsion :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \bullet\times\lambda} & & \downarrow & & \\ 0 & \longrightarrow & \lambda N & \longrightarrow & \lambda M & \longrightarrow & \lambda M/\lambda N & \longrightarrow & 0 \end{array}$$

□

Proposition 3.58. *Soit A un anneau de Dedekind et $\mathfrak{p}$ un premier de A. On note $\kappa = A/\mathfrak{p}$. Soit $k \geq 0$. Le choix d'un élément $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ donne un isomorphisme de k-espaces vectoriels :*

$$\kappa \cong \mathfrak{p}^k/\mathfrak{p}^{k+1}$$

induit par $x \mapsto \pi^k x$.

Démonstration. Notons qu'un tel élément π existe car $\mathfrak{p}^2 \neq \mathfrak{p}$ (sinon on pourrait simplifier par $\mathfrak{p}$). On a :

$$\mathfrak{p}^{k+1} \subsetneq \mathfrak{p}^{k+1} + \pi^k A \subseteq \mathfrak{p}^k$$

car $v_\mathfrak{p}(\pi^k) = k v_\mathfrak{p}(\pi) = k$. Par unicité de la décomposition en facteurs premiers, on a donc :

$$\mathfrak{p}^{k+1} + \pi^k A = \mathfrak{p}^k$$

et ainsi la flèche induite sur les quotients :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{p} & \longrightarrow & A & \longrightarrow & \kappa & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \times\pi^k} & & \downarrow & & \\ 0 & \longrightarrow & \mathfrak{p}^{k+1} & \longrightarrow & \mathfrak{p}^k & \longrightarrow & \mathfrak{p}^k/\mathfrak{p}^{k+1} & \longrightarrow & 0 \end{array}$$

est surjective et en regardant les valuations $\mathfrak{p}$-adiques on obtient qu'elle est injective. □

Corollaire 3.59. *Soit A un anneau de Dedekind et $\mathfrak{p}$ un premier de A. On note $\kappa = A/\mathfrak{p}$ le corps résiduel, que l'on suppose fini de cardinal q. Alors les $\mathfrak{p}^k/\mathfrak{p}^\ell$ avec $k \leq \ell$ sont finis et de cardinal $q^{\ell-k}$.*

Démonstration. On a des suites exactes :

$$0 \longrightarrow \mathfrak{p}^\ell/\mathfrak{p}^{\ell+1} \longrightarrow \mathfrak{p}^k/\mathfrak{p}^{\ell+1} \longrightarrow \mathfrak{p}^k/\mathfrak{p}^\ell \longrightarrow 0$$

où le premier terme est isomorphe à κ par ce qui précède, et donc on a $\left|\mathfrak{p}^k/\mathfrak{p}^{\ell+1}\right| = q \times \left|\mathfrak{p}^k/\mathfrak{p}^\ell\right|$ et on conclut par récurrence sur $\ell - k$. □

Le théorème suivant généralise 3.58 et 3.57. Cependant on n'obtient pas un isomorphisme explicite.

Théorème 3.60. *Soit I un idéal non nul de A, et $N \subseteq M$ deux A-modules. On suppose M (et donc N) sans torsion et de type fini et on suppose que l'inclusion $N \otimes_A K \longrightarrow M \otimes_A K$ est surjective. Alors on a un isomorphisme (non canonique) :*

$$IM/IN \cong M/N$$

Démonstration. D'abord, remarquons que :

$$\left(\frac{IM}{IN}\right) \otimes_A K \cong \frac{IM \otimes_A K}{IN \otimes_A K} \cong \frac{M \otimes_A K}{N \otimes_A K} = 0$$

car M et N sont sans torsion, car $I \neq 0$ et par hypothèse sur M et N. Ainsi IM/IN est un A-module de type fini et de torsion.
Par la preuve du théorème 3.55, on a donc un isomorphisme canonique :

$$IM/IN \cong \bigoplus_{\mathfrak{p}} \left(\frac{IM}{IN}\right)_{\mathfrak{p}} \cong \bigoplus_{\mathfrak{p}} \frac{I_{\mathfrak{p}}M_{\mathfrak{p}}}{I_{\mathfrak{p}}N_{\mathfrak{p}}}$$

et $I_{\mathfrak{p}}$ est un idéal principal non nul de l'anneau de valuation discrète $A_{\mathfrak{p}}$, donc par le lemme précédent 3.57 on a :

$$IM/IN \cong \bigoplus_{\mathfrak{p}} \frac{M_{\mathfrak{p}}}{N_{\mathfrak{p}}} \cong \bigoplus_{\mathfrak{p}} \left(\frac{M}{N}\right)_{\mathfrak{p}}$$

qui est isomorphe à M/N par hypothèse sur M et N et par la preuve du théorème 3.55. □

Chapitre 4

Algèbre et géométrie des réseaux

> La géométrie est l'archétype de la beauté du monde.
>
> Johannes Kepler

Il existe plusieurs notions de réseaux en mathématiques : réseaux d'un espace vectoriel réel ou d'un groupe localement compact, ou réseaux algébriques abstraits.
Dans tous les cas, la philosophie est la même : étant donné un objet V qui soit "lisse", ou "continu" (ce qui se traduit par des propriétés topologiques ou algébriques selon le contexte), un réseau de V est un sous-objet Λ qui est "discret" en un sens qui peut encore une fois varier selon le contexte, et qui occupe suffisament d'espace dans l'objet V ambiant.
Avec ce sens informel on peut déjà citer plusieurs exemples : $\mathbb{Z}^n$ est un réseau de $\mathbb{R}^n$, $\mathbb{U}_n$ est un réseau du groupe des nombres complexes de module 1, et $\mathbb{Z}[i]$ est un réseau de $\mathbb{Q}(i)$.
Dans ce chapitre, on va détailler deux notions de réseaux qui se rejoignent assez naturellement : la notion algébrique de quasi-réseaux et la notion géométrique de réseaux d'un espace vectoriel réel de dimension finie.

4.1 Étude algébrique

4.1.1 Quasi-réseaux sur un anneau noéthérien intègre

On fixe A un anneau noéthérien intègre, K un corps qui contient A et V un K-espace vectoriel de dimension n.

Définition 4.1. *Un quasi-réseau $\Lambda \subseteq V$ de V est un sous-A-module de V de type fini tel que le morphisme canonique :*

$$\Lambda \otimes_A K \longrightarrow V$$

est un isomorphisme. Si de plus Λ est libre comme A-module, on dit que Λ est un réseau. Pour insister sur l'anneau A, on pourra aussi dire A-quasi-réseau et A-réseau.
On note $V^* = \mathrm{Hom}_K(V, K)$ l'espace dual de V. On identifie canoniquement V^{**} et V. Enfin,

si M est un sous-A-module de V, on définit le polaire de M comme le sous-A-module suivant de V^* :

$$M^\circ = \{\alpha \in V^* \mid \alpha(M) \subseteq A\} \subseteq V^*$$

et on a naturellement $M \subseteq M^{\circ\circ}$ bien que ce ne soit pas une égalité en général.

Remarque 4.2. Le corps K est plat sur A car les morphismes $A \longrightarrow \operatorname{Frac} A$ et FracA $\longrightarrow K$ sont plats.

Proposition 4.3. *Si Λ est un réseau de V, il est libre de rang $n = \dim_K V$.*

Démonstration. On écrit $\Lambda \cong A^k$ car Λ est libre de rang fini, et en tensorisant par K on obtient :

$$V \cong K^k$$

donc $k = n$. □

Proposition 4.4. *Soit Λ un quasi-réseau de V. Le polaire Λ° est alors un quasi-réseau de V^* et on a un isomorphisme canonique :*

$$\Lambda^\circ \cong \Lambda^\vee$$

où $\Lambda^\vee = \operatorname{Hom}_A(\Lambda, A)$.
De plus, si Λ est un réseau, alors Λ° aussi.

Démonstration. On a des isomorphismes canoniques :

$$V^* = \operatorname{Hom}_K(V, K) \cong \operatorname{Hom}_K(\Lambda \otimes_A K, K) \cong \operatorname{Hom}_A(\Lambda, K)$$

puisque Λ est un quasi-réseau. Or le sous-module $\Lambda^\circ \subseteq V^*$ correspond via cet isomorphisme au sous-module $\Lambda^\vee = \operatorname{Hom}_A(\Lambda, A) \subseteq \operatorname{Hom}_A(\Lambda, K)$. Ainsi on a bien un isomorphisme canonique $\Lambda^\circ \cong \Lambda^\vee$. Ensuite, puisque Λ est de type fini sur un anneau noéthérien, il est aussi de présentation finie et donc par 1.52 :

$$V^* = \operatorname{Hom}_K(\Lambda \otimes_A K, K) \cong \operatorname{Hom}_A(\Lambda, A) \otimes_A K \cong \Lambda^\circ \otimes_A K$$

et l'isomorphisme obtenu $\Lambda^\circ \otimes_A K \longrightarrow V^*$ est bien le morphisme canonique. Ainsi Λ° est un quasi-réseau de V^* puisque il est aussi de type fini : en effet, il existe une surjection $A^n \longrightarrow \Lambda \longrightarrow 0$ qui induit une injection $0 \longrightarrow \Lambda^\vee \longrightarrow A^n$ et A est noéthérien. Si Λ est un réseau, son dual est encore libre donc son polaire est un réseau. □

Le polaire est compatible à la localisation.

Proposition 4.5. *Soit Λ un A-quasi-réseau de V et soit S une partie multiplicative de A ne contenant pas 0. On a :*

$$S^{-1}(\Lambda^\circ) = (S^{-1}\Lambda)^\circ.$$

Démonstration. On a une inclusion :

$$\Lambda^\circ \subseteq (S^{-1}\Lambda)^\circ$$

car pour tout $\alpha \in \Lambda^\circ$ et tout $x/s \in S^{-1}\Lambda$ avec $x \in \Lambda, s \in S$:

$$\alpha(x/s) = \frac{1}{s}\alpha(x) \in S^{-1}A$$

et comme $(S^{-1}\Lambda)^\circ$ est un $S^{-1}A$-module, on obtient :

$$S^{-1}(\Lambda^\circ) \subseteq (S^{-1}\Lambda)^\circ.$$

On a alors un diagramme commutatif :

$$\begin{array}{ccc} S^{-1}(\Lambda^\circ) & \hookrightarrow & (S^{-1}\Lambda)^\circ \\ \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \sim} \\ S^{-1}\operatorname{Hom}_A(\Lambda, A) & \xrightarrow[\sim]{} & \operatorname{Hom}_{S^{-1}A}(S^{-1}\Lambda, S^{-1}A) \end{array}$$

dont la flèche du bas est un isomorphisme d'après le théorème 1.52 car Λ est de présentation finie sur A.
L'inclusion est alors un isomorphisme et donc une égalité. □

Démonstration. On extrait une base B du K-espace vectoriel V contenue dans M. On pose alors $L = \operatorname{Vect}_A(B)$ qui est un réseau contenu dans M. □

Remarque 4.6. Pour les considérations algébriques, on aura souvent $K = \operatorname{Frac} A$. Dans ce cas, on a $V \otimes_A K = V$, et donc pour $M \subseteq V$ un sous-A-module, par platitude de K, la flèche $M \otimes_A K \longrightarrow V \otimes_A K = V$ est *toujours injective*.
On peut alors remplacer la définition de quasi-réseau par celle-ci qui lui est équivalente : Λ est un quasi-réseau s'il est de type fini comme A-module et si $K\Lambda = V$.
Attention, cela ne fonctionne plus pour K général.

La notion de quasi-réseau se comporte bien en changeant de corps contenant A.

Proposition 4.7. *Soit L un surcorps de K et Λ un sous-A-module de V.*
Alors Λ est un quasi-réseau (resp. réseau) de V si et seulement si Λ est un quasi-réseau (resp. réseau) de $V_L = V \otimes_K L$ via l'injection canonique $V \hookrightarrow V_L$ (puisque V est un K-module plat).

Démonstration. Le fait d'être de type fini sur A est inchangé. Supposons que $\Lambda \otimes_A K \longrightarrow V$ est un isomorphisme. On a alors :

$$\Lambda \otimes_A L = (\Lambda \otimes_A K) \otimes_K L \cong V \otimes_K L = V_L.$$

Réciproquement, si $\Lambda \otimes_A L \longrightarrow V_L$ est un isomorphisme alors on a un diagramme commutatif :

$$\begin{array}{ccc} \Lambda \otimes_A K & \longrightarrow & V \\ \downarrow & & \downarrow \\ \Lambda \otimes_A L & \xrightarrow[\sim]{} & V_L \end{array}$$

où la flèche de gauche est injective : en effet pour tout K-espace vectoriel W, la flèche $W \longrightarrow W \otimes_K L$ est injective car W est K-plat et ici $(\Lambda \otimes_A K) \otimes_K L = \Lambda \otimes_A L$. En particulier

la flèche du haut $\Lambda \otimes_A K \hookrightarrow V$ est injective, et il reste à voir qu'elle est surjective : si $x \in V \setminus \{0\}$, on peut écrire :

$$x = \ell\lambda \in V_L$$

avec $\lambda \in \Lambda$ et $\ell \in L$ par surjectivité de la flèche du bas, et puisque $\lambda \in V$ et $x \in V$, on a $\ell \in K$. Pour s'en convaincre, on peut supposer $V = K^n$, $V_L = L^n$ et regarder les coordonnées de x. Ainsi x est bien dans l'image de la flèche du haut.
Le cas des réseaux est clair. □

4.1.2 Quasi-réseaux sur un anneau de Dedekind

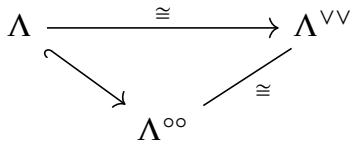
On suppose à présent que A est un anneau de Dedekind de corps des fractions K et que $A \neq K$ (en particulier la remarque 4.6 s'applique dans toute cette partie et donc un quasi-réseau de V est simplement un sous-A-module de type fini de V qui l'engendre K-linéairement). On se donne aussi V un K-espace vectoriel de dimension finie n et de dual V^*.
Par le théorème 3.48, les sous-modules de type fini de V sont projectifs car ils sont sans torsion, en particulier tout quasi-réseau est projectif.
Ainsi si A est principal, un quasi-réseau est automatiquement un réseau.

Proposition 4.8. *Soit Λ un quasi-réseau de V. On a alors l'égalité :*

$$\Lambda^{\circ\circ} = \Lambda$$

en identifiant V et V^{**} canoniquement.

Démonstration. Puisque Λ est projectif de type fini, le morphisme canonique $\Lambda \longrightarrow \Lambda^{\vee\vee}$ est un isomorphisme (voir 1.48). Il suffit alors de constater que le diagramme suivant commute :



□

La proposition suivante permet d'approcher un quasi-réseau par des réseaux.

Proposition 4.9. *(Approximation d'un quasi-réseau par des réseaux) Soit Λ un quasi-réseau de V. Il existe deux réseaux L_1, L_2 de V tels que :*

$$L_1 \subseteq \Lambda \subseteq L_2.$$

De plus, pour tout premier $\mathfrak{p}$, il existe L_1, L_2 deux réseaux de V (dépendant de $\mathfrak{p}$) tels que $L_1 \subseteq \Lambda \subseteq L_2$ et :

$$(L_1)_\mathfrak{p} = \Lambda_\mathfrak{p} = (L_2)_\mathfrak{p}.$$

Démonstration. On trouve un réseau L_1 contenu dans Λ et un réseau $\mathcal{L}_2$ contenu dans Λ° en prenant une base de V (respectivement V^*) contenue dans Λ (respectivement Λ°). On a alors $\Lambda^{\circ\circ} \subseteq \mathcal{L}_2^\circ$ et on conclut avec la proposition précédente.

Voyons le deuxième énoncé : $\Lambda_\mathfrak{p}$ est libre et possède une $A_\mathfrak{p}$-base $\underline{e}$ contenue dans Λ quitte à multiplier par des éléments inversibles.
On pose alors $L_1 = \mathrm{Vect}_A(\underline{e})$ qui est un A-réseau de V qui vérifie :

$$L_1 \subseteq \Lambda$$

et

$$(L_1)_\mathfrak{p} = \Lambda_\mathfrak{p}.$$

On construit L_2 par dualité en appliquant ce qui précède à Λ° et à l'aide de la proposition 4.5. □

4.1.3 Indice d'un couple de réseaux

On considère A un anneau noéthérien intègre de corps de fractions K et V un K-espace vecotoriel de dimension n.

Étant donnés deux réseaux ou quasi-réseaux de V, on peut se demander si l'un est plus étroit que l'autre.
Sur l'anneau $\mathbb{Z}$, une manière quantitative de mesurer ceci est d'inclure les deux réseaux L_1 et L_2 dans un plus grand réseau et de calculer la quantité (finie) :

$$[L_2 : L_1] = \frac{[L_3 : L_1]}{[L_3 : L_2]}$$

En général sur un anneau de Dedekind, les quotients de réseaux ne sont pas finis mais sont seulement des modules de type fini de torsion. On pourra alors définir un indice noté $(L_1 : L_2)$ qui sera cette fois-ci un idéal fractionnaire non nul de A.
On commence par le cas des réseaux.

Définition 4.10. *Soit L un A-réseau de V. Pour toute A-base $\underline{e}$ de L, on peut considérer le n-vecteur non nul $\wedge\underline{e} = e_1 \wedge \cdots \wedge e_n \in \Lambda^n_K V$.*
Si on change de base, on multiplie $\wedge\underline{e}$ par le déterminant du changement de base, donc par un élément de $A^\times$.
Ainsi la classe de $\wedge\underline{e}$ dans $\left(\Lambda^n_K V \setminus \{0\}\right)/A^\times$ ne dépend que du réseau L, on la note $\wedge(L)$.
Si L et M sont deux A-réseaux, puisque $\Lambda^n_K V$ est un K-espace vectoriel de dimension 1, on peut écrire $\wedge(M)$ comme un multiple de $\wedge(L)$ à un élément de $A^\times$ près :

$$\wedge(M) = \alpha \cdot \wedge(L)$$

On définit alors l'indice de M dans L par :

$$(L : M) = \frac{\wedge(M)}{\wedge(L)} = \alpha \in K^\times/A^\times.$$

De façon plus élémentaire, si $\underline{m}$ est une A-base de M et $\underline{\ell}$ est une A-base de L, l'indice est la classe modulo $A^\times$ du déterminant de la famille $\underline{m}$ dans la base $\underline{\ell}$.
Notons de plus que $K^\times/A^\times$ s'identifie au groupe des idéaux fractionnaires principaux non nuls de A et en particulier on peut voir $(L : M)$ comme un élément de $\mathcal{F}(A)^\times$.

Remarque 4.11. Il existe une notion voisine à celle d'indice d'un couple de réseaux : on peut considérer si $L \subseteq M$ l'idéal J annulateur de M/L (parfois noté aussi $(M : L)$ dans la littérature). Ces deux notions sont bien distinctes : par exemple pour $M = \mathbb{Z}^2$ et $L = \mathbb{Z}2e_1 + \mathbb{Z}4e_2$, on a $M/L = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ et l'annulateur est (4), tandis que l'indice est (8).
On verra plus tard que l'indice aussi ne dépend que du quotient M/L dans le cas $L \subseteq M$ (voir 4.19).

La proposition suivante est très facile à vérifier.

Proposition 4.12. *Soient L, M, N des réseaux de V. On a $(L : L) = 1$, $(L : M)(M : N) = (L : N)$ et $(L : M) = (M : L)^{-1}$. De plus si $M \subseteq L$, alors $(L : M)$ est un idéal contenu dans A et cet idéal est égal à A si et seulement si $M = L$.*

La notion d'indice d'un réseau est compatible à la localisation.

Proposition 4.13. *Soient L, M deux A-réseaux de V et S une partie multiplicative de A ne contenant pas 0. Alors $S^{-1}L$ et $S^{-1}M$ sont des $S^{-1}A$-réseaux de V et on a :*

$$(S^{-1}L : S^{-1}M) = S^{-1}(L : M)$$

dans le groupe $\mathcal{F}(S^{-1}A)^\times$.

Démonstration. Si $\underline{\ell}$ est une A-base de L alors c'est aussi une $S^{-1}A$-base de $S^{-1}L$ et le résultat en découle directement. □

Dans le cas d'un anneau principal, on dispose de la formule suivante.

Théorème 4.14. *On suppose A principal. Soient L et M deux A-réseaux de V avec $M \subseteq L$ (on peut toujours se ramener à ce cas en incluant les deux réseaux dans le réseau $L + M$). Le quotient L/M est un A-module de type fini de torsion car $(L/M) \otimes_A K = (L \otimes_A K)/(M \otimes_A K) = V/V = 0$.*
Supposons que :

$$L/M \cong A/(d_1) \oplus \cdots \oplus A/(d_k)$$

avec $d_i \geq 1$. On a alors :

$$(L : M) = \prod_i d_i \cdot A.$$

Démonstration. On se donne $\underline{\ell}$ une A-base de L et $\underline{m}$ une A-base de M. On note :

$$m_i = \sum_j a_{ij} \ell_j$$

avec $a_{ij} \in A$. On considère la matrice $P = (a_{ij}) \in \mathrm{GL}_n(K)$. Puisque P est à coeffients dans A, en utilisant la forme normale de Smith on écrit :

$$UPV = \mathrm{Diag}(t_1, \ldots, t_n)$$

avec $U, V \in \mathrm{GL}_n(A)$ et $t_1 \mid \cdots \mid t_n$. Ainsi puisque U et V ont leur déterminant dans $A^\times$ on a :

$$(L : M) = \prod_i t_i \cdot A$$

et il reste à voir que $\prod_i t_i \cdot A = \prod_j d_j \cdot A$. Or on a :

$$L/M \cong \operatorname{Coker} P \cong \operatorname{Coker} UPV = A/(t_1) \oplus \cdots \oplus A/(t_n) \cong A/(d_1) \oplus \cdots \oplus A/(d_k)$$

Pour tout p premier de A, en localisant, on obtient :

$$\bigoplus_i A_p/p^{v_p(t_i)} \cong \bigoplus_j A_p/p^{v_p(d_j)}$$

En prenant la longueur de ces A_p-modules on a :

$$\sum_i v_p(t_i) = \sum_j v_p(d_j)$$

et ceci est vrai pour tout p donc :

$$\prod_i t_i \cdot A = \prod_j d_j \cdot A.$$

□

Voyons deux cas particuliers fondamentaux : lorsque $A = \mathbb{Z}$ et lorsque A est un anneau de valuation discrète.

Corollaire 4.15. *Soient L et M deux A-réseaux de V avec $M \subseteq L$.*
Si $A = \mathbb{Z}$, on a :

$$(L : M) = [L : M] \cdot \mathbb{Z}$$

avec $[L : M]$ le cardinal du quotient (fini) L/M.
Si A est un anneau de valuation discrète d'idéal maximal $\mathfrak{m}$, alors $(L : M)$ est déterminé par sa valuation $\mathfrak{m}$-adique, qui est :

$$v_{\mathfrak{m}}((L : M)) = \operatorname{long}_A(L/M)$$

où long_A désigne la longueur d'un A-module.

Démonstration. Cela découle directement du théorème précédent en observant que pour Q un A-module de type fini de torsion, ou bien $A = \mathbb{Z}$ et le cardinal de Q est le produit de ses facteurs invariants, ou bien A est un anneau de valuation discrète d'idéal maximal $\mathfrak{m}$ et en écrivant $M \cong A/\mathfrak{m}^{t_1} \oplus \ldots A/\mathfrak{m}^{t_n}$ avec $t_1 \leq \cdots \leq t_n$ on a :

$$\operatorname{long}_A(M) = \sum_i \operatorname{long}_A(A/\mathfrak{m}^{t_i}) = \sum_i t_i.$$

□

4.1.4 Indice d'un couple de quasi-réseaux

On se place maintenant dans le cadre d'un *anneau de Dedekind* A de corps des fractions K et on considère V un K-espace vectoriel de dimension finie.
On souhaite étendre la définition de l'indice au cas des quasi-réseaux. Pour cela on procède en passant du local au global : pour tout premier $\mathfrak{p}$, le localisé d'un quasi-réseau est un réseau car $A_\mathfrak{p}$ est principal et l'indice a alors du sens.
Le lemme suivant indique que deux A-quasi-réseaux de V sont toujours localement égaux pour presque tout premier.

Lemme 4.16. *Soient L et M deux A-quasi-réseaux de V. Alors pour tout premier $\mathfrak{p}$ sauf éventuellement un nombre fini, on a :*

$$(L_\mathfrak{p} : M_\mathfrak{p}) = 1$$

et $L_\mathfrak{p} = M_\mathfrak{p}$.

Démonstration. Traitons d'abord le cas où $M \subseteq L$. C'est alors le même argument que 3.55 : puisque L/M est de torsion et de type fini, il existe $\lambda \in A \setminus \{0\}$ tel que :

$$\lambda L \subseteq M$$

et ainsi pour tout premier qui ne divise pas λ on a $L_\mathfrak{p} = M_\mathfrak{p}$.
En général, $L + M$ est un quasi-réseau contenu dans un réseau N d'après 4.9 et on a alors pour tout premier $\mathfrak{p}$ sauf un nombre fini :

$$L_\mathfrak{p} = N_\mathfrak{p}$$

et

$$M_\mathfrak{p} = N_\mathfrak{p}$$

aussi pour tout premier sauf un nombre fini. Ainsi en enlevant ces deux ensembles finis de premiers, on conclut. □

Définition 4.17. *Grâce au lemme précédent, on peut poser, pour L et M deux quasi-réseaux de V :*

$$(L : M) = \prod_\mathfrak{p} \mathfrak{p}^{v_{\mathfrak{p}_\mathfrak{p}}((L_\mathfrak{p} : M_\mathfrak{p}))} \in \mathcal{F}(A)^\times$$

et cette définition coïncide avec celle déjà connue dans le cas où L et M sont des quasi-réseaux car l'indice est compatible à la localisation d'après 4.13.

On vérifie encore facilement les propriétés suivantes qui découlent de leurs analogues pour les réseaux (voir 4.12).

Proposition 4.18. *Soient L, M, N des quasi-réseaux de V. On a $(L : L) = 1$, $(L : M)(M : N) = (L : N)$ et $(L : M) = (M : L)^{-1}$. De plus si $M \subseteq L$, alors $(L : M)$ est un idéal contenu dans A et cet idéal est A si et seulement si $L = M$.*

Le théorème 4.14 est encore valable.

Théorème 4.19. *Soient L et M deux A-quasi-réseaux de V avec $M \subseteq L$. Le quotient L/M est un A-module de type fini de torsion car $(L/M) \otimes_A K = (L \otimes_A K)/(M \otimes_A K) = V/V = 0$. Supposons que :*

$$L/M \cong A/I_1 \oplus \cdots \oplus A/I_k$$

avec I_i des idéaux non nuls de A (un tel isomorphisme peut provenir du théorème de structure 3.55 mais ici on n'impose pas de divisibilité entre les I_i). On a alors :

$$(L : M) = \prod_i I_i.$$

Démonstration. Soit $\mathfrak{p}$ un premier, on a :

$$(L : M)_\mathfrak{p} = (L_\mathfrak{p} : M_\mathfrak{p})$$

et $L_\mathfrak{p}/M_\mathfrak{p} \cong A_\mathfrak{p}/(I_1)_\mathfrak{p} \oplus \cdots \oplus A_\mathfrak{p}/(I_k)_\mathfrak{p}$ et donc, par 4.14 appliqué à l'anneau principal $A_\mathfrak{p}$:

$$(L_\mathfrak{p} : M_\mathfrak{p}) = \prod_i (I_i)_\mathfrak{p} = \left(\prod_i I_i\right)\mathfrak{p}$$

et ainsi $(L : M) = \prod_i I_i$. □

Corollaire 4.20. *(Théorème de Lagrange pour les indices) Soient L et M deux A-quasi-réseaux de V avec $M \subseteq L$.*
On a alors :

$$(L : M)L \subseteq M.$$

Démonstration. On écrit :

$$L/M \cong A/I_1 \oplus \cdots \oplus A/I_k$$

comme précedemment et on a $(L : M) = I_1 \cdot \cdots \cdot I_k$ qui annule le module L/M. □

Proposition 4.21. *Soient L et M deux A-quasi-réseaux de V. On a :*

$$(L^\circ : M^\circ) = (L : M)^{-1}.$$

Démonstration. Puisque le polaire (voir 4.5), l'indice et l'inversion d'idéaux sont compatibles à la localisation (l'inversion l'est car le produit l'est), on peut supposer que A est un anneau de valuation discrète et que L et M sont des réseaux de V. Il existe alors $\underline{\ell}$ une A-base de L et $\underline{m}$ une A-base de M et on note $\underline{\ell}^*$ et $\underline{m}^*$ les bases duales.
On note :

$$m_i = \sum_j a_{ij} \ell_j$$

et $P = (a_{ij}) \in \mathrm{GL}_n(K)$. On a alors pour tout $x = \sum_i x_i m_i \in V$:

$$\ell_j^*(x) = \ell_j^*\left(\sum_i x_i m_i\right) = \sum_i x_i a_{ij} = \sum_i a_{ij} m_i^*(x)$$

de sorte que :

$$\ell_j^* = \sum_i a_{ij} m_i^*$$

et :

$$\wedge \underline{\ell}^* = \det(P) \cdot \wedge \underline{m}^*$$

donc :

$$(L^\circ : M^\circ) = \frac{\wedge \underline{m}^*}{\wedge \underline{\ell}^*} A = \frac{1}{\det(P)} A = \frac{\wedge \underline{\ell}}{\wedge \underline{m}} A = (L : M)^{-1}$$

comme voulu. □

La proposition suivante s'obtient de la même façon en raisonnant localement : nous la laissons en exercice.

Proposition 4.22. *Soient L et M deux A-quasi-réseaux de V et f un automorphisme K-linéaire de V. On a alors :*

$$(L : f(M)) = \det(f)(L : M)$$

et :

$$(f(L) : M) = \det(f)^{-1}(L : M).$$

Le théorème suivant permet d'obtenir des génétareurs de l'indice $(L : M)$ avec des déterminants de familles contenues dans M dans des bases qui engendrent un réseau contenant L.
On peut le voir comme un énoncé de continuité : on peut approcher les quasi-réseaux par des réseaux (comme dans la proposition 4.9), et l'indice s'obtient comme une limite d'indices de réseaux. On rappelle que la somme d'idéaux correspond au pgcd et que l'intersection d'idéaux correspond au ppcm, selon 3.39.

Théorème 4.23. *(Approximation de l'indice) Soient L et M des A-quasi-réseaux de V et $L' \supseteq L$, $M' \subseteq M$ des A-quasi-réseaux de V. On a alors :*

$$(L : M) \mid (L' : M')$$

avec égalité si et seulement si $L = L'$ et $M = M'$.
De plus, si L et M sont deux quasi-réseaux de V, on a :

$$(L : M) = \sum_{L' \supseteq L, M' \subseteq M} (L' : M') = \bigcap_{L' \subseteq L, M' \supseteq M} (L' : M')$$

où L' et M' sont des réseaux.

Démonstration. On a, par 4.18 :

$$(L' : M')/(L : M) = (L' : L)(M : M') \subseteq A.$$

De plus on a égalité si et seulement si $(L : L')(M : M') = A$, or ce sont des idéaux de A donc leurs valuations sont positives, et c'est donc équivalent à avoir $(L : L') = A$ et

$(M : M') = A$, i.e. $L = L'$ et $M = M'$.
De ce qui précède on a :

$$(L : M) \mid \sum_{L' \supseteq L, M' \subseteq M} (L' : M')$$

où les L' et M' sont des réseaux. Il suffit de montrer que cette divisibilité est une égalité après localisation par $\mathfrak{p}$, pour tout $\mathfrak{p}$ premier. On a en effet :

$$(L : M)_\mathfrak{p} = (L_\mathfrak{p} : M_\mathfrak{p}) = \sum_{U \supseteq L_\mathfrak{p}, V \subseteq M_\mathfrak{p}} (U : V)$$

car $L_\mathfrak{p}$ et $M_\mathfrak{p}$ sont eux mêmes des réseaux. Il reste à se convaincre que :

$$\sum_{U \supseteq L_\mathfrak{p}, V \subseteq M_\mathfrak{p}} (U : V) = \sum_{L' \supseteq L, M' \subseteq M} (L'_\mathfrak{p} : M'_\mathfrak{p})$$

où les L' et M' sont des réseaux.
Chaque $(L'_\mathfrak{p} : M'_\mathfrak{p})$ intervient bien dans la somme de gauche. Réciproquement soient U et V des $A_\mathfrak{p}$-réseaux vérifiant $U \supseteq L_\mathfrak{p}$ et $V \subseteq M_\mathfrak{p}$.
On imite à présent la preuve de l'approximation des quasi-réseaux par des réseaux 4.9. Il existe une $A_\mathfrak{p}$-base $\underline{v}$ de V *contenue dans* M quitte à multiplier les vecteurs de la base par des inversibles. On considère alors le A-réseau $M' = \mathrm{Vect}_A(\underline{v})$ de sorte que $M'_\mathfrak{p} = V$ et $M' \subseteq M$.
Ensuite, on a $U^\circ \subseteq L_\mathfrak{p}^\circ$ car la polarisation commute à la localisation (4.5) donc de la même façon on trouve un réseau $\mathcal{L}$ de V^* tel que $\mathcal{L}_\mathfrak{p} = U^\circ$ et $\mathcal{L} \subseteq L^\circ$. On considère alors le réseau $L' = \mathcal{L}^\circ$ et on a bien :

$$L'_\mathfrak{p} = U$$

et

$$L' \supseteq L.$$

Ainsi $(U : V) = (L'_\mathfrak{p} : M'_\mathfrak{p})$ avec L' et M' des réseaux qui vérifient $L' \supseteq L$ et $M' \subseteq M$. On a donc bien l'énoncé voulu pour la somme.
L'énoncé pour l'intersection s'obtient en passant à l'inverse :

$$(L : M) = (M : L)^{-1} = \left(\sum_{M' \supseteq M, L' \subseteq L} (M' : L') \right)^{-1} = \bigcap_{M' \supseteq M, L' \subseteq L} (M' : L')^{-1} = \bigcap_{M' \supseteq M, L' \subseteq L} (L' : M')$$

ce qui est clair en prenant les valuations $\mathfrak{p}$-adiques. □

4.1.5 Réseaux sur un anneau euclidien

On considère A un anneau euclidien (en particulier A est intègre et principal, donc de Dedekind et tout ce qui précède s'applique, avec en plus le fait que tout quasi-réseau est un réseau). On note K le corps des fractions de A, et v le stathme euclidien sur A. Par convention, $v(0) = -\infty$.

On commence par mentionner un théorème qui permet de construire une base adaptée pour un sous-module de A^n.

Théorème 4.24. *(Base adaptée pour un sous-module) Soient $L \subseteq M$ deux A-modules libres de même rang n.*
Pour toute base $(m_1,\dots,m_n)$ de M il existe une base $(\ell_1,\dots,\ell_n)$ de L avec une matrice de passage $P = (p_{ij})$ triangulaire et à coefficients dans A, au sens où :

$$\ell_i = \sum_j p_{ij} m_j$$

avec $p_{ij} \in A$, et $p_{ij} = 0$ pour $j > i$, et de plus $v(p_{ij}) < v(p_{jj})$ pour $j < i$. De façon plus visuelle :

$$\begin{aligned}
\ell_1 &= p_{11} m_1 \\
\ell_2 &= p_{21} m_1 + p_{22} m_2 \\
\ell_3 &= p_{31} m_1 + p_{32} m_2 + p_{33} m_3 \\
&\vdots
\end{aligned}$$

En particulier P est inversible dans $M_n(K)$ car $p_{ii} \neq 0$.
Dans le cas où $A = \mathbb{Z}$, on peut aussi demander (en plus de tout cela) que les coefficients de P soient tous positifs.

Démonstration. Fixons $(m_1,\dots,m_n)$ une base de M. Puisque M et L sont de même rang, M/L est de torsion (c'est clair en tensorisant par K) et donc pour tout i l'ensemble :

$$L \cap \{p_{i1} m_1 + \cdots + p_{ii} m_i \mid p_{ij} \in A,\ p_{ii} \neq 0\}$$

est non vide. On prend $\ell_i = p_{i1} m_1 + \cdots + p_{ii} m_i$ dans cet ensemble avec $v(p_{ii})$ minimal.
Voyons maintenant que $(\ell_1,\dots,\ell_n)$ est une base de L. Elle est libre car la matrice de passage P est inversible dans $M_n(K)$. Il faut voir qu'elle engendre L. Soit $x \in L \setminus \{0\}$ qui n'est pas engendré par cette famille, on peut écrire :

$$x = x_1 m_1 + \cdots + x_k m_k$$

avec $k \leq n$ et $x_k \neq 0$ et k minimal. On écrit la division euclidienne :

$$x_k = q p_{kk} + r$$

avec $v(r) < v(p_{kk})$. On a alors :

$$x = q\ell_k + (x_1 - p_{k1}) m_1 + \cdots + (x_{k-1} - p_{k,k-1}) m_{k-1} + r m_k$$

donc $(x_1 - p_{k1}) m_1 + \cdots + (x_{k-1} - p_{k,k-1}) m_{k-1} + r m_k$ est un élément de L, et pour ne pas contredire la minimalité de $v(p_{ii})$, on a nécessairement :

$$r = 0$$

donc $(x_1 - p_{k1}) m_1 + \cdots + (x_{k-1} - p_{k,k-1}) m_{k-1}$ est un élément de L, et par minimalité de k, il est engendré par les ℓ_i, ce qui est absurde car dans ce cas x aussi.
Ainsi $\underline{\ell}$ est bien une base de L. On va à présent la modifier par un changement de

variable triangulaire pour obtenir les conditions supplémentaires du théorème. Pour cela, on considère des éléments de la forme :

$$\ell'_i = t_{i1}\ell_1 + \cdots + t_{ii}\ell_i$$

avec les t_{ij} dans A à choisir plus tard et $t_{ii} = 1$. Ainsi la matrice de passage $T = (t_{ij})$ est inversible dans A puisque de déterminant 1, et donc $\underline{\ell'}$ est encore une base de L.
En notant $P' = TP$, encore triangulaire et avec $p'_{ii} = p_{ii}$, on a ainsi :

$$\ell'_i = p'_{i1}m_1 + \cdots + p'_{ii}m_i$$

et il reste à s'assurer que l'on peut choisir les t_{ij} de sorte à avoir pour tout $j < i$:

$$v(p'_{ij}) < v(p'_{jj}) = v(p_{jj})$$

On fixe i et on va choisir $t_{i,i-1}$ puis $t_{i,i-2}$ jusqu'à $t_{i,1}$. On a :

$$p'_{i,i-1} = t_{i,i-1}p_{i-1,i-1} + p_{i,i-1}$$

ce qui permet, en faisant varier $t_{i,i-1}$, de choisir pour $p'_{i,i-1}$ n'importe quel élément congru à $p_{i,i-1}$ modulo $p_{i-1,i-1}$, et il en existe un (un reste dans la division euclidienne) qui vérifie :

$$v(p'_{i,i-1}) < v(p_{i-1,i-1})$$

et ainsi de suite avec les autres lignes du système.

Dans le cas où $A = \mathbb{Z}$, on commence par choisir les $p_{ii} > 0$ quitte à remplacer ℓ_i par son opposé, puis dans la suite on peut toujours prendre des restes positifs dans une division euclidienne, ce qui permet aussi d'avoir les p'_{ij} positifs. □

Le théorème précédent permet de construire une base de L à partir d'une base de M. On a un théorème analogue pour construire une base de M à partir d'une base de L.

Théorème 4.25. *(Base adaptée pour un sur-module) Soient $L \subseteq M$ deux A-modules libres de même rang n.*
Pour toute base $(\ell_1, \ldots, \ell_n)$ de L il existe une base $(m_1, \ldots, m_n)$ de M avec une matrice de passage $P = (p_{ij})$ triangulaire et à coefficients dans A, au sens où :

$$\ell_i = \sum_j p_{ij}m_j$$

avec $p_{ij} \in A$, et $p_{ij} = 0$ pour $j > i$, et de plus $v(p_{ij}) < v(p_{ii})$ pour $j < i$ (ce n'est pas la même condition que dans 4.24). De façon plus visuelle :

$$\begin{aligned}
\ell_1 &= p_{11}m_1 \\
\ell_2 &= p_{21}m_1 + p_{22}m_2 \\
\ell_3 &= p_{31}m_1 + p_{32}m_2 + p_{33}m_3 \\
&\vdots
\end{aligned}$$

En particulier P est inversible dans $M_n(K)$ car $p_{ii} \neq 0$.
Dans le cas où $A = \mathbb{Z}$, on peut aussi demander (en plus de tout cela) que les coefficients de P soient tous positifs.

Démonstration. Soit $\underline{\ell}$ une base de L. Puisque M/L est de torsion et de type fini, il existe $D \in A \setminus \{0\}$ tel que :

$$DM \subseteq L$$

Ainsi DM est un sous-A-module de L libre de rang n donc par le théorème précédent 4.24 il existe une base $(Dm_1, \dots, Dm_n)$ de DM telle que :

$$\begin{aligned} Dm_1 &= q_{11}\ell_1 \\ Dm_2 &= q_{21}\ell_1 + q_{22}\ell_2 \\ Dm_3 &= q_{31}\ell_1 + q_{32}\ell_2 + q_{33}\ell_3 \\ &\vdots \end{aligned}$$

avec $q_{ij} \in A$ et $q_{ii} \neq 0$. En inversant le système, on obtient un sytème toujours triangulaire :

$$\begin{aligned} \ell_1 &= u_{11}Dm_1 \\ \ell_2 &= u_{21}Dm_1 + u_{22}Dm_2 \\ \ell_3 &= u_{31}Dm_1 + u_{32}Dm_2 + u_{33}Dm_3 \\ &\vdots \end{aligned}$$

avec $U = Q^{-1} \in M_n(K)$. Puisque $\underline{m}$ est une base de M, les $u_{ij}D$ sont dans A. En posant $p_{ij} = Du_{ij}$, et en effectuant les mêmes manipulations que dans la preuve du théorème précédent pour avoir les inégalités sur les stathmes, on a ce qu'on souhaite. □

4.2 Étude géométrique

4.2.1 Propriétés élémentaires des réseaux

On fixe V un espace vectoriel réel de dimension $d \geq 1$. On pourrait définir un réseau de V comme un $\mathbb{Z}$-réseau de V au sens de 4.1, mais ce serait aller contre l'intuition géométrique élémentaire de la notion de réseau dans ce contexte. On donne donc la définition suivante, plus élémentaire, et on montre qu'elle est équivalente à celle de $\mathbb{Z}$-réseau.

Définition 4.26. *Un réseau de V est un sous-groupe Λ de V discret et libre de rang d.*

Avant de donner d'autres définitions équivalentes, mentionnons le théorème suivant sur les sous-groupes discrets de V.

Théorème 4.27. *Soit Λ un sous-groupe discret de V. Alors Λ est un groupe abélien libre de rang inférieur ou égal à d. De plus le rang de Λ est égal à la dimension du sous-espace de V engendré par Λ.*

Démonstration. Notons $W \subseteq V$ le sous-espace engendré par Λ. Il existe une base $(e_1, \dots, e_k)$ de W, avec $k \leq d$, contenue dans Λ. Notons Z le sous-groupe de W engendré par $e_1, \dots, e_k$: c'est un groupe abélien libre de rang k fermé et discret qui engendre $\mathbb{R}$-linéairement W, et donc le quotient W/Z est compact (en effet, il y a un isomorphisme

de paires de groupes topologiques entre (W,Z) et $(\mathbb{R}^k,\mathbb{Z}^k)$). Notons $\pi : W \longrightarrow W/Z$ la surjection canonique, de sorte que $\pi(\Lambda)$ est discret car π est ouverte et $Z \subseteq \Lambda$, et $\pi(\Lambda)$ est fermé dans W/Z car Λ est un fermé Z-saturé de W. Ainsi $\pi(\Lambda)$ est compact et discret donc *fini*. On a alors une suite exacte :

$$0 \longrightarrow Z \longrightarrow \Lambda \longrightarrow \pi(\Lambda) \longrightarrow 0$$

ce qui montre que Λ est de type fini, or Λ est sans torsion car contenu dans V, et par le théorème de structure des groupes abéliens de type fini, Λ est donc libre de même rang que Z (c'est clair en tensorisant la suite exacte par $\mathbb{Q}$ qui est plat sur $\mathbb{Z}$). □

Ceci permet la caractérisation suivante.

Proposition 4.28. *Soit Λ un sous-groupe de V. Les propositions suivantes sont équivalentes :*

(i) Λ *est un réseau de* V.

(ii) Λ *est discret et engendre linéairement* V.

(iii) Λ *est libre de rang* d *et engendre linéairement* V.

(iv) Il existe un isomorphisme $\mathbb{R}$*-linéaire entre* V *et* $\mathbb{R}^d$ *qui envoie* Λ *sur* $\mathbb{Z}^d$.

(v) Λ *est discret et cocompact (i.e* V/Λ *est compact).*

(vi) Λ *est un* $\mathbb{Z}$*-(quasi)-réseau de* V *au sens de 4.1.*

Démonstration. Si Λ est un réseau de V, il est par définition discret, et le théorème 4.27 assure alors que le rang de Λ est égal à la dimension de l'espace engendré par Λ, or ici Λ est de rang d donc il engendre linéairement V.
L'implication $(ii) \implies (iii)$ découle directement du théorème 4.27. Si (iii) est vrai, prenons $(e_1,\dots,e_d)$ une $\mathbb{Z}$-base de Λ qui est aussi une base de V puisqu'elle génère V. Ainsi on a un isomorphisme linéaire $V \longrightarrow \mathbb{R}^d$ qui envoie Λ sur $\mathbb{Z}^d$. Si un tel isomorphisme existe, c'est aussi un homéomorphisme donc Λ est discret.
Si (iv) est vraie, alors $\mathbb{R}^d/\mathbb{Z}^d$ et V/Λ sont homéomorphes donc V/Λ est compact. Enfin, si Λ est discret et cocompact, notons W l'espace $\mathbb{R}$-engendré par Λ, de sorte que $V/\Lambda \cong W/\Lambda \times V/W$. Donc V/W est compact et donc de dimension 0, i.e. $W = V$. Ceci montre $(v) \implies (ii)$, et $(ii) \implies (i)$ est immédiat avec le théorème 4.27.
Enfin le point (vi) est clairement équivalent au point (iii). □

On dispose d'une notion naturelle de sous-réseau : Λ' est un sous-réseau de Λ si c'est un sous-groupe de Λ qui est aussi un réseau de V.

Proposition 4.29. *Un sous-groupe Λ' de Λ est un sous-réseau de Λ si et seulement si il est d'indice fini dans Λ.*

Démonstration. On peut supposer $V = \mathbb{R}^d$ et $\Lambda = \mathbb{Z}^d$ en choisissant une $\mathbb{Z}$-base de Λ car les isomorphismes linéaires sont des homéomorphismes en dimension finie. Ainsi Λ' est un sous-groupe de $\mathbb{Z}^d$ donc est libre (car $\mathbb{Z}$ est principal) de rang $r \leq d$ et on a :

$$(\Lambda/\Lambda') \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^{d-r}$$

car $\mathbb{Q}$ est plat sur $\mathbb{Z}$. Ainsi Λ/Λ' est fini si et seulement si $d = r$ (car c'est un groupe abélien de type fini). □

Définition 4.30. *Soit D une partie de V et Λ un réseau de V. D est un domaine libre pour Λ si les $D+\lambda$, pour $\lambda \in \Lambda$, sont deux à deux disjoints. D est un domaine générateur pour Λ si les $D+\lambda$ recouvrent V. Enfin, D est un domaine fondamental pour Λ si c'est à la fois un domaine libre et un domaine générateur pour Λ, autrement dit si :*

$$V = \bigsqcup_{\lambda\in\Lambda} (D+\lambda)$$

À partir de maintenant on fixe μ une mesure de Lebesgue sur V. Le lemme suivant va permettre de définir un invariant pour les réseaux de V. Par analogie avec l'algèbre linéaire, on pourra l'appeler lemme de *Steinitz*.

Lemme 4.31. *Soit L un domaine libre et G un domaine générateur pour Λ un réseau de V. On les suppose mesurables. On a :*

$$\mu(L) \leq \mu(G)$$

Démonstration. Puisque L est libre, on a :

$$G \supseteq \bigsqcup_{\lambda\in\Lambda} (G \cap (L+\lambda))$$

On a donc, Λ étant dénombrable :

$$\mu(G) \geq \sum_{\lambda\in\Lambda} \mu(G\cap(L+\lambda)) = \sum_{\lambda\in\Lambda} \mu((G-\lambda)\cap L) = \sum_{\lambda\in\Lambda} \mu((G+\lambda)\cap L) \geq \mu\left(\bigcup_{\lambda\in\Lambda} (G+\lambda)\cap L\right) = \mu(L)$$

car G est génétareur. □

Proposition 4.32. *Tous les domaines fondamentaux mesurables pour Λ ont la même mesure. Cette mesure commune est un réel strictement positif.*

Démonstration. Le lemme de Steinitz 4.31 implique que deux domaines fondamentaux mesurables ont la même mesure. De plus Λ admet un domaine fondamental mesurable de mesure strictement positive : on peut supposer $V = \mathbb{R}^d$ et $\Lambda = \mathbb{Z}^d$ (quitte à changer la mesure de Lebesgue d'un facteur strictement positif) et prendre $D = [0,1[^d$ comme domaine fondamental. □

On appelle *covolume* de Λ la mesure d'un domaine fondamental de Λ, et on le note $\mathrm{covol}(\Lambda)$.

Remarque 4.33. L'inverse du covolume est parfois appelé *densité* du réseau Λ, et on la notera $\delta(\Lambda)$.

Proposition 4.34. *Soit $g \in \mathrm{GL}(V)$. On a*

$$\mathrm{covol}(g\Lambda) = |\det(g)|\,\mathrm{covol}(\Lambda)$$

En particulier, si $e_1,\dots,e_d$ est une $\mathbb{Z}$-base de Λ, le covolume de Λ est égal à la valeur absolue du déterminant de $(e_1,\dots,e_d)$ dans une base de V qui engendre un réseau de covolume 1. Si $\Lambda' \subseteq \Lambda$ est un sous-réseau, on a :

$$\frac{\mathrm{covol}(\Lambda')}{\mathrm{covol}(\Lambda)} = [\Lambda : \Lambda']$$

Démonstration. Le premier point découle de la formule du chnagement de variable. Pour le second point, prenons D un domaine fondamental mesurable de Λ et considérons $x_1, \dots, x_p$ un système de représentants de Λ/Λ'. On pose :

$$D' = \bigsqcup_i (D + x_i)$$

On vérifie alors sans problème que D' est un domaine fondamental mesurable de Λ'. Ainsi :

$$\operatorname{covol}(\Lambda') = p \operatorname{covol}(\Lambda)$$

or $p = [\Lambda : \Lambda']$, donc cela conclut.

□

4.2.2 Théorèmes de Blichfeldt et Minkowski

On fixe V un espace vectoriel réel de dimension $d \geq 1$, μ une mesure de Lebesgue sur V et Λ un réseau de V.

Théorème 4.35. *(Blichfeldt) Soit A une partie mesurable de V vérifiant $\mu(A) > \operatorname{covol}(\Lambda)$. Alors il existe $x, y \in A$ tels que $x - y \in \Lambda \setminus \{0\}$.*
Si A est compacte, on peut supposer seulement $\mu(A) \geq \operatorname{covol}(\Lambda)$.

Démonstration. Le premier point est exactement la contraposée du lemme de Steinitz 4.31, puisque si A ne vérifie pas la conclusion, A est libre donc de mesure inférieure ou égale à $\operatorname{covol}(\Lambda)$.

Si A est compacte et vérifie $\mu(A) \geq \operatorname{covol}(\Lambda)$, alors pour tout $n \geq 1$ l'ensemble mesurable $(1+1/n)A$ vérifie les conditions du premier point donc il existe $x_n, y_n \in (1+1/n)A$ vérifiant $x_n - y_n \in \Lambda \setminus \{0\}$. On écrit $x_n = (1+1/n)a_n$ et $y_n = (1+1/n)b_n$. Les suites (a_n) et (b_n) sont à valeurs dans A qui est compact donc admettent des valeurs d'adhérence a et b dans A, qui sont aussi valeurs d'adhérence de (x_n) et (y_n) respectivement donc par fermeture de $\Lambda \setminus \{0\}$, on a $a - b \in \Lambda \setminus \{0\}$. □

Le théorème suivant, dû à Minkowski, est fondamental en théorie des nombres. Il assure notamment l'existence de "petits" vecteurs dans un réseau.

Théorème 4.36. *(Minkowski) Soit $A \subseteq V$ mesurable, convexe (ou seulement stable par milieux) et symétrique par rapport à 0. Si $\mu(A) > 2^d \operatorname{covol}(\Lambda)$, alors A contient un élément non nul de Λ.*
Si A est de plus compacte, on peut supposer seulement $\mu(A) \geq 2^d \operatorname{covol}(\Lambda)$.
Si V est muni d'une norme $|\bullet|$, alors Λ possède un élément $\lambda \neq 0$ tel que :

$$|\lambda| \leq 2\left(\frac{\operatorname{covol}(\Lambda)}{\mu(B)}\right)^{1/d}$$

avec B la boule unité ouverte de V.

Démonstration. On pose $C = \frac{1}{2}A$ qui est bien mesurable et vérifie alors $\mu(C) > \mathrm{covol}(\Lambda)$ (ou $\mu(C) \geq \mathrm{covol}(\Lambda)$ dans le cas compact). Par le théorème de Blichfeldt 4.35, il existe donc $x, y \in C$ tels que $x - y \in \Lambda \setminus \{0\}$. Mais $x - y \in A$ car A est symétrique par rapport à 0 et stable par milieu, ce qui conclut pour les deux premiers points.
Soit $R > 0$, la boule unité fermée de rayon R, $R\overline{B}$, est convexe, compacte et symétrique par rapport à 0. De plus sa mesure est $R^d\mu(B)$, et ainsi dès que $R^d\mu(B) \geq 2^d\,\mathrm{covol}(\Lambda)$, $R\overline{B}$ possède un élément non nul du réseau. Il suffit donc de prendre $R = 2\left(\frac{\mathrm{covol}(\Lambda)}{\mu(B)}\right)^{1/d}$ pour conclure. □

4.2.3 Minima successifs et second théorème de Minkowski

On fixe V un espace vectoriel de dimension d muni d'une norme $|\bullet|$, et Λ un réseau de V. On note B la boule unité ouverte de V et $\overline{B}$ la boule unité fermée de V.

Lemme 4.37. *Soit A une partie discrète et fermée de V. Alors l'ensemble $N = \{|a| \mid a \in A\}$ est une partie discrète et fermée de $\mathbb{R}_+$. C'est en particulier le cas quand A est un réseau.*

Démonstration. On utilise un criète séquentiel. Soit (a_n) une suite d'éléments de A telle que $|a_n| \longrightarrow \ell$. Il s'agit de montrer $|a_n| = \ell$ à partir d'un certain rang (cela donne aussi la fermeture de N). La suite (a_n) est bornée et V est de dimension finie, et A est discrète et fermée, donc (a_n) prend un nombre fini de valeurs, et $(|a_n|)$ aussi, or cette suite converge donc elle est stationnaire. □

Définition 4.38. *(Minima successifs) Soit $1 \leq k \leq d$ un entier. On définit le k-ème minimum successif de Λ pour la norme $|\bullet|$ comme :*

$$\lambda_k = \inf\left\{r > 0 \mid \mathrm{Rg}\left(r\overline{B} \cap \Lambda\right) \geq k\right\}$$

où $\mathrm{Rg}(S)$ désigne le rang d'un sous-ensemble S de V, c'est à dire la dimension du sous-espace vectoriel engendré par S.

Proposition 4.39. *Dans la définition précédente, la borne inférieure est aussi un minimum. Ainsi, pour $r < \lambda_k$, la famille $\Lambda \cap r\overline{B}$ est de rang au plus $k-1$, et pour $r \geq \lambda_k$, elle est de rang au moins k.*

Démonstration. L'ensemble $N = \{|x| \mid x \in \Lambda\}$ est discret et fermé dans $\mathbb{R}_+$, donc il existe $u > \lambda_k$ tel que :

$$]\lambda_k, u] \cap N = \emptyset.$$

Ainsi pour tout $r \in [\lambda_k, u]$ on a :

$$r\overline{B} \cap \Lambda = \lambda_k\overline{B} \cap \Lambda$$

et donc les rangs de $\lambda_k\overline{B}$ et $u\overline{B}$ sont égaux et plus grands que k. □

Remarque 4.40. On a naturellement :

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_d.$$

Il n'y a aucune raison pour que ces inégalités soient strictes : par exemple pour $\Lambda = \mathbb{Z}^d \subseteq \mathbb{R}^d$ avec la norme euclidienne usuelle, on a $\lambda_1 = \lambda_2 = \cdots = \lambda_d = 1$.
De plus, la quantité λ_1 est simplement le minimum des normes des éléments non nuls de Λ. Par le premier théorème de Minkowski 4.36 on a d'ailleurs :

$$\lambda_1 \leq 2\left(\frac{\mathrm{covol}(\Lambda)}{\mu(B)}\right)^{1/d}$$

pour μ une mesure de Lebesgue quelconque sur V.

Théorème 4.41. *(Existence d'une base de Minkowski) Il existe des vecteurs $v_1, \ldots, v_d \in \Lambda$ linéairement indépendants tels que :*

$$|v_k| = \lambda_k$$

et en particulier :

$$\mathrm{Vect}_{\mathbb{R}}\left(\Lambda \cap \lambda_k \overline{B}\right) = \mathrm{Vect}_{\mathbb{R}}(v_1, \ldots, v_k)$$

(donc tout vecteur de Λ qui est hors de l'espace vectoriel engendré par $v_1, \ldots, v_k$ a une norme strictement supérieure à λ_k) pour tout $1 \leq k \leq d$.

Démonstration. Supposons $v_1, \ldots, v_{k-1}$ construits et vérifiant $|v_i| = \lambda_i$ pour $i < k$. Par 4.39, la famille $\lambda_k \overline{B} \cap \Lambda$ est de rang k et contient $v_1, \ldots, v_{k-1}$ donc il existe $v_k \in \Lambda$ hors de l'espace vectoriel engendré par les v_i pour $i < k$ tel que $|v_k| \leq \lambda_k$. On a nécessairement $|v_k| \geq \lambda_k$ par définition de λ_k, et donc :

$$|v_k| = \lambda_k$$

La deuxième affirmation vient du fait que ces deux espaces ont la même dimension et on a clairement $v_i \in \Lambda \cap \lambda_k \overline{B}$ pour $i \leq k$. □

Remarque 4.42. En général il n'existe pas de tels v_i qui forment une base de Λ. En revanche on a tout de même l'énoncé suivant qui repose sur le théorème 4.25 et qui assure l'existence d'une "petite" base de Λ.

Corollaire 4.43. *Il existe une base $(w_1, \ldots, w_d)$ de Λ vérifiant :*

$$|w_k| \leq 2^{k-1} \lambda_k$$

et

$$\Lambda \cap \lambda_k B \subseteq \mathrm{Vect}_{\mathbb{Z}}(w_1, \ldots, w_{k-1})$$

pour tout $1 \leq k \leq d$, où B désigne toujours la boule unité ouverte.

Démonstration. On prend une base (v_i) comme dans 4.41. Le groupe $\mathrm{Vect}_{\mathbb{Z}}(v_1, \ldots, v_k)$ est un sous-réseau de Λ. Par le théorème de la base adaptée 4.25 il existe alors une base $(w_1, \ldots, w_d)$ de Λ et des entiers a_{ij} tels que :

$$v_i = a_{i1} w_1 + \cdots + a_{ii} w_i$$

pour tout i, avec $0 \leq a_{ij} < a_{ii}$. On montre alors par récurrence forte que :

$$\left|w_j\right| \leq 2^{j-1} \lambda_j$$

pour tout j. Soit $j \geq 1$, on suppose que l'énoncé est vrai pour tout $k < j$, et on a alors :

$$\left|w_j\right| = \frac{\left|v_j - a_{j1}w_1 - \cdots - a_{j,j-1}w_{j-1}\right|}{a_{jj}} \leq \sum_{k=1}^{j-1} |w_k| + \lambda_j \leq \sum_{k=1}^{j-1} 2^{k-1}\lambda_k + \lambda_j \leq 2^{j-1}\lambda_j.$$

ce qui achève la récurrence.
On a ensuite pour tout k, par construction de $(v_1, \ldots, v_d)$:

$$\Lambda \cap \lambda_k B \subseteq \Lambda \cap \mathrm{Vect}_{\mathbb{R}}(v_1, \ldots, v_{k-1}) \subseteq \Lambda \cap \mathrm{Vect}_{\mathbb{R}}(w_1, \ldots, w_{k-1})$$

car le changement de base est triangulaire. Or $\Lambda \cap \mathrm{Vect}_{\mathbb{R}}(w_1, \ldots, w_{k-1}) = \mathrm{Vect}_{\mathbb{Z}}(w_1, \ldots, w_{k-1})$ puisque $\underline{w}$ est une base de Λ. □

Le second théorème de Minkowski donne un encadrement de la quantité :

$$\prod_{k=1}^{d} \lambda_k$$

qui généralise l'inégalité

$$\lambda_1 \leq 2\left(\frac{\mathrm{covol}(\Lambda)}{\mu(B)}\right)^{1/d}$$

issue du premier théorème de Minkowski. Il existe plusieurs versions de ce théorème, nous nous contentons de donner la plus simple, celle où la norme est supposée *euclidienne*.

Théorème 4.44. *(Second théorème de Minkowski) On suppose que la norme $|\bullet|$ est issue d'un produit scalaire $\langle \bullet, \bullet \rangle$ sur V. On a alors l'encadrement suivant, en choisissant μ une mesure de Lebesgue quelconque sur V :*

$$\beta_d \frac{\mathrm{covol}(\Lambda)}{\mu(B)} \leq \prod_{k=1}^{d} \lambda_k \leq 2^d \frac{\mathrm{covol}(\Lambda)}{\mu(B)}$$

avec :

$$\beta_d = \frac{\pi^{d/2}}{\Gamma(\frac{d}{2}+1)} = \frac{1}{\sqrt{\pi d}}\left(\frac{2\pi e}{d}\right)^{d/2}(1 + o(1))$$

le volume de la boule unité de $\mathbb{R}^d$.

Démonstration. La formule à démontrer ne dépend pas du choix de la mesure de Lebesgue, et on peut donc supposer qu'elle est compatible avec la structure euclidienne au sens où la mesure d'un hypercube bordé par une base orthonormale de V vaut 1.
On se donne des familles $(v_1, \ldots, v_d)$ et $(w_1, \ldots, w_d)$ comme dans les théorèmes 4.41 et 4.43 :
ce sont des familles linéairement indépendantes de vecteurs de Λ, avec $|v_i| = \lambda_i$, $\underline{w}$ est une base de Λ et on a :

$$\Lambda \cap \lambda_k B \subseteq \mathrm{Vect}_{\mathbb{Z}}(w_1, \ldots, w_{k-1})$$

pour tout k. On note $\Lambda' = \mathrm{Vect}_{\mathbb{Z}}(v_1, \dots, v_d)$, qui est un sous-réseau de Λ, donc d'indice fini dans Λ.
On note $[x_1, \dots, x_d]$ le produit mixte de la famille $x_1, \dots, x_d$, définie au signe près comme le déterminant de la famille $\underline{x}$ dans une base orthonormale de V.
Par l'inégalité d'Hadamard on a :

$$|[v_1, \dots, v_d]| \leq \prod_{k=1}^{d} |v_k| = \prod_{k=1}^{d} \lambda_k$$

et d'autre part :

$$|[v_1, \dots, v_d]| = \mathrm{covol}(\Lambda') = \mathrm{covol}(\Lambda) \cdot [\Lambda : \Lambda'] \geq \mathrm{covol}(\Lambda)$$

donc :

$$\prod_{k=1}^{d} \lambda_k \geq \mathrm{covol}(\Lambda) = \beta_d \frac{\mathrm{covol}(\Lambda)}{\mu(B)}$$

comme souhaité.
Montrons la majoration. Pour cela, par le procédé d'orthonormalisation de Schmidt, il existe $(e_1, \dots, e_d)$ une base orthonormale de V et des réels t_{ij} tels que :

$$w_i = \sum_{j \leq i} t_{ij} e_j$$

avec $t_{ii} > 0$. On considère alors les vecteurs :

$$w_i' = \sum_{j \leq i} \frac{t_{ij}}{\lambda_j} e_j$$

qui forment une base de V. Ces vecteurs engendrent un réseau L de V de covolume :

$$\mathrm{covol}(L) = \left| \det \left(\frac{t_{ij}}{\lambda_j} \right)_{i,j} \right| = \prod_i \frac{t_{ii}}{\lambda_i} = \frac{\mathrm{covol}(\Lambda)}{\prod_i \lambda_i}$$

Montrons à présent que le premier minimum successif de L est au moins égal à 1 :

$$\lambda_1(L) \geq 1$$

Soit $x \in L$ non nul, on écrit :

$$x = \sum_{i=1}^{p} x_i w_i' = \sum_{i=1}^{p} \sum_{j=1}^{i} \frac{t_{ij} x_i}{\lambda_j} e_j = \sum_{j=1}^{p} \left(\sum_{i=j}^{p} \frac{t_{ij} x_i}{\lambda_j} \right) e_j$$

avec $x_i \in \mathbb{Z}$ et $x_p \neq 0$ de sorte que :

$$\begin{aligned}
|x|^2 &= \sum_{j=1}^{p} \left(\sum_{i=j}^{p} \frac{t_{ij} x_i}{\lambda_j} \right)^2 \\
&= \sum_{j=1}^{p} \frac{1}{\lambda_j^2} \left(\sum_{i=j}^{p} t_{ij} x_i \right)^2 \\
&\geq \frac{1}{\lambda_p^2} \sum_{j=1}^{p} \left(\sum_{i=j}^{p} t_{ij} x_i \right)^2 \\
&= \frac{1}{\lambda_p^2} \left| \sum_{i=1}^{p} x_i w_i \right|^2 \\
&\geq 1
\end{aligned}$$

comme voulu, car $\sum_{i=1}^{p} x_i w_i \in \Lambda \setminus \mathrm{Vect}_{\mathbb{Z}}(w_1, \ldots, w_{p-1}) \subseteq V \setminus \lambda_p B$. Par le premier théorème de Minkowski on obtient :

$$1 \leq \lambda_1(L) \leq 2 \left(\frac{\mathrm{covol}(L)}{\mu(B)} \right)^{1/d}$$

et donc :

$$\prod_i \lambda_i \leq 2^d \frac{\mathrm{covol}(\Lambda)}{\mu(B)}.$$

□

4.2.4 Nombre de points d'un réseau dans un ensemble

Ce paragraphe s'inspire de [9].
On fixe V un espace vectoriel réel de dimension $d \geq 1$ muni d'une mesure de Lebesgue μ. Soit A une partie mesurable de V et Λ un réseau de V. Le but de ce paragraphe est d'estimer le nombre de points de Λ dans rA quand r tend vers l'infini en fonction de la densité de Λ (l'inverse du covolume) et de la mesure de A. Pour un A général, on ne peut pas s'attendre à un résultat satisfaisant : par exemple si $V = \mathbb{R}$, $\Lambda = \mathbb{Z}$ et $A = \mathbb{Q}$, A est de mesure nulle mais le nombre de points de $\Lambda \cap rA$ oscille entre 1 et l'infini. On va donner une condition nécessaire sur A pour avoir une bonne estimation. Rappelons que $\delta(\Lambda)$ est une notation pour l'inverse du covolume de Λ (appelé densité du réseau).

Définition 4.45. *Une partie A de V "intersecte bien les réseaux" si elle est mesurable de mesure finie et si pour tout réseau Λ de V, on a :*

$$|\Lambda \cap rA| = \mu(A)\delta(\Lambda) r^d + O(r^{d-1})$$

quand r tend vers $+\infty$ dans $]0, \infty[$. Cette borne inférieure est aussi un minimum

Remarque 4.46. C'est en effet l'estimation que l'on peut attendre (du moins pour le premier terme) si l'on croit l'appellation "densité" : quand r est très grand, le nombre de points de Λ dans rA devrait être de l'ordre du volume de rA multiplié par la densité de Λ, car cette densité représente le nombre de points de Λ par unité de volume.

La proposition suivante est suffisante pour la plupart des applications.

Proposition 4.47. *Une boule (fermée ou ouverte et pour n'importe quelle norme sur V) intersecte bien les réseaux.*
Si $A \sqcup B = C$, et si deux des trois parties A, B et C intersectent bien les réseaux, alors la troisième aussi. Toute partie finie intersecte bien les réseaux.
Soit A une partie qui intersecte bien les réseaux et $\varphi \in \mathrm{GL}(V)$ une bijection affine. Alors $\varphi(A)$ intersecte bien les réseaux.

Démonstration. Le second point est clair. Pour le troisième point, $\varphi(A)$ intersecte bien les réseaux puisque pour tout Λ un réseau, $\varphi^{-1}(\Lambda)$ est un réseau de densité $|\det(\varphi)|\,\delta(\Lambda)$ et on a :

$$\left|\varphi^{-1}(\Lambda) \cap rA\right| = \mu(A)\,|\det(\varphi)|\,\delta(\Lambda) r^d + O(r^{d-1})$$

donc $|\Lambda \cap r\varphi(A)| = \mu(A)\,|\det(\varphi)|\,\delta(\Lambda) r^d + O(r^{d-1}) = \mu(\varphi(A))\delta(\Lambda) r^d + O(r^{d-1})$.
Enfin, montrons que la boule $B(x,s)$ (fermée ou ouverte) de centre $x \in V$ et de rayon s intersecte bien les réseaux. On peut supposer $s = 1$ par ce qui précède. On note $\nu(r) = |\Lambda \cap rB(x,1)|$. Prenons $(e_1, \dots, e_d)$ une $\mathbb{Z}$-base de Λ et $D = \{\sum \lambda_i e_i \mid \lambda_i \in [0,1[\}$ un domaine fondamental mesurable associé. Soit $r > 0$ assez grand. Pour chaque point λ de $\Lambda \cap rB(x,1)$, on a :

$$D + \lambda \subseteq \overline{B(rx, r + C)}$$

avec C le diamètre de D.
Puisque D est un domaine *libre*, on a donc $\nu(r)\mu(D) \leq \mu(\overline{B(rx, r+C)})$, c'est à dire :

$$\nu(r) \leq \delta(\Lambda)(r + C)^d \mu(B(x,1))$$

Ensuite, la boule fermée $\overline{B(rx, r - 2C)}$ est recouverte par les $D + \lambda$ avec $\lambda \in \Lambda \cap B(rx, r)$: en effet, si $p \in \overline{B(rx, r-2C)}$, p est dans un certain $D + \lambda$ avec $|p - \lambda| \leq C$ donc $|\lambda - rx| \leq |\lambda - p| + |p - rx| \leq C + r - 2C \leq r - C < r$. On a donc :

$$(r - 2C)^d \mu(B(x,1)) \leq \nu(r)\mu(D)$$

On a ainsi :

$$\delta(\Lambda)\mu(B(x,1)) r^d + O(r^{d-1}) \leq \nu(r) \leq \delta(\Lambda)\mu(B(x,1)) r^d + O(r^{d-1})$$

en faisant un développement limité quand r tend vers l'infini.

□

Pour un énoncé sur le nombre d'idéaux de norme inférieure à r dans un anneau d'entiers de corps de nombres (voir 6.21), on a besoin du résultat suivant, bien plus fort (tiré de [9]) :

Théorème 4.48. *On munit V d'une norme quelconque. Soit A une partie mesurable de V telle qu'il existe $f_1, \dots, f_k : [0,1]^{d-1} \longrightarrow V$ lipschitziennes dont les images recouvrent la frontière (topologique) de A, notée ∂A. Alors A intersecte bien les réseaux.*

Remarque 4.49. Le fait que les boules intersectent bien les réseaux est un corollaire direct du théorème 4.48. Cependant la preuve donnée précedemment est bien plus facile que la preuve du théorème 4.48.

Démonstration. Par un isomorphisme linéaire se ramener au cas où $V = \mathbb{R}^d$ et $\Lambda = \mathbb{Z}^d$ quitte à changer les mesures par un facteur constant. Prenons C une constante de Lipschitz commune aux f_i. On note $D = [0,1[^d$ un domaine fondamental de Λ, et on s'intéresse d'abord à la quantité suivante :

$$m(r) = |\{\lambda \in \Lambda \mid (D+\lambda) \cap r\partial(A) \neq \emptyset\}|$$

c'est à dire au nombre de translatés de D qui intersectent le bord de rA. On commence par montrer le résultat suivant :

$$m(r) = O(r^{d-1})$$

quand r tend vers l'infini. Pour cela, on subdivise $[0,1]^{d-1}$ en $\lfloor r \rfloor^{d-1}$ petits "cubes" de façon naturelle, en faisant une grille d'arête de longueur $1/\lfloor r \rfloor$. Le diamètre de chacun de ces petits cubes est, par le théorème de Pythagore, $\sqrt{d-1}/\lfloor r \rfloor$ et donc pour tout i et tout petit cube γ, le diamètre de $rf_i(\gamma)$ vérifie :

$$\operatorname{diam}(rf_i(\gamma)) \leq C\sqrt{d-1}\frac{r}{\lfloor r \rfloor} \leq 2C\sqrt{d-1}$$

pour r assez grand.
Fixons maintenant $p \in rf_i(\gamma)$, on a donc $rf_i(\gamma) \subseteq \overline{B}(p, 2C\sqrt{d-1})$ tandis que la boule $\overline{B}(p, 2C\sqrt{d-1})$ intersecte au plus $(aC\sqrt{d-1}+b)^d$ translatés de domaines fondamentaux $D+\lambda$ avec a et b des constantes qui ne dépendent que de la norme choisie sur V : on peut s'en convaincre en incluant cette boule dans un pavé de côté suffisament grand, c'est à dire une constante fois le rayon de la boule puisque la norme choisie est équivalente à la norme infinie sur V. Puisque $r\partial A \subseteq \bigcup_\gamma \bigcup_i rf_i(\gamma)$, on a donc :

$$m(r) \leq k(aC\sqrt{d-1}+b)^d \times \lfloor r \rfloor^{d-1} = O(r^{d-1})$$

Ensuite, notons $\nu(r)$ le nombre de points du réseau dans rA. On va montrer que :

$$\left|\nu(r) - \mu(rA)\right| \leq 2m(r)$$

En effet, on a :

$$\begin{aligned}
\left|\nu(r) - \mu(rA)\right| &= \left| \sum_{x \in \Lambda \cap rA} 1 - \sum_{x \in \Lambda} \lambda(rA \cap (x+D)) \right| \\
&\leq \sum_{x \in \Lambda \cap rA} |1 - \lambda(rA \cap (x+D))| + \sum_{x \in \Lambda \setminus rA} \lambda(rA \cap (x+D)) \\
&\leq \sum_{x \in \Lambda \cap rA} \lambda((x+D) \setminus rA) + \sum_{x \in \Lambda \setminus rA} \lambda(rA \cap (x+D))
\end{aligned}$$

Puisque D est de mesure 1, le second terme est majoré par le nombre de points $x \in \Lambda \setminus rA$ qui vérifient $rA \cap (x+D) \neq \emptyset$. Par le théorème du passage à la douane, puisque D est connexe, ces points x vérifient aussi $(x+D) \cap r\partial A \neq \emptyset$ et donc le second terme est majoré par $m(r)$. Pour le premier terme, le même raisonnement montre qu'il est aussi majoré par $m(r)$.
On a donc finalement :

$$v(r) = \mu(rA) + O(r^{d-1}) = r^d \mu(A) + O(r^{d-1})$$

donc A intersecte bien les réseaux (ici Λ est de densité 1). □

Ce qui précède permet d'estimer le nombre de points d'un réseau dans un ensemble A suffisament "grand". On donne à présent une version exacte et non asymptotique pour une partie quelconque.

Théorème 4.50. *On suppose que V est muni d'une norme et on note λ_d le d-ème minimum successif de Λ pour cette norme (voir 4.38). Soit A une partie mesurable de V et F un domaine fondamental mesurable de Λ. On a :*

$$|\Lambda \cap A| \leq \frac{\mu(A+F)}{\mathrm{covol}(\Lambda)}$$

De plus, il existe un domaine fondamental F mesurable tel que F est contenu dans la boule fermée de centre 0 et rayon $2^{d-1} d\lambda_d$.

$$F \subseteq \overline{B}(0, 2^{d-1} d\lambda_d)$$

On a donc aussi :

$$|\Lambda \cap A| \leq \frac{\mu(A + \overline{B}(0, 2^{d-1} d\lambda_d))}{\mathrm{covol}(\Lambda)}.$$

Démonstration. Le premier point s'obtient en remarquant que :

$$\bigsqcup_{x \in \Lambda \cap A} (x+F) \subseteq A+F$$

et donc $\mu(F) \times |\Lambda \cap A| \leq \mu(A+F)$, ce qui donne la première inégalité. Ensuite, il existe une base (w_i) de Λ avec :

$$|w_k| \leq 2^{k-1} \lambda_k$$

pour tout k d'après le corollaire 4.43. On considère alors F le domaine fondamental bordé par la base (w_i) autrement dit :

$$F = \left\{ \sum_i t_i w_i \mid (t_i) \in [0,1[^d \right\}$$

et on a bien par inégalité triangulaire :

$$F \subseteq \overline{B}(0, 2^{d-1} d\lambda_d).$$

En réalité on peut même prendre $\sum_{k=1}^{d} 2^{k-1} \lambda_k$ plutôt que $2^{d-1} d\lambda_d$. □

4.2.5 Le théorème des 4 carrés par les réseaux

On donne une première application célèbre des réseaux en théorie des nombres : le théorème des 4 carrés de Lagrange, qui stipule que tout entier est somme de 4 carrés. La preuve donnée est basée sur le cours de Chenevier [3]. On énonce d'abord un lemme d'arithmétique.

Lemme 4.51. *Soit p un nombre premier. Tout élément de $\mathbb{F}_p$ est somme de deux carrés.*

Démonstration. Si $p = 2$, c'est évident. On suppose à présent $p \geq 3$ et on considère la suite exacte :

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{F}_p^\times \xrightarrow{x \mapsto x^2} \{x^2 \mid x \in \mathbb{F}_p^\times\} \longrightarrow 1$$

qui montre qu'il y a exactement $1 + \frac{p-1}{2} = \frac{p+1}{2}$ carrés dans $\mathbb{F}_p$. Ainsi pour tout $a \in \mathbb{F}_p$, les ensembles :

$$A = \{x^2 \mid x \in \mathbb{F}_p\}$$

et

$$B = a - A$$

sont de cardinal $\frac{p+1}{2}$ et sont contenus dans un ensemble de cardinal p donc :

$$|A \cap B| = |A| + |B| - |A \cup B| \geq p + 1 - p \geq 1$$

et ainsi on trouve $x, y \in \mathbb{F}_p$ tels que $x^2 = a - y^2$ et donc $a = x^2 + y^2$. □

Théorème 4.52. *(des 4 carrés de Lagrange) Soit n un entier naturel. Il existe a, b, c, d des entiers tels que :*

$$n = a^2 + b^2 + c^2 + d^2.$$

Démonstration. On peut clairement supposer $n \geq 1$. On traite d'abord le cas où n est sans facteur carré. Soit p un diviseur premier de n. D'après le lemme 4.51, il existe $u_p, v_p \in \mathbb{Z}$ tels que :

$$u_p^2 + v_p^2 \equiv -1 \ [p]$$

et par le théorème des restes Chinois, puisque n est sans facteur carré, on peut trouver $u, v \in \mathbb{Z}$ tels que pour tout p premier divisant n on ait $u \equiv u_p \ [p]$ et $v \equiv v_p \ [p]$ de sorte que :

$$u^2 + v^2 \equiv -1 \ [n].$$

On considère à présent le groupe suivant dans $\mathbb{R}^4$:

$$\Lambda = \Big\{(a, b, c, d) \in \mathbb{Z}^4 \mid c \equiv au + bv \ [n], d \equiv av - bu \ [n]\Big\}.$$

On a une suite exacte :

$$0 \longrightarrow \Lambda \longrightarrow \mathbb{Z}^4 \xrightarrow{f} (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \longrightarrow 0$$

avec $f(a, b, c, d) = (au + bv - c, av - bu - d)$. On voit que f est surjective en prenant par exemple $a = b = 0$ et en faisant varier c et d. Ainsi Λ est un sous-groupe de $\mathbb{Z}^4$ d'indice n^2 et donc de covolume n^2 vis à vis de la mesure de Lebesgue usuelle sur $\mathbb{R}^4$.

Par le premier théorème de Minkowsi 4.36 on trouve donc un vecteur $x = (a,b,c,d) \in \Lambda \setminus \{0\}$ tel que :

$$|x| \leq 2\left(\frac{\text{covol}(\Lambda)}{\mu(B)}\right)^{1/4} = 2\left(2! \cdot \frac{n^2}{\pi^2}\right)^{1/4} = \frac{2^{5/4}}{\pi^{1/2}}\sqrt{n}$$

avec $|\bullet|$ la norme euclidienne et B la boule unité fermée pour cette norme dont le 4-volume est donné par $\pi^2/2!$. Puisque $x \in \Lambda$, on a $c \equiv au + bv \ [n]$ et $d \equiv av - bu \ [n]$. Ainsi :

$$a^2+b^2+c^2+d^2 \equiv a^2+b^2+(au+bv)^2+(av-bu)^2 \equiv a^2+b^2+a^2(u^2+v^2)+b^2(u^2+v^2) \equiv 0 \ [n]$$

par construction de u et v. Ainsi :

$$n \mid |x|^2 \leq \frac{2^{5/2}}{\pi} n.$$

Puisque $x \neq 0$ et que $\frac{2^{5/2}}{\pi} < 2$, on a $|x|^2 = n$ autrement dit :

$$n = a^2 + b^2 + c^2 + d^2.$$

Traitons enfin le cas général. On écrit, pour tout nombre premier p divisant n :

$$v_p(n) = 2k_p + r_p$$

avec $r_p \in \{0,1\}$ de sorte que $n = \prod_p \left(p^{k_p}\right)^2 \prod_p p^{r_p} = m^2 s$ avec m un entier et s un entier naturel sans facteur carré. Ainsi par ce qui précède on peut écrire $s = a^2 + b^2 + c^2 + d^2$ avec $a,b,c,d \in \mathbb{Z}$ de sorte que :

$$n = (ma)^2 + (mb)^2 + (mc)^2 + (md)^2$$

ce qui conclut. □

Chapitre 5

Extensions de Dedekind

Des branches. Des feuilles.
Des pétioles. Des folioles.
Un monde ramifié qui bouge,
bruit et bondit.
Un royaume de verdures, de
vertiges et de vents.
Un labyrinthe de souffles et de
murmures.
Un arbre en somme.

Jacques Lacarrière

5.1 Généralités

Définition 5.1. *On appelle extension de Dedekind la donnée d'un anneau de Dedekind A de corps des fractions $K \neq A$ et d'une extension finie et séparable L de K. On note alors B la clôture intégrale de A dans L. On verra plus tard que B est encore un anneau de Dedekind, ce qui justifie la terminologie.*
Dans ce contexte, le K-espace vectoriel L est équipé d'une forme bilinéaire symétrique non dégénérée :

$$b(x,y) = \mathrm{Tr}_{L/K}(xy)$$

qui permet d'identifier L et son dual $L^* = \mathrm{Hom}_K(L,K)$, ce que l'on fera dans la suite. De plus, on a $B \cap K = A$ puisque A est intégralement clos, en particulier B n'est pas non plus un corps.

On fixe $A \subseteq B$ une extension de Dedekind.

Lemme 5.2. *On a l'égalité suivante :*

$$BK = L$$

et en particulier L est le corps des fractions de B.

Démonstration. Soit $x \in L$. Puisque L/K est finie, on peut écrire :

$$\sum_{k=0}^{m} a_k x^k = 0$$

avec $a_i \in A$ et $a_m \neq 0$. Ainsi on a, en multipliant par a_m^{m-1} :

$$\sum_{k=0}^{m} a_k a_m^{m-k-1} (a_m x)^k = 0$$

et donc $a_m x$ est entier sur A et donc $a_m x \in B$ ce qui permet de conclure. □

Théorème 5.3. *Le A-module B est un A-quasi-réseau de L. De plus B est un anneau de Dedekind et pour tout $\mathfrak{q}$ idéal premier non nul de B, $\mathfrak{q} \cap A$ est un idéal premier non nul de A. Dans le cas où A est principal, B est alors un réseau mais B n'a pas de raison d'être principal.*
De plus, tout idéal fractionnaire non nul de B est un A-quasi-réseau de L.

Démonstration. Puisque $BK = L$, il existe $\Lambda \subseteq B$ un A-réseau de L en prenant une base de V contenue dans B. On a alors :

$$B^\circ \subseteq \Lambda^\circ$$

Or sous-l'identification $L^* = L$, le polaire d'un A-module M est simplement $\{x \in L \mid \forall m \in M \ b(x,m) \in A\}$ et donc clairement $B \subseteq B^\circ$. Ainsi B est contenu dans un réseau donc B est de type fini puisque A est noéthérien. C'est donc un quasi-réseau de L.
Puisque $A \longrightarrow B$ est un morphisme entier, B est intégralement clos et B est noéthérien car de type fini sur A noéthérien.
Ensuite, comme B est un quasi-réseau de L, $B \otimes_A K \cong L$ et donc $\operatorname{Spec}(B \otimes_A K) \cong \operatorname{Spec} L$ qui est un singleton. Or la fibre de l'idéal nul par $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ est exactement :

$$\operatorname{Spec}(B \otimes_A K)$$

d'après 1.22. La fibre de l'idéal nul est donc le singleton réduit à l'idéal nul de B. Par conséquent, si $\mathfrak{q}$ est un idéal premier non nul de B, il n'est pas dans la fibre de l'idéal nul, et donc :

$$\mathfrak{q} \cap A \neq 0.$$

On en déduit que B est de dimension de Krull au plus 1 puisque si $\mathfrak{q}$ est un idéal premier non nul de B, $\mathfrak{p} = \mathfrak{q} \cap A$ est un idéal premier non nul de A donc maximal (car A est de dimension de Krull au plus 1) et le morphisme $A \longrightarrow B$ induit un morphisme injectif :

$$A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$$

qui fait de $B/\mathfrak{q}$ une $A/\mathfrak{p}$-algèbre intègre de dimension finie (car B est fini sur A). Une telle algèbre est un corps : si x est un élément non nul de cette algèbre, la multiplication par x est un endomorphisme $A/\mathfrak{p}$-linéaire injectif et donc surjectif par le théorème du rang. Ainsi $\mathfrak{q}$ est maximal.
Enfin, soit I un idéal fractionnaire non nul de B. Il existe $x \in I \setminus \{0\}$ de sorte que $KI \supseteq KxB = xL = L$ et I est de type fini sur B donc sur A donc c'est bien un A-quasi-réseau de L. □

Les extensions de Dedekind se comportent bien vis à vis de la localisation.

Proposition 5.4. *Soit S une partie multiplicative de A ne contenant pas 0. Alors $S^{-1}A \subseteq S^{-1}B$ est encore une extension de Dedekind avec pour corps de fractions K et L.*

Démonstration. L'anneau localisé $S^{-1}A$ est un anneau de Dedekind car le fait d'être noéthérien, intégralement clos et de dimension de Krull au plus 1 passe à la localisation. Le corps des fractions de $S^{-1}A$ est encore K. Vérifions que $S^{-1}B$ est la clôture intégrale de $S^{-1}A$ dans L.
Soit $b/s \in S^{-1}B$, ainsi b est entier sur A donc on peut écrire :

$$b^n = a_{n-1}b^{n-1} + \cdots + a_0$$

Puis :

$$(b/s)^n = a_{n-1}/s(b/s)^{n-1} + \cdots + a_0/s^n$$

donc b/s est entier sur $S^{-1}A$. Réciproquement, si $x \in L$ est entier sur $S^{-1}A$, on peut écrire :

$$x^n = a_{n-1}/s_{n-1}x^{n-1} + \cdots + a_0/s_0$$

et donc $x\prod s_i$ est entier sur A, or A est intégralement clos donc $x \in S^{-1}A$. □

Remarque 5.5. Se donner une extension de Dedekind revient exactement à se donner deux anneaux de Dedekind $A \subseteq B$ qui ne sont pas des corps avec B fini sur A et tel que $\operatorname{Frac} B/\operatorname{Frac} A$ est séparable. En effet, avec une telle donnée, en posant $K = \operatorname{Frac} A$ et $L = \operatorname{Frac} B$, on a que B est la clôture intégrale de A dans L car B est intégralement clos et entier sur A, et l'extension L/K est finie : elle est d'abord algébrique car la clôture algébrique de K dans L est un corps qui contient B donc c'est L, et il s'en suit que $KB = L$ avec le même raisonnement que précedemment, et donc le morphisme $B \otimes_A K \longrightarrow L$ est surjectif et L est une extension finie de K.

Proposition 5.6. *Les applications norme et trace $L \longrightarrow K$ se restreignent en des applications $B \longrightarrow A$. De même, le discriminant d'une famille d'éléments de B est un élément de A et le polynôme caractéristique d'un élément de B est à coefficients dans A.*

Démonstration. L'énoncé pour le discriminant découle de celui pour la trace.
Si A est local, B est un réseau et l'énoncé est clair car pour tout $x \in B$, l'endomorphisme μ_x peut se voir comme un endomorphisme A-linéaire du A-module libre B et donc dans une certaine base sa matrice est à coefficients dans A.
En général, il suffit de constater que pour tout $x \in B$, et pour tout $\mathfrak{p}$ premier, on a :

$$\chi_x^{L/K} \in A_{\mathfrak{p}}[X]$$

par ce qui précède, et donc $\chi_x^{L/K} \in A[X]$ (car $A = \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$) et le reste en découle. □

5.2 Ramification dans les extensions de Dedekind

Définition 5.7. *(Décomposition d'un premier dans une extension) On appellera premier tout idéal premier non nul d'un anneau de Dedekind. Pour un anneau de Dedekind qui*

n'est pas un corps, c'est simplement un idéal maximal.
Soit $\mathfrak{p}$ *un premier de* A*. L'idéal* $\mathfrak{p}B$ *est non nul et donc se factorise dans l'anneau de Dedekind* B*. On note, pour* $\mathfrak{q}$ *un premier de* B*,* $e(\mathfrak{q} \mid \mathfrak{p}) = v_{\mathfrak{q}}(\mathfrak{p}B)$ *l'indice de ramification de* $\mathfrak{q}$ *au dessus de* $\mathfrak{p}$*. On dit que* $\mathfrak{q}$ *est au dessus de* $\mathfrak{p}$ *si* $\mathfrak{p} \subseteq \mathfrak{q}$*, ou de manière équivalente si* $e(\mathfrak{q} \mid \mathfrak{p}) \geq 1$ *ou encore* $\mathfrak{q} \cap A = \mathfrak{p}$*. On a par définition :*

$$\mathfrak{p} = \prod_{\mathfrak{q}} \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}$$

et en particulier il n'y a qu'un nombre fini de premiers au dessus de $\mathfrak{p}$ *(c'est plus généralement vrai pour tout morphisme d'anneaux fini).*
Par le lemme de montée-descente 1.47, l'application $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *est surjective, autrement dit il existe toujours un premier au dessus de* $\mathfrak{p}$*.*
Par ce même lemme, tout premier $\mathfrak{q}$ *de* B *est au dessus d'un unique premier de* A*, à savoir* $\mathfrak{q} \cap A \neq 0$*.*
Enfin, si $\mathfrak{q}$ *est au dessus de* $\mathfrak{p}$*, puisque* $\mathfrak{p} \subseteq \mathfrak{q}$ *on a un plongement de corps :*

$$A/\mathfrak{p} \longrightarrow B/\mathfrak{q}$$

qui fait de $B/\mathfrak{q}$ *une extension finie de* $A/\mathfrak{p}$ *puisque* $A \longrightarrow B$ *est fini. On note alors* $f(\mathfrak{q} \mid \mathfrak{p})$ *le degré de cette extension, appelé indice d'inertie de* $\mathfrak{q}$ *au dessus de* $\mathfrak{p}$*.*
Un premier $\mathfrak{p}$ *de* A *est dit ramifié s'il existe* $\mathfrak{q}$ *au dessus de* $\mathfrak{p}$ *avec* $e(\mathfrak{q} \mid \mathfrak{p}) > 1$*. Il est dit totalement ramifié si :*

$$\mathfrak{p}B = \mathfrak{q}^e$$

pour un certain $\mathfrak{q}$ *premier de* B *et avec* $e > 1$*. Il est dit inerte si* $\mathfrak{p}B$ *est encore un premier de* B*, et enfin il est dit totalement décomposé si pour tout premier* $\mathfrak{q}$ *au dessus de* $\mathfrak{p}$*, on a :*

$$e(\mathfrak{q} \mid \mathfrak{p}) = f(\mathfrak{q} \mid \mathfrak{p}) = 1.$$

Les degrés de ramification et d'inertie satisfont une propriété de multiplicativité vis à vis des tours d'extensions.

Proposition 5.8. *Soit* $A \subseteq B \subseteq C$ *une tour d'extensions de Dedekind de corps de fractions* $K \subseteq L \subseteq M$*. Soient* $\mathfrak{p} \subseteq \mathfrak{q} \subseteq \mathfrak{r}$ *des premiers de* A*,* B *et* C *respectivement. Alors on a :*

$$e(\mathfrak{r} \mid \mathfrak{p}) = e(\mathfrak{r} \mid \mathfrak{q}) e(\mathfrak{q} \mid \mathfrak{p})$$

et

$$f(\mathfrak{r} \mid \mathfrak{p}) = f(\mathfrak{r} \mid \mathfrak{q}) f(\mathfrak{q} \mid \mathfrak{p}).$$

Démonstration. Le second point découle du théorème de la base télescopique pour les tours d'extensions. Montrons le premier point. On a :

$$\mathfrak{p}B = \prod_{\mathfrak{q}' \supseteq \mathfrak{p}} (\mathfrak{q}')^{e(\mathfrak{q}'|\mathfrak{p})}$$

où le produit porte sur les premiers de B au dessus de $\mathfrak{p}$. On a donc :

$$\mathfrak{p}C = \prod_{\mathfrak{q}' \supseteq \mathfrak{p}} (\mathfrak{q}'C)^{e(\mathfrak{q}'|\mathfrak{p})}$$

par le fait suivant : pour tous I, J idéaux de B, on a $IJC = (IC)(JC)$ car $CC = C$. On décompose alors chaque $\mathfrak{q}'C$ en produit de premiers de C pour obtenir :

$$\mathfrak{p}C = \prod_{\mathfrak{q}' \supseteq \mathfrak{p}} \prod_{\mathfrak{r}' \supseteq \mathfrak{q}'} (\mathfrak{r}')^{e(\mathfrak{r}'|\mathfrak{q}')e(\mathfrak{q}'|\mathfrak{p})}$$

où $\mathfrak{q}'$ désigne un premier de B et $\mathfrak{r}'$ un premier de C. On conclut alors en observant que si $\mathfrak{r}' = \mathfrak{r}$, alors il n'y a qu'un seul choix possible de $\mathfrak{q}'$, à savoir $\mathfrak{q}' = \mathfrak{q}$. □

Lemme 5.9. *Si A est semi-local (au sens où $\operatorname{Spec} A$ est fini), alors B est principal. En particulier, si A est un anneau de valuation discrète, B est principal (mais n'a aucune raision d'être un anneau de valuation discrète).*

Démonstration. Si $\operatorname{Spec} A$ est fini, puisque $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ est surjective et à fibres finies, le spectre de B est aussi fini, et un anneau de Dedekind semi-local est principal par le lemme 3.44. □

En particulier, pour tout premier $\mathfrak{p}$, l'anneau $B_{\mathfrak{p}}$ est principal et est un $A_{\mathfrak{p}}$-module libre de rang $[L : K]$ car c'est un $A_{\mathfrak{p}}$-réseau de L d'après 5.3.

Théorème 5.10. *Soit $\mathfrak{p}$ un premier de A. La localisation induit un morphisme surjectif $\mathcal{F}(A)^\times \longrightarrow \mathcal{F}(A_{\mathfrak{p}})^\times$ qui rentre dans le diagramme commutatif suivant :*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \operatorname{Ker} v_{\mathfrak{p}} & \longrightarrow & \mathcal{F}(A)^\times & \longrightarrow & \mathcal{F}(A_{\mathfrak{p}})^\times & \longrightarrow & 1 \\
 & & \cong \downarrow & & \cong \downarrow & & \cong \downarrow & & \\
0 & \longrightarrow & \bigoplus_{\mathfrak{p}' \in \operatorname{Spec} A \setminus \{0,\mathfrak{p}\}} \mathbb{Z}\mathfrak{p}' & \longrightarrow & \bigoplus_{\mathfrak{p}' \in \operatorname{Spec} A \setminus \{0\}} \mathbb{Z}\mathfrak{p}' & \longrightarrow & \mathbb{Z}\mathfrak{p}_{\mathfrak{p}} & \longrightarrow & 0
\end{array}$$

De plus, pour tout $I \in \mathcal{F}(A)^\times$, on a l'égalité :

$$v_{\mathfrak{p}}(I) = v_{\mathfrak{p}_{\mathfrak{p}}}(I_{\mathfrak{p}})$$

et deux idéaux fractionnaires sont égaux si et seulement si tous leurs localisés en les premiers de A le sont.

Démonstration. Le fait que ce morphisme est surjectif est clair : tout idéal de $A_{\mathfrak{p}}$ provient d'un idéal de A par localisation, et on en déduit que c'est aussi vrai pour les idéaux fractionnaires. Les isomorphismes verticaux sur le diagramme sont la traduction du théorème de factorisation en produit d'idéaux, et $A_{\mathfrak{p}}$ n'a qu'un seul premier car c'est un anneau de valuation discrète.
Le lemme 3.29 assure l'exactitude de cette suite. Le reste se déduit de la contemplation du diagramme. □

5.3 Norme relative

On introduit à présent le concept fondamental de *norme relative* d'un idéal. On la définit d'abord à partir de la notion d'indice d'un couple de quasi-réseaux (voir 4.17), mais on verra plus tard (théorème 5.16) deux autres définitions équivalentes possibles.

Définition 5.11. *Soit I un idéal fractionnaire non nul de B. On définit la norme relative de I par l'indice du couple de A-quasi-réseaux B, I :*

$$\|I\|_{B/A} = (B : I)$$

qui est un idéal fractionnaire non nul de A puisque I est un A-quasi-réseau de L d'après 5.3. On pose aussi :

$$\|0\|_{B/A} = 0.$$

Puisque l'indice se comporte bien avec la localisation, la norme aussi : pour toute partie multiplicative S de A ne contenant pas 0, on a ainsi :

$$\left\|S^{-1}I\right\|_{S^{-1}B/S^{-1}A} = S^{-1}\|I\|_{B/A}.$$

Remarquons que la norme d'un idéal principal est un idéal principal puisque pour tout $x \in L \setminus \{0\}$ on a :

$$\|xB\|_{B/A} = (B : xB) = N_{L/K}(b)(B : B) = N_{L/K}(b)A$$

d'après la proposition 4.22.

Théorème 5.12. *(Le morphisme norme) La norme $\|\bullet\|_{B/A}$ est un morphisme de groupes :*

$$\mathcal{F}(B)^\times \longrightarrow \mathcal{F}(A)^\times$$

autrement dit $\|IJ\|_{B/A} = \|I\|_{B/A} \cdot \|J\|_{B/A}$ pour tous $I, J \in \mathcal{F}(B)^\times$, et on a aussi $\left\|I^{-1}\right\|_{B/A} = \|I\|_{B/A}^{-1}$ et $\|B\|_{B/A} = A$.
De plus on a pour tout premier $\mathfrak{q}$ au dessus d'un premier $\mathfrak{p}$:

$$\|\mathfrak{q}\|_{B/A} = \mathfrak{p}^{f(\mathfrak{q}|\mathfrak{p})}$$

et ainsi pour tout I idéal fractionnaire non nul de B :

$$\|I\|_{B/A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\left(\sum_{\mathfrak{q} \supseteq \mathfrak{p}} v_{\mathfrak{q}}(I) f(\mathfrak{q} \mid \mathfrak{p})\right)}.$$

En particulier on a un diagramme commutatif de groupes abéliens :

$$\begin{array}{ccccccccc}
1 & \longrightarrow & B^\times & \longrightarrow & L^\times & \longrightarrow & \mathcal{F}(B)^\times & \longrightarrow & \mathrm{Cl}(B) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \|\bullet\|_{B/A}} & & \vdots{\scriptstyle \|\bullet\|_{B/A}} & & \\
1 & \longrightarrow & A^\times & \longrightarrow & K^\times & \longrightarrow & \mathcal{F}(A)^\times & \longrightarrow & \mathrm{Cl}(A) & \longrightarrow & 1
\end{array}$$

et un morphisme induit au niveau des groupes de classes, que l'on note toujours $\|\bullet\|_{B/A}$.

Démonstration. Notons que l'indice $f(\mathfrak{q} \mid \mathfrak{p})$ est compatible à la localisation par $\mathfrak{p}$, car :

$$B_{\mathfrak{p}}/\mathfrak{q}_{\mathfrak{p}} \cong (B/\mathfrak{q})_{\mathfrak{p}} = B/\mathfrak{q}.$$

Par compatibilité à la localisation il suffit donc de le prouver dans le cas où A est un anneau de valuation discrète d'idéal maximal $\mathfrak{p}$.
Il suffit alors de montrer la deuxième formule. On commence par le cas où $I \subseteq B$. Ainsi par le théorème chinois :

$$B/I \cong \prod_{\mathfrak{q}} B/\mathfrak{q}^{v_{\mathfrak{q}}(I)}.$$

Mais pour tout $k \geq 1$ on a une suite exacte :

$$0 \longrightarrow \mathfrak{q}^{k-1}/\mathfrak{q}^k \longrightarrow B/\mathfrak{q}^k \longrightarrow B/\mathfrak{q}^{k-1} \longrightarrow 0$$

Par le théorème de simplification 3.60 on a un isomorphisme de B-modules :

$$\mathfrak{q}^{k-1}/\mathfrak{q}^k \cong B/\mathfrak{q}$$

donc :

$$\operatorname{long}_A(B/\mathfrak{q}^k) = \operatorname{long}_A(B/\mathfrak{q}^{k-1}) + \operatorname{long}_A(B/\mathfrak{q})$$

et par récurrence :

$$\operatorname{long}_A(B/\mathfrak{q}^k) = k \cdot \operatorname{long}_A(B/\mathfrak{q}) = k \operatorname{long}_{A/\mathfrak{p}}(B/\mathfrak{q}) = k \cdot f(\mathfrak{q} \mid \mathfrak{p})$$

car $B/\mathfrak{q}$ est un $A/\mathfrak{p}$-espace vectoriel de dimension $f(\mathfrak{q} \mid \mathfrak{p})$. On a donc :

$$\operatorname{long}_A(B/I) = \sum_{\mathfrak{q}} v_{\mathfrak{q}}(I) \cdot f(\mathfrak{q} \mid \mathfrak{p})$$

et par 4.15 on a $v_{\mathfrak{p}}(\|I\|_{B/A}) = \operatorname{long}_A(B/I)$ ce qui conclut.
Enfin traitons le cas où I n'est pas contenu dans B. Puisque A est un anneau de valuation on a donc $B \subseteq I$.
Il existe $b \in B \setminus \{0\}$ tel que $bI \subseteq B$. On a alors avec la proposition 4.22 et le calcul de la norme d'un idéal principal fait précedemment :

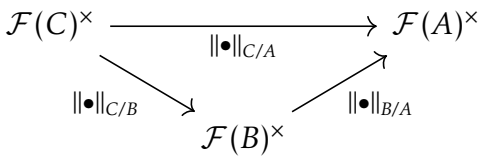
$$\|I\|_{B/A} = (B : I) = \frac{1}{N_{L/K}(b)}(B : bI) = \|bI\|_{B/A} / \|bB\|_{B/A}$$

et on conclut en utilisant ce qui précède sur les idéaux bI et bB qui sont contenus dans B. □

Définition 5.13. *Le noyau du morphisme* $\mathrm{Cl}(B) \longrightarrow \mathrm{Cl}(A)$ *est appelé groupe des classes relatif de B par rapport à A et est noté* $\mathrm{Cl}(B/A)$ *: c'est le groupe des idéaux fractionnaires de B modulo ceux dont la norme est un idéal fractionnaire principal de A. Si A est principal, on retrouve le groupe des classes de B.*

Avec la formule du théorème 5.12, il est facile de voir que la norme vérifie une propriété de transitivité (cela découle directement de 5.8).

Proposition 5.14. *Soit $A \subseteq B \subseteq C$ une tour d'extensions de Dedekind de corps de fractions $K \subseteq L \subseteq M$. Alors le diagramme suivant commute :*



Remarque 5.15. Si I est un idéal fractionnaire non nul de B qui est libre sur A et si B est libre sur A, de par la première définition de l'indice d'un couple de réseaux 4.10 on a :

$$\|I\|_{B/A} = \det_{\underline{b}}(\underline{e})A$$

avec $\underline{b}$ une A-base de B et $\underline{e}$ une A-base de I.

On peut donner une autre formule pour la norme relative : c'est l'objet de la proposition suivante.

Proposition 5.16. *Soit $I \in \mathcal{F}(B)^\times$. Les trois idéaux suivants sont égaux à la norme relative de I :*

- $(B : I)$
- $\displaystyle\prod_{\mathfrak{p}} \mathfrak{p}^{\left(\sum_{\mathfrak{q}\supseteq\mathfrak{p}} v_{\mathfrak{q}}(I) f(\mathfrak{q} \mid \mathfrak{p})\right)}$
- $\mathrm{Vect}_A(N_{L/K}(x) \mid x \in I)$.

Démonstration. On traite d'abord le cas où I est contenu dans B. On note :

$$N = \mathrm{Vect}_A(N_{L/K}(x) \mid x \in I)$$

et on remarque que pour tout $x \in I \setminus \{0\}$, on a $I \mid xB$ donc par ce qui précède :

$$\|I\|_{B/A} \mid N_{L/K}(x)A$$

et donc $N \subseteq \|I\|_{B/A}$, autrement dit :

$$\|I\|_{B/A} \mid N.$$

Pour établir l'autre divisibilité, soit $\mathfrak{p}$ un premier et $k \geq 0$ tel que $\mathfrak{p}^k \mid N$. Il s'agit de montrer que $\mathfrak{p}^k \mid \|I\|_{B/A}$, ou de façon équivalente que :

$$\mathfrak{p}_{\mathfrak{p}}^k \mid \left\|I_{\mathfrak{p}}\right\|_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}$$

Or $B_{\mathfrak{p}}$ est principal donc il existe $x \in I \setminus \{0\}$ tel que $I_{\mathfrak{p}} = xB_{\mathfrak{p}}$. Or $N_{L/K}(x) \in N$ donc :

$$\mathfrak{p}^k \mid N \mid N_{L/K}(x)$$

et $\left\|I_{\mathfrak{p}}\right\|_{B_{\mathfrak{p}}/A_{\mathfrak{p}}} = N_{L/K}(x)A_{\mathfrak{p}}$ donc $\mathfrak{p}_{\mathfrak{p}}^k \mid N_{L/K}(x)A_{\mathfrak{p}} = \left\|I_{\mathfrak{p}}\right\|_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}$ ce qui conclut.
Dans le cas général, on écrit $I = J/b$ avec J un idéal non nul de B et $b \in B \setminus \{0\}$, de sorte

que :

$$\begin{aligned}\mathrm{Vect}_A(N_{L/K}(x) \mid x \in I) &= \mathrm{Vect}_A(N_{L/K}(y/b) \mid y \in J) \\ &= \frac{1}{N_{L/K}(b)} \mathrm{Vect}_A(N_{L/K}(y) \mid y \in J) \\ &= \frac{\|J\|_{B/A}}{N_{L/K}(b)} \\ &= \|J\|_{B/A} \left\|b^{-1}B\right\|_{B/A} \\ &= \|I\|_{B/A}\end{aligned}$$

□

Les indices de ramification et d'inertie sont reliés par la formule suivante.

Théorème 5.17. *(Formule des degrés) Soit* $\mathfrak{p}$ *un premier de A. On a :*

$$[L : K] = \sum_{\mathfrak{q} \supseteq \mathfrak{p}} e(\mathfrak{q} \mid \mathfrak{p}) f(\mathfrak{q} \mid \mathfrak{p})$$

et pour tout idéal fractionnaire I de A :

$$\|IB\|_{B/A} = I^{[L:K]}.$$

Démonstration. On traite d'abord le cas local pour la deuxième formule : supposons que A est un anneau de valuation discrète, $\mathfrak{p} = (\pi)$ est alors l'unique premier de $\mathfrak{p}$ et on a :

$$\|\mathfrak{p}B\|_{B/A} = \|\pi B\|_{B/A} = N_{L/K}(\pi)A = \pi^{[L:K]}A = \mathfrak{p}^{[L:K]}A$$

comme souhaité.
Dans le cas général, il suffit de montrer la deuxième formule pour $I = \mathfrak{p}$ premier de A. On a alors d'une part :

$$\|\mathfrak{p}B\|_{B/A} = \prod_{\mathfrak{q} \supseteq \mathfrak{p}} \mathfrak{p}^{e(\mathfrak{q}|\mathfrak{p}) f(\mathfrak{q}|\mathfrak{p})}$$

par multiplicativité de la norme et en factorisant $\mathfrak{p}B$ dans B. Et d'autre part, par le cas local :

$$\left(\|\mathfrak{p}B\|_{B/A}\right)_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}^{[L:K]}$$

donc :

$$[L : K] = \sum_{\mathfrak{q} \supseteq \mathfrak{p}} e(\mathfrak{q} \mid \mathfrak{p}) f(\mathfrak{q} \mid \mathfrak{p})$$

et la formule pour la norme en découle. □

On dispose d'une formule pour l'indice de ramification en terme de longueur de modules.

Proposition 5.18. *Soit* $\mathfrak{q}$ *un premier de B au dessus de* $\mathfrak{p}$*. Alors on a :*

$$e(\mathfrak{q} \mid \mathfrak{p}) = \mathrm{long}_{B_{\mathfrak{q}}}(B/\mathfrak{p}B)_{\mathfrak{q}}$$

Démonstration. Par le théorème chinois, on a :

$$B/\mathfrak{p}B \cong \prod_{\mathfrak{q}' \supseteq \mathfrak{p}} B/\mathfrak{q}'^{e(\mathfrak{q}'|\mathfrak{p})}$$

En localisant et avec le lemme 3.29 :

$$(B/\mathfrak{p}B)_{\mathfrak{q}} \cong B_{\mathfrak{q}}/\mathfrak{q}_{\mathfrak{q}}^{e(\mathfrak{q}|\mathfrak{p})}$$

et la longueur de ce $B_{\mathfrak{q}}$-module est $e(\mathfrak{q} \mid \mathfrak{p})$. □

5.4 Polaire d'un idéal

On considère toujours B/A une extension de Dedekind de corps de fractions L/K. On identifie $L^* = \mathrm{Hom}_K(L, K)$ à L grâce à la forme bilinéaire symétrique non dégénérée $b(x, y) = \mathrm{Tr}_{L/K}(xy)$.

Proposition 5.19. *Soit I un idéal fractionnaire non nul de B. Alors I est un A-quasi-réseau de L et le polaire I° de I, sous l'identification $L = L^*$, est encore un idéal fractionnaire de B.*

Démonstration. D'abord I est un B-module de type fini et on a :

$$KI = L$$

car, en prenant un $x \in I \setminus \{0\}$ on a $KI \supseteq xKB = xL = L$. Donc I est un quasi-réseau de L. On a ensuite :

$$I^\circ = \{x \in L \mid \forall y \in I \ b(x, y) \in A\}$$

qui est un quasi-réseau de $L^* = L$ et qui est aussi un sous-B-module de L (car I l'est), de type fini comme A-module donc de type fini comme B-module. C'est donc bien un idéal fractionnaire de B. □

Remarque 5.20. Lorsque $B = A$, le polaire de I est simplement I^{-1} :

$$\{x \in K \mid \forall y \in I \ xy \in A\} = I^{-1}.$$

En général, on a toujours :

$$I^{-1} \subseteq I^\circ$$

autrement dit $I^\circ \mid I^{-1}$.

La formule suivante permet de calculer le polaire d'un idéal fractionnaire.

Proposition 5.21. *Soit I un idéal fractionnaire non nul de B. On a :*

$$I^\circ = I^{-1} B^\circ.$$

Démonstration. Soit $x \in I$ et $y \in I^\circ$. On a alors pour tout $b \in B$:

$$\mathrm{Tr}_{L/K}(bxy) \in A$$

car $bx \in I$. Ainsi on a :

$$II^\circ \subseteq B^\circ$$

donc $I^\circ \subseteq I^{-1}B^\circ$. Ensuite, soit $\beta \in B^\circ$ et $\alpha \in I^{-1}$. Soit $x \in I$. On a :

$$\mathrm{Tr}_{L/K}(\alpha\beta x) \in A$$

car $\alpha x \in B$. On a donc :

$$B^\circ I^{-1} \subseteq I^\circ$$

ce qui conclut. □

Par le théorème de l'élément primitif, on peut toujours trouver $\alpha \in B$ tel que $L = K[\alpha]$. Le théorème suivant donne une base de $A[\alpha]^\circ$.

Théorème 5.22. *Soit $\alpha \in B$ un générateur de l'extension L/K et $\pi_\alpha \in A[X]$ son polynôme minimal : c'est un polynôme unitaire à coefficients dans A de degré $n = [L : K]$ et séparable. Le dual du réseau $A[\alpha]$ est alors donné par :*

$$A[\alpha]^\circ = \frac{1}{\pi'_\alpha(\alpha)} A[\alpha].$$

Démonstration. On fixe Ω un corps algébriquement clos contenant L et Σ l'ensemble des plongements K-linéaires de L dans Ω : il y en a n car l'extension est séparable et :

$$\pi_\alpha = \prod_{\sigma \in \Sigma} (X - \sigma\alpha)$$

de sorte que :

$$\pi'_\alpha(\alpha) = \prod_{\sigma \neq \mathrm{id}} (\alpha - \sigma\alpha).$$

On pose :

$$Q(X) = \frac{\pi_\alpha(X)}{X - \alpha} = \prod_{\sigma \neq \mathrm{id}} (\alpha - \sigma\alpha)$$

de sorte que $\pi'_\alpha(\alpha) = Q(\alpha) \neq 0$. Pour tout k entre 0 et $n-1$ on pose :

$$f_k(X) = \frac{Q(X)}{Q(\alpha)} \alpha^k = \alpha^k \prod_{\sigma \neq \mathrm{id}} \frac{X - \sigma\alpha}{\alpha - \sigma\alpha} \in L[X]$$

On considère la trace de f_k :

$$\mathrm{Tr}(f_k) = \sum_{\sigma \in \Sigma} \sigma f_k \in K[X]$$

Les coefficients de ce polynôme sont les traces des coefficients de f_k donc il est à coefficients dans K. De plus on a :

$$\mathrm{Tr}(f_k)(\alpha) = \alpha^k$$

donc $\mathrm{Tr}(f_k) - X^k$ est divisible par π_α, or il est de degré au plus $n-1$ donc :

$$\mathrm{Tr}(f_k) = X^k.$$

On note $Q = \sum_{i=0}^{n-1} q_i X^i$ de sorte que, en identifiant les coefficients dans cette identité :

$$\mathrm{Tr}_{L/K}\left(\frac{q_i}{\pi'_\alpha(\alpha)}\alpha^k\right) = \delta_{ik}$$

et donc, en posant $e_i = \frac{q_i}{\pi'_\alpha(\alpha)} \in L$, on obtient la base duale de $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. Ainsi on a :

$$A[\alpha]^\circ = \bigoplus_{i=0}^{n-1} Ae_i.$$

Il reste à montrer que $\bigoplus_{i=0}^{n-1} Ae_i = \frac{1}{\pi'_\alpha(\alpha)} A[\alpha]$, autrement dit que la matrice de passage de $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ à $(q_0, \ldots, q_{n-1})$ est dans $\mathrm{GL}_n(A)$. Pour cela on écrit :

$$\pi_\alpha = \sum_{i=0}^{n} a_i X^i$$

avec $a_n = 1$. On a alors :

$$Q(X) = \frac{\pi_\alpha(X) - \pi_\alpha(\alpha)}{X - \alpha} = \sum_i a_i \frac{X^i - \alpha^i}{X - \alpha} = \sum_{i=0}^{n} a_i \sum_{j=0}^{i-1} \alpha^{i-j-1} X^j$$

de sorte que :

$$q_j = \sum_{i=j+1}^{n} a_i \alpha^{i-j-1}$$

et donc la matrice de passage de $(\alpha^{n-1}, \ldots, 1)$ à $(q_0, \ldots, q_{n-1})$ est triangulaire, à coefficients dans A, et avec des $a_n = 1$ sur la diagonale, donc elle est dans $\mathrm{GL}_n(A)$. □

5.5 Différent et discriminant relatif

On considère toujours B/A une extension de Dedekind de corps de fractions L/K.

Définition 5.23. *On définit l'idéal différent de l'extension B/A comme :*

$$\mathrm{Diff}_{B/A} = (B^\circ)^{-1}.$$

Puisque $B \subseteq B^\circ$, on a $\mathrm{Diff}_{B/A} \subseteq B$. C'est un idéal non nul de B. L'idéal différent est compatible à la localisation au sens où pour toute partie multiplicative S de A ne contenant pas 0, on a :

$$\mathrm{Diff}_{S^{-1}B/S^{-1}A} = S^{-1}\,\mathrm{Diff}_{B/A}$$

puisque c'est le cas pour l'inversion et pour la polarisation.
Soit M un A-quasi-réseau de L. On définit son discriminant $\mathrm{Disc}_{B/A}(M)$ comme l'idéal fractionnaire non nul de A suivant :

$$\mathrm{Disc}_{B/A}(M) = (M^\circ : M).$$

Cette définition sera justifiée dans la suite de ce paragraphe. Enfin on définit le discriminant de l'extension B/A :

$$\mathcal{D}_{B/A} = \mathrm{Disc}_{B/A}(B) = (B^\circ : B)$$

qui est un idéal contenu dans A puisque $B \subseteq B^\circ$. Ainsi le discriminant de l'extension B/A mesure à quel point B est loin d'être égal à B°.
On a alors la relation suivante entre le différent et le discriminant de l'extension B/A :

$$\mathcal{D}_{B/A} = \left\|\mathrm{Diff}_{B/A}\right\|_{B/A}.$$

Encore une fois, le discriminant est compatible à la localisation.
La notion de discriminant peut se généraliser au contexte d'un K-espace vecotoriel quelconque muni d'une forme bilinéaire symétrique non dégénérée mais nous n'en ferons pas usage ici.

Remarque 5.24. Pour tout idéal fractionnaire non nul I de B, on a en appliquant la proposition 5.21 :

$$\mathrm{Disc}_{B/A}(I) = \|I\|^2 \cdot \mathcal{D}_{B/A}.$$

En effet :

$$\mathrm{Disc}_{B/A}(I) = (I^\circ : I) = (I^{-1}B^\circ : I) = (I^{-1}B^\circ : B)(B : I) = \left\|I^{-1}B^\circ\right\|^{-1} \|I\| = \|I\|^2 \mathcal{D}_{B/A}.$$

Proposition 5.25. *Soit M un A-quasi-réseau de L et u un automorphisme K-linéaire de L. On a :*

$$\mathrm{Disc}_{B/A}(u(M)) = \det(u)^2 \,\mathrm{Disc}_{B/A}(M).$$

Démonstration. On remarque d'abord que :

$$u(M)^\circ = (u^*)^{-1}(M^\circ)$$

avec u^* l'automorphisme adjoint de u pour la forme non dégénérée donnée par $\mathrm{Tr}(xy)$.
On a alors :

$$\mathrm{Disc}_{B/A}(u(M)) = (u(M)^\circ : u(M)) = ((u^*)^{-1}(M^\circ) : u(M)) = \det(u)\cdot\det(u^*)\cdot(M^\circ : M) = \det(u)^2\,\mathrm{Disc}_{B/A}(M)$$

d'après 4.22. □

Remarque 5.26. Si $M \subseteq B$, alors le discriminant de M est contenu dans A car $M \subseteq M^\circ$.
De façon générale, en appliquant le théorème 4.23, on voit que si $M \subseteq M'$, alors :

$$\mathrm{Disc}_{B/A}(M') \mid \mathrm{Disc}_{B/A}(M).$$

Plus précisément :

$$\mathrm{Disc}_{B/A}(M) = (M' : M)^2 \cdot \mathrm{Disc}_{B/A}(M').$$

On voit alors que si $M \subseteq M'$, on a $M = M'$ si et seulement si $\mathrm{Disc}_{B/A}(M) = \mathrm{Disc}_{B/A}(M')$.

Dans le cas où M est un A-réseau, le mot "discriminant" fait sens car $\mathrm{Disc}_{B/A}(M)$ est alors l'idéal engendré par le discriminant d'une quelconque A-base de M.

Proposition 5.27. *Soit M un A-réseau de L et $\underline{e}$ une A-base de M. On a alors :*

$$\mathrm{Disc}_{B/A}(M) = D_{L/K}(e_1, \dots, e_n) \cdot A$$

avec $\underline{b}$ une A-base quelconque de B.

Démonstration. Puisque M est un A-réseau, M° est aussi un A-réseau. Notons $\underline{e}^*$ la base duale de $\underline{e}$: c'est une A-base de M°.
On écrit :

$$e_i^* = \sum_j a_{ij} e_j$$

avec $a_{ij} \in K$. De $\mathrm{Tr}(e_i^* e_j) = \delta_{ij}$ on obtient en notant P la matrice (a_{ij}) et T la matrice $(\mathrm{Tr}(e_i e_j))$:

$$PT = I_n$$

où I_n désigne la matrice identité. Par définition du discriminant relatif :

$$\mathrm{Disc}_{B/A}(M) = (M^\circ : M) = \det_{\underline{e}^*}(\underline{e})A = \det(P)^{-1}A = \det(T)A = D_{L/K}(\underline{e})A$$

comme voulu. □

La proposition précédente permet de déterminer les valuations du discriminant : pour tout premier $\mathfrak{p}$, $M_\mathfrak{p}$ est un $A_\mathfrak{p}$-réseau et le discriminant est compatible à la localisation donc on a :

$$v_\mathfrak{p}(\mathrm{Disc}_{B/A}(M)) = v_\mathfrak{p}(D_{L/K}(\underline{e}))$$

avec $\underline{e}$ une $A_\mathfrak{p}$-base de $M_\mathfrak{p}$ (qui dépend de $\mathfrak{p}$). C'est d'ailleurs comme cela que la plupart des ouvrages définissent le discriminant relatif d'une extension.

Corollaire 5.28. *Soit M un A-réseau de L et $\underline{e}$ une famille de vecteurs de M. On a alors $D_{L/K}(\underline{e}) \in \mathrm{Disc}_{B/A}(M)$, et $D_{L/K}(\underline{e})$ engendre le discriminant de M si et seulement si $\underline{e}$ est une A-base de M.*

Démonstration. Notons $N = \mathrm{Vect}_A(\underline{e})$. Si $\underline{e}$ n'est pas libre, l'énoncé est clair (le discriminant de $\underline{e}$ est nul).
Sinon, N est un réseau contenu dans M et donc son discriminant est contenu dans celui de M avec égalité si et seulement si $N = M$ d'après la remarque 5.26.
On conclut alors avec la proposition précédente 5.27. □

Le discriminant peut être obtenu en utilisant une approximation par des réseaux.

Théorème 5.29. *Soit M un A-quasi-réseau de L. On a la formule suivante :*

$$\mathrm{Disc}_{B/A}(M) = \sum_{\underline{e} \subseteq M} D_{L/K}(\underline{e})A = \bigcap_{\mathrm{Vect}_A(\underline{e}) \supseteq M} D_{L/K}(\underline{e})A.$$

Démonstration. Il suffit d'adapter la preuve de 4.23 :
Cela revient à montrer que pout $\mathfrak{p}$:

$$\sum_{U \subseteq M_\mathfrak{p}} (U^\circ : U) = \sum_{L \subseteq M} (L^\circ_\mathfrak{p} : L_\mathfrak{p})$$

où les L et les U sont des réseaux. Mais si $U \subseteq M_\mathfrak{p}$, il existe L un A-réseau tel que $L \subseteq M$ et $L_\mathfrak{p} = U$ (en prenant $\underline{e}$ une $A_\mathfrak{p}$-base de U contenue dans M et en posant $L = \mathrm{Vect}_A(\underline{e})$).
On a alors :

$$(U^\circ : U) = (L^\circ_\mathfrak{p} : L_\mathfrak{p})$$

et donc ces deux sommes sont égales.
Pour l'intersection, il suffit de remarquer que $\mathrm{Disc}_{B/A}(M^\circ) = \mathrm{Disc}_{B/A}(M)^{-1}$. □

Le théorème de Lagrange pour les indices 4.20 s'applique au cas particulier du discriminant d'un quasi-réseau.

Théorème 5.30. *Soit $M \subseteq B$ un A-quasi-réseau de L. On a alors :*

$$B \subseteq \mathrm{Disc}_{B/A}(M)^{-1} M.$$

Ainsi, si $\underline{e}$ une K-base de L contenue dans B, en notant $d = D_{L/K}(\underline{e})$, tout élément de B s'écrit $\frac{1}{d}\sum_i \lambda_i e_i$ avec $\lambda_i \in A$. De plus on a $d \mid \lambda_i^2$ pour tout i.

Démonstration. Par le théorème de Lagrange pour les indices 4.20, on a :

$$(M^\circ : M) M^\circ \subseteq M$$

car $M \subseteq M^\circ$. Puisque $M \subseteq B$, on a $M \subseteq B \subseteq B^\circ \subseteq M^\circ$ et donc :

$$(M^\circ : M) B \subseteq (M^\circ : M) M^\circ \subseteq M$$

d'où :

$$B \subseteq \mathrm{Disc}_{B/A}(M)^{-1} M.$$

Ainsi, en notant $M = \mathrm{Vect}_A(\underline{e})$, M est un quasi-réseau contenu dans B et donc :

$$B \subseteq \frac{1}{d} M$$

par 5.27.
Montrons enfin que si $b = \sum_i \frac{\lambda_i}{d} e_i \in B$, alors $d \mid \lambda_i^2$ pour tout i.
Pour cela, fixons $\overline{L}$ un corps algébriquement clos contenant L et numérotons $\sigma_1, \ldots, \sigma_n$ les K-plongements de L dans $\overline{L}$.
On note $\overline{A}$ la clôture intégrale de A dans $\overline{L}$ de sorte que la matrice $P = (\sigma_i(e_j))$ est à coefficients dans $\overline{A}$ et de l'identité :

$$\overline{A} \ni \sigma_i(b) = \sum_j \frac{\lambda_j}{d} \sigma_i(e_j)$$

on obtient, en inversant le système et en utilisant la formule de Cramer qui donne que P^{-1} est à coefficients dans $\frac{1}{\det P}\overline{A}$:

$$\frac{\lambda_j}{d} \in \frac{1}{\det P}\overline{A}$$

et ainsi $\frac{\det P \cdot \lambda_j}{d} = \frac{\lambda_j}{\det P}$ est entier sur A (on utilise ici la formule 2.14 selon laquelle $d = \det(P)^2$). Donc $\frac{\lambda_j^2}{(\det P)^2} = \frac{\lambda_j^2}{d}$ est dans $\overline{A} \cap K = A$, et on a bien :

$$d \mid \lambda_j^2.$$

□

Remarque 5.31. Si $L = K[\alpha]$ avec $\alpha \in B$, le théorème 5.22 donne :

$$A[\alpha]^\circ = \frac{1}{\pi'_\alpha(\alpha)} A[\alpha]$$

donc

$$\mathrm{Disc}_{B/A}(A[\alpha]) = (A[\alpha]^\circ : A[\alpha]) = N_{L/K}(\pi'(\alpha))A$$

en utilisant la proposition 4.22. Ceci est cohérent avec la formule :

$$D_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\binom{d}{2}} N_{L/K}(\pi'_\alpha(\alpha))$$

du théorème 2.15.

Proposition 5.32. *Soit $\alpha \in B$ tel que $L = K[\alpha]$. Pour tout premier $\mathfrak{p}$ ne divisant pas $(B : A[\alpha])$ (donc pour une infinité de premiers), on a :*

$$(\mathrm{Diff}_{B/A})_\mathfrak{p} = \pi'_\alpha(\alpha) B_\mathfrak{p}$$

et pour le discriminant :

$$(\mathrm{Disc}_{B/A})_\mathfrak{p} = \mathrm{Disc}(\pi_\alpha) A_\mathfrak{p}.$$

Cette dernière relation justifie encore l'appellation "discriminant". On a aussi la relation de divisibilité suivante :

$$\mathrm{Diff}_{B/A} \mid \pi'_\alpha(\alpha) B.$$

Dans le cas où $B = A[\alpha]$ on a exactement $\mathrm{Diff}_{B/A} = \pi'_\alpha(\alpha)B$.
En particulier, si le différent n'est pas principal, B n'admet pas de base de la forme $(1, \alpha, \ldots, \alpha^{n-1})$.

Démonstration. Soit $\mathfrak{p}$ ne divisant pas $(B : A[\alpha])$. On a donc $B_\mathfrak{p} = A[\alpha]_\mathfrak{p}$ et donc, par le théorème 5.22 :

$$(\mathrm{Diff}_{B/A})_\mathfrak{p} = \left(B_\mathfrak{p}^\circ\right)^{-1} = \left(A[\alpha]_\mathfrak{p}^\circ\right)^{-1} = \left(\frac{1}{\pi'_\alpha(\alpha)} A[\alpha]_\mathfrak{p}\right)^{-1} = \left(\frac{1}{\pi'_\alpha(\alpha)} B_\mathfrak{p}\right)^{-1} = \pi'_\alpha(\alpha) B_\mathfrak{p}.$$

On peut en déduire la formule pour le discriminant en passant à la norme, ou bien directement avec 2.15. De plus, comme $A[\alpha] \subseteq B$, on a :

$$\frac{1}{\pi'_\alpha(\alpha)} B \supseteq \frac{1}{\pi'_\alpha(\alpha)} A[\alpha] = A[\alpha]^\circ \supseteq B^\circ$$

donc en passant à l'inverse :

$$\mathrm{Diff}_{B/A} \mid \pi'_\alpha(\alpha) B.$$

□

On dispose de formules de transitivité pour le différent et le discriminant.

Théorème 5.33. *(Transitivité du discriminant relatif) Soit $A \subseteq B \subseteq C$ une tour d'extensions de Dedekind de corps de fractions $K \subseteq L \subseteq M$.*
On a alors :

$$\mathrm{Diff}_{C/A} = \mathrm{Diff}_{B/A} \cdot \mathrm{Diff}_{C/B} = (\mathrm{Diff}_{B/A} \cdot C) \cdot \mathrm{Diff}_{C/B}$$

et :

$$\mathcal{D}_{C/A} = \left\|\mathcal{D}_{C/B}\right\|_{B/A} \mathcal{D}_{B/A}^{[M:L]}.$$

Démonstration. Notons que l'application $\mathcal{F}(B)^\times \longrightarrow \mathcal{F}(C)^\times$ qui envoie I sur IC est un morphisme de groupes. Pour ne pas créer d'ambiguïté, on écrira $C^{\circ,A}$ pour le polaire de C vu comme un A-module et $C^{\circ,B}$ pour le polaire de C vu comme un B-module. La première formule est équivalente à :

$$C^{\circ,A} = B^{\circ,A} \cdot C^{\circ,B}$$

et c'est équivalent aux deux inclusions suivantes :

$$\begin{cases} C^{\circ,A} \supseteq B^{\circ,A} \cdot C^{\circ,B} \\ \left(B^{\circ,A}\right)^{-1} C^{\circ,A} \subseteq C^{\circ,B} \end{cases}$$

qui se vérifient formellement :

— Pour la première, si $\beta \in B^{\circ,A}$ et $\gamma \in C^{\circ,B}$, alors $\beta\gamma \in C^{\circ,A}$ car pour tout $c \in C$ on a :

$$\mathrm{Tr}_{M/K}(\beta\gamma c) = \mathrm{Tr}_{L/K}(\beta \cdot \mathrm{Tr}_{M/L}(\gamma c))$$

par la transitivité de la trace 2.10. Or $\mathrm{Tr}_{M/L}(\gamma c) \in B$ donc $\mathrm{Tr}_{L/K}(\beta \cdot \mathrm{Tr}_{M/L}(\gamma c)) \in A$.

— Voyons la seconde : soit $u \in \left(B^{\circ,A}\right)^{-1}$ et $\gamma \in C^{\circ,A}$. Il s'agit de voir que pour $c \in C$ quelconque on a :

$$\mathrm{Tr}_{M/L}(u\gamma c) \in B.$$

Or $\mathrm{Tr}_{M/L}(u\gamma c) = u\,\mathrm{Tr}_{M/L}(\gamma c)$ et donc il suffit de voir que $\mathrm{Tr}_{M/L}(\gamma c) \in B^{\circ,A}$, et c'est bien le cas car pour tout $b \in B$:

$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\gamma c)b) = \mathrm{Tr}_{M/K}(\gamma cb) \in A$$

car $cb \in C$.

L'égalité sur les discriminants s'obtient alors à partir de celle sur les différents en appliquant la norme relative de l'extension C/A et en utilisant la transitivité de la norme relative 5.14.

On peut aussi prouver la formule sur les discriminants en utilisant la transitivité du discriminant dans une tour d'extension de corps 2.16 : Il suffit de traiter le cas où A est un anneau de valuation discrète car tout est compatible à la localisation.
Dans ce cas B et C sont principaux et ont un nombre fini de premiers d'après 3.44.
En particulier C est un B-module libre et la formule se déduit alors de la proposition 5.27 sur le discriminant d'un réseau et de la formule 2.16 de transitivité du discriminant. □

5.6 Trace d'un idéal

On fixe B/A une extension de Dedekind de corps des fractions L/K. On définit la trace d'un idéal fractionnaire de B.

Définition 5.34. *Pour I un idéal fractionnaire de B, on pose :*

$$\mathrm{Tr}_{B/A}(I) = \mathrm{Tr}_{L/K}(I) = \{\mathrm{Tr}_{L/K}(x) \mid x \in I\}.$$

C'est clairement un A-module car la trace est A-linéaire, et il est de type fini car I est de type fini (sur B qui est de type fini sur A). C'est donc un idéal fractionnaire de A.

Proposition 5.35. *Si $I \neq 0$, sa trace est non nulle.*
De plus, la trace commute au pgcd *: si I et J sont deux idéaux fractionnaires de B, on a :*

$$\mathrm{Tr}_{B/A}(I+J) = \mathrm{Tr}_{B/A}(I) + \mathrm{Tr}_{B/A}(J).$$

Enfin, si X est un idéal fractionnaire de A et I un idéal fractionnaire de B, on a :

$$\mathrm{Tr}_{B/A}(XI) = X\,\mathrm{Tr}_{B/A}(I).$$

Démonstration. Si $I \neq 0$, on a $IK = L$ et puisque la trace est K-linéaire, si $\mathrm{Tr}_{B/A}(I) = 0$ alors $\mathrm{Tr}_{L/K}(L) = 0$, ce qui contredit la séparabilité de l'extension L/K. La trace commute clairement à la somme et la dernière égalité vient du fait que X est un A-module. □

Le lemme suivant sera utilisé dans la preuve du théorème de Dedekind 5.41.

Lemme 5.36. *Soit I un idéal fractionnaire non nul de B. On a l'équivalence suivante :*

$$I \supseteq \mathrm{Diff}_{B/A} \iff \mathrm{Tr}_{B/A}(I^{-1}) \subseteq A$$

ou encore, en langage arithmétique :

$$I \mid \mathrm{Diff}_{B/A} \iff A \mid \mathrm{Tr}_{B/A}(I^{-1}).$$

De plus, si $\mathfrak{p}$ est un premier de A tel que $I \mid \mathfrak{p}B$, alors $I \mid \mathrm{Diff}_{B/A}$ si et seulement si pour tout $x \in \mathfrak{p}I^{-1}$ on a :

$$\mathrm{Tr}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})}(\overline{x}) = 0.$$

Démonstration. I contient $\mathrm{Diff}_{B/A}$ si et seulement si $I^{-1} \subseteq B^\circ$, ce qui est équivalent à $\mathrm{Tr}_{B/A}(I^{-1}) \subseteq A$.
Supposons maintenant que $I \mid \mathfrak{p}B$, autrement dit que $\mathfrak{p} \subseteq I$. Ainsi :

$$\mathfrak{p}I^{-1} \subseteq B.$$

On a alors :

$$I \mid \mathrm{Diff}_{B/A} \iff \mathrm{Tr}_{B/A}(I^{-1}) \subseteq A \iff \mathrm{Tr}_{B/A}(\mathfrak{p}I^{-1}) \subseteq \mathfrak{p}$$

car $\mathrm{Tr}_{B/A}(\mathfrak{p}I^{-1}) = \mathfrak{p}\,\mathrm{Tr}_{B/A}(I^{-1})$ d'après 5.35. Ceci est équivalent à dire que pour tout $x \in \mathfrak{p}I^{-1}$, la trace $\mathrm{Tr}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})}(\overline{x})$ est nulle car on vérifie facilement que :

$$\overline{\mathrm{Tr}_{L/K}(x)} = \mathrm{Tr}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})}(\overline{x})$$

pour tout $x \in B$ (c'est clairement vrai si B est un A-module libre car dans ce cas une A-base de B induit une $A/\mathfrak{p}$-base de $B/\mathfrak{p}B$, et en général on peut localiser en $\mathfrak{p}$ pour se ramener à ce cas). □

On rappelle enfin une propriété sur les traces dont on laisse la preuve au lecteur (il s'agit simplement de choisir un supplémentaire de E dans F et de l'identifier à G).

Proposition 5.37. *Soit k un corps et :*

$$0 \longrightarrow E \longrightarrow F \longrightarrow G \longrightarrow 0$$

une suite exacte de k-espaces vectoriels de dimension finie. Soit f un endomorphisme de F tel que $f(E) \subseteq E$. Alors f induit un (unique) endomorphisme de G de telle sorte que le diagramme suivant commute :

$$\begin{array}{ccccc} E & \longrightarrow & F & \longrightarrow & G \\ {\scriptstyle f_E}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle f_G}\downarrow \\ E & \longrightarrow & F & \longrightarrow & G \end{array}$$

et on a :

$$\mathrm{Tr}(f) = \mathrm{Tr}(f_E) + \mathrm{Tr}(f_G).$$

5.7 Théorème de Dedekind

On fixe B/A une extension de Dedekind de corps des fractions L/K. Le théorème de Dedekind 5.41 permet de caractériser les premiers qui se ramifient dans l'extension B/A à l'aide du discriminant ou à l'aide du différent.
On introduit une hypothèse simplificatrice : la notion d'anneau de Dedekind localement parfait.
En théorie des nombres, les anneaux que l'on va considérer vérifieront souvent cette propriété. Il est possible de ne pas faire cette hypothèse au prix de compliquer légèrement la théorie générale.

Définition 5.38. *(Anneau de Dedekind localement parfait) On dit que A est localement parfait (resp. localement fini) si tous ses corps résiduels $A/\mathfrak{p}$ pour $\mathfrak{p}$ premier (non nul) sont des corps parfaits (resp. finis).*
Pour B/A une extension de Dedekind, cela entraîne que B est aussi localement parfait (resp. localement fini) car toute extension finie d'un corps parfait est un corps parfait.
Notons que si S est une partie multiplicative de A ne contenant pas 0, le localisé $S^{-1}A$ est encore localement parfait (resp. localement fini) : en effet tout premier de $S^{-1}A$ est de la forme $S^{-1}\mathfrak{p}$ avec $\mathfrak{p}$ premier de A tel que $\mathfrak{p} \cap S = \emptyset$ (ainsi tout élément de S est inversible modulo $\mathfrak{p}$) et :

$$S^{-1}A/S^{-1}\mathfrak{p} \cong A/\mathfrak{p} \otimes_A S^{-1}A \cong A/\mathfrak{p}$$

car $A/\mathfrak{p}$ est déjà un $S^{-1}A$-module.
Bien sûr si A est localement fini il est localement parfait, et en pratique, les anneaux que l'on rencontrera seront localement finis.

Remarque 5.39. Si A est fini sur $\mathbb{Z}$, A est localement fini (et ce sera le cas pour les anneaux d'entiers de corps de nombres) car $A/\mathfrak{p}$ est un corps fini pour tout premier $\mathfrak{p}$. En effet un corps finiment engendré comme groupe abélien est toujours fini : soit K

un tel corps, il ne contient pas $\mathbb{Q}$ car, $\mathbb{Z}$ étant noétherien, $\mathbb{Q}$ serait un groupe abélien de type fini.
Il est donc de caractéristique $p > 0$ et de type fini sur $\mathbb{F}_p$, donc de dimension finie sur $\mathbb{F}_p$: c'est un corps fini.
De même, si A est une k-algèbre avec k un corps de caractéristique nulle, $A/\mathfrak{p}$ est une extension de k de caractéristique nulle donc est parfait et donc A est localement parfait.

Dans cette partie, on suppose A localement parfait.

Lemme 5.40. *Soit $\mathfrak{q}$ un premier de B au dessus de $\mathfrak{p}$ un premier de A. On a alors la divisibilité suivante :*

$$\mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})-1} \mid \mathrm{Diff}_{B/A}.$$

En particulier si $\mathfrak{q} \mid \mathfrak{p}$ est ramifié (si $e(\mathfrak{q} \mid \mathfrak{p}) \geq 2$), alors $\mathfrak{q} \mid \mathrm{Diff}_{B/A}$.

Démonstration. On note $e = e(\mathfrak{q} \mid \mathfrak{p})$ et $\kappa = A/\mathfrak{p}$. D'après le lemme 5.36, puisque $\mathfrak{q}^{e-1} \mid \mathfrak{q}^e \mid \mathfrak{p}B$, cela revient à montrer que pour tout $x \in \mathfrak{p}\mathfrak{q}^{1-e}$, on a :

$$\mathrm{Tr}_{(B/\mathfrak{p}B)/(\kappa)(\overline{x})} = 0.$$

Soit donc $x \in \mathfrak{p}\mathfrak{q}^{1-e}$. Un tel x est divisible par tous les premiers au dessus de $\mathfrak{p}$ car ceux-ci divisent $\mathfrak{p}\mathfrak{q}^{1-e}$ (en effet $\mathfrak{q} \mid \mathfrak{p}\mathfrak{q}^{1-e}$ car $\mathfrak{q}^e \mid \mathfrak{p}B$ et si $\mathfrak{q}'$ est un premier au dessus de $\mathfrak{p}$ distinct de $\mathfrak{q}$, alors il divise aussi $\mathfrak{p}\mathfrak{q}^{1-e}$). On a donc :

$$x \in \sqrt{\mathfrak{p}B}$$

car x est dans l'intersection des premiers contenant $\mathfrak{p}B$. Ainsi $\overline{x}$ est nilpotent dans la κ-algèbre $B/\mathfrak{p}B$, et donc sa trace est nulle (un endomorphisme nilpotent a une trace nulle), comme souhaité. □

Théorème 5.41. *(Dedekind) Soit $\mathfrak{q}$ un premier de B au dessus de $\mathfrak{p}$ un premier de A. Notons $e = e(\mathfrak{q} \mid \mathfrak{p})$.*
Si $\mathfrak{p} \mid e$, (au sens où $\mathfrak{p} \mid e \cdot 1_A$), alors :

$$v_{\mathfrak{q}}(\mathrm{Diff}_{B/A}) \geq e$$

et sinon :

$$v_{\mathfrak{q}}(\mathrm{Diff}_{B/A}) = e - 1.$$

Démonstration. On note toujours $\kappa = A/\mathfrak{p}$. On a déjà montré dans le lemme 5.40 que cette valuation est au moins $e-1$. Il s'agit donc de montrer que $\mathrm{Diff}_{B/A}$ est divisible par $\mathfrak{q}^e$ si et seulement si $\mathfrak{p} \mid e$.
Notons :

$$\mathfrak{p}B = \mathfrak{q}^e I$$

de sorte que $I \subseteq B$ et $\mathfrak{p} \nmid I$. D'après le lemme 5.36 appliqué à l'idéal $\mathfrak{q}^e$ qui divise $\mathfrak{p}B$, la relation $\mathfrak{q}^e \mid \mathrm{Diff}_{B/A}$ est équivalente à ce que, pour tout $x \in I$, on ait :

$$\mathrm{Tr}_{(B/\mathfrak{p}B)/\kappa}(\overline{x}) = 0.$$

Par le théorème chinois, on a un isomorphisme canonique de κ-algèbres :

$$B/\mathfrak{p}B \cong B/\mathfrak{q}^e \times B/I$$

et pour tout $x \in B$, la multiplication par $\overline{x}$ agit "diagonalement par blocs" sur $B/\mathfrak{p}B = B/\mathfrak{q}^e \oplus B/I$ de sorte que :

$$\mathrm{Tr}_{(B/\mathfrak{p}B)/\kappa}(\overline{x}) = \mathrm{Tr}_{(B/\mathfrak{q}^e)/\kappa}(\overline{x}) + \mathrm{Tr}_{(B/I)/\kappa}(\overline{x})$$

et donc, pour $x \in I$:

$$\mathrm{Tr}_{(B/\mathfrak{p}B)/\kappa}(\overline{x}) = \mathrm{Tr}_{(B/\mathfrak{q}^e)/\kappa}(\overline{x}).$$

Ainsi on a :

$$\mathfrak{q}^e \mid \mathrm{Diff}_{B/A} \iff \forall x \in I \ \mathrm{Tr}_{(B/\mathfrak{q}^e)/\kappa}(\overline{x}) = 0.$$

Or on a $I + \mathfrak{q}^e = B$ donc la projection $I \longrightarrow B/\mathfrak{q}^e$ est surjective et cette condition est équivalente à :

$$\forall x \in B \ \mathrm{Tr}_{(B/\mathfrak{q}^e)/\kappa}(\overline{x}) = 0$$

autrement dit à :

$$\mathrm{Tr}_{(B/\mathfrak{q}^e)/\kappa} = 0.$$

Or on a une suite exacte de κ-espaces vectoriels et de B-modules :

$$0 \longrightarrow \mathfrak{q}^{e-1}/\mathfrak{q}^e \longrightarrow B/\mathfrak{q}^e \longrightarrow B/\mathfrak{q}^{e-1} \longrightarrow 0$$

et plus généralement pour tout $k \geq 0$:

$$0 \longrightarrow \mathfrak{q}^k/\mathfrak{q}^{k+1} \longrightarrow B/\mathfrak{q}^{k+1} \longrightarrow B/\mathfrak{q}^k \longrightarrow 0$$

ce qui permet d'écrire, en notant, pour $x \in B$ et pour tout B-module M, $\mu_x \mid M$ l'endomorphisme de multiplication par x sur M :

$$\mathrm{Tr}_{(B/\mathfrak{q}^e)/\kappa}(\overline{x}) = \sum_{k=0}^{e-1} \mathrm{Tr}(\mu_x \mid \mathfrak{q}^k/\mathfrak{q}^{k+1})$$

à l'aide de la proposition 5.37 appliquée plusieurs fois.
On choisit alors $\pi \in \mathfrak{q} \setminus \mathfrak{q}^2$ de sorte que le morphisme de multiplication par π^k induise un isomorphisme qui commute à la multiplication par x (voir la proposition3.58) :

$$\begin{array}{ccc} B/\mathfrak{q} & \xrightarrow[\sim]{\times\pi^k} & \mathfrak{q}^k/\mathfrak{q}^{k+1} \\ {\scriptstyle \mu_x}\downarrow & & \downarrow{\scriptstyle \mu_x} \\ B/\mathfrak{q} & \xrightarrow[\times\pi^k]{\sim} & \mathfrak{q}^k/\mathfrak{q}^{k+1} \end{array}$$

On a donc pour tout $x \in B$ et tout $k \geq 0$:

$$\mathrm{Tr}(\mu_x \mid \mathfrak{q}^k/\mathfrak{q}^{k+1}) = \mathrm{Tr}(\mu_x \mid B/\mathfrak{q}) = \mathrm{Tr}_{(B/\mathfrak{q})/\kappa}(\overline{x})$$

et donc en sommant :

$$\mathrm{Tr}_{(B/\mathfrak{q}^e)/\kappa}(\overline{x}) = e \cdot \mathrm{Tr}_{(B/\mathfrak{q})/\kappa}(\overline{x}).$$

Or A est localement parfait donc l'extension $(B/\mathfrak{q})/\kappa$ est séparable, ainsi $\mathrm{Tr}_{(B/\mathfrak{q})/\kappa} \neq 0$. Par intégrité de κ, on a donc :

$$\mathrm{Tr}_{(B/\mathfrak{q}^e)/\kappa} = 0 \iff e = 0 \text{ dans } \kappa \iff \mathfrak{p} \mid e$$

comme souhaité. □

On en déduit le corollaire suivant, très utile en pratique.

Corollaire 5.42. *Les premiers de A qui se ramifient dans B sont exactement les diviseurs du discriminant $\mathcal{D}_{B/A}$, et les premiers $\mathfrak{q}$ de B qui sont ramifiés (au sens où $e(\mathfrak{q} \mid \mathfrak{q} \cap A) \geq 2$) sont exactement les diviseurs du différent $\mathrm{Diff}_{B/A}$. En particulier cela ne concerne qu'un nombre fini de premiers (de A comme de B).*
De plus, si $\mathfrak{p}$ est un premier de A, on a toujours :

$$v_{\mathfrak{p}}(\mathcal{D}_{B/A}) \geq n - \sum_{\mathfrak{q} \supseteq \mathfrak{p}} f(\mathfrak{q} \mid \mathfrak{p})$$

avec $n = [L : K]$ et il y a égalité si et seulement si aucun des $e(\mathfrak{q} \mid \mathfrak{p})$ n'est divisible par $\mathfrak{p}$. Si tous sont divisibles par $\mathfrak{p}$, on a :

$$v_{\mathfrak{p}}(\mathcal{D}_{B/A}) \geq n.$$

Démonstration. Soit $\mathfrak{q}$ un premier de B au dessus de $\mathfrak{p}$ un premier de A. Si $e(\mathfrak{q} \mid \mathfrak{p}) \geq 2$, alors par le théorème de Dedekind on a $v_{\mathfrak{q}}(\mathrm{Diff}_{B/A}) \geq e(\mathfrak{q} \mid \mathfrak{p}) - 1 \geq 1$ donc $\mathfrak{q} \mid \mathrm{Diff}_{B/A}$. Si $e(\mathfrak{q} \mid \mathfrak{p}) = 1$, alors $\mathfrak{p} \nmid e(\mathfrak{q} \mid \mathfrak{p})$ donc par le théorème de Dedekind on a :

$$v_{\mathfrak{q}}(\mathrm{Diff}_{B/A}) = e(\mathfrak{q} \mid \mathfrak{p}) - 1 = 0$$

donc $\mathfrak{q}$ n'est pas ramifié.
Fixons ensuite $\mathfrak{p}$ un premier de A. On écrit :

$$\mathrm{Diff}_{B/A} = I \cdot \prod_{\mathfrak{q} \supseteq \mathfrak{p}} \mathfrak{q}^{w_{\mathfrak{q}}}$$

avec I premier à $\mathfrak{p}B$. On prend la norme :

$$\mathcal{D}_{B/A} = J \cdot \mathfrak{p}^t$$

avec J pemier à $\mathfrak{p}$ et :

$$t = \sum_{\mathfrak{q} \supseteq \mathfrak{p}} f(\mathfrak{q} \mid \mathfrak{p}) w_{\mathfrak{q}}.$$

Ainsi $\mathfrak{p} \mid \mathcal{D}_{B/A}$ si et seulement si $t \geq 1$, ce qui équivaut à dire que l'un des $\mathfrak{q}$ au dessus de $\mathfrak{p}$ divise le différent et donc par ce qui précède que $e(\mathfrak{q} \mid \mathfrak{p}) \geq 2$, donc $\mathfrak{p}$ divise le discriminant si et seulement si il se ramifie.
Par le théorème de Dedekind on a $w_{\mathfrak{q}} \geq e(\mathfrak{q} \mid \mathfrak{p}) - 1$ donc :

$$t \geq \sum_{\mathfrak{q} \supseteq \mathfrak{p}} f(\mathfrak{q} \mid \mathfrak{p})(e(\mathfrak{q} \mid \mathfrak{p}) - 1) = n - \sum_{\mathfrak{q} \supseteq \mathfrak{p}} f(\mathfrak{q} \mid \mathfrak{p})$$

par la formule des degrés 5.17. Il y a égalité si et seulement si pour tout $\mathfrak{q}$ au dessus de $\mathfrak{p}$ on a $w_\mathfrak{q} = e(\mathfrak{q} \mid \mathfrak{p}) - 1$, ce qui équivaut à dire, par le théorème de Dedekind, qu'aucun des $e(\mathfrak{q} \mid \mathfrak{p})$ n'est divisible par $\mathfrak{p}$.
Enfin, si tous les indices de ramification sont divisibles par $\mathfrak{p}$, alors tous les $w_\mathfrak{q}$ valent au moins $e(\mathfrak{q} \mid \mathfrak{p})$ et donc :

$$t \geq n.$$

□

Remarque 5.43. Dans le cas où l'extension L/K est galoisienne, on verra dans la suite que les indices $e(\mathfrak{q} \mid \mathfrak{p})$ et $f(\mathfrak{q} \mid \mathfrak{p})$ ne dépendent que de $\mathfrak{p}$ (voir 7.2). Dans ce cas, le corollaire 5.42 donne :

$$v_\mathfrak{p}(\mathcal{D}_{B/A}) = n - rf = \frac{n(e-1)}{e}$$

si $\mathfrak{p} \nmid e$ et :

$$v_\mathfrak{p}(\mathcal{D}_{B/A}) \geq n$$

si $\mathfrak{p} \mid e$, en notant r le nombre de premiers au dessus de $\mathfrak{p}$, e l'indice de ramification et f l'indice d'inertie des premiers au dessus de $\mathfrak{p}$.

5.8 Factorisation dans une extension donnée par un élément primitif

Dans la pratique, les extensions finies séparables sont souvent données par un élément primitif. On étudie ici le cas de A un anneau de Dedekind localement parfait de corps des fractions K (souvent on aura $A = \mathbb{Z}$) et d'une extension finie séparable $L = K(\alpha)$ de K, avec α entier sur A. On note alors $\pi_\alpha \in A[X]$ le polynôme minimal de α et B la clôture intégrale de A dans L.
On a toujours $A[\alpha] \subseteq B$ mais en général ce n'est pas une égalité.

Exemple 5.44. *Considérons $\alpha = \sqrt{5}$ et $L = \mathbb{Q}(\alpha)$. On montrera plus tard (théorème 6.7) que puisque $5 \equiv 1\ [4]$, on a en fait ici $B = \mathbb{Z}[\omega] = \mathbb{Z} \oplus \omega\mathbb{Z}$ avec :*

$$\omega = \frac{1+\sqrt{5}}{2}.$$

Notons que $\omega \notin \mathbb{Z}[\sqrt{5}]$.

Cependant, l'égalité est presque toujours vraie localement puisque $A[\alpha]$ est un quasi-réseau de L et en vertu du lemme 4.16, on a pour presque tout premier $\mathfrak{p}$ de A :

$$A[\alpha]_\mathfrak{p} = B_\mathfrak{p}.$$

Ceci permet, pour presque tout $\mathfrak{p}$, de faire comme si B était $A[\alpha]$ pour les questions de factorisation de $\mathfrak{p}B$ dans B. On illustre cette idée avec les deux théorèmes suivants.

Théorème 5.45. *Soit B/A une extension de Dedekind avec A localement parfait de corps des fractions L/K avec $L = K[\alpha]$ et $\alpha \in B$.*
Si $\mathfrak{p}$ ne divise pas $\mathrm{Disc}(\pi_\alpha)$ (autrement dit si π_α est séparable dans $(A/\mathfrak{p})[X]$), alors on a $B_\mathfrak{p} = A_\mathfrak{p}[\alpha]$ et $\mathfrak{p}$ n'est pas ramifié dans l'extension de Dedekind B/A.

Démonstration. D'après la remarque 5.26 :

$$\mathrm{Disc}_{B/A}(A[\alpha]) = (B : A[\alpha])^2 \cdot \mathrm{Disc}_{B/A}(B)$$

ce qui se réécrit, avec 2.15 :

$$\mathrm{Disc}(\pi_\alpha) \cdot A = (B : A[\alpha])^2 \cdot \mathcal{D}_{B/A}.$$

En particulier les idéaux (contenus dans A) $\mathcal{D}_{B/A}$ et $(B : A[\alpha])$ divisent le discriminant de π_α. Ainsi si $\mathfrak{p}$ ne divise pas le discriminant de π_α, il ne divise aucun de ces deux idéaux et donc d'une part $(B_\mathfrak{p} : A[\alpha]_\mathfrak{p}) = (B : A[\alpha])_\mathfrak{p} = A_\mathfrak{p}$ donc $B_\mathfrak{p} = A[\alpha]_\mathfrak{p}$ puisqu'on a une inclusion, et d'autre part $\mathfrak{p}$ n'est pas ramifié d'après le théorème de Dedekind 5.41. □

Le théorème 5.45 ne permet pas de trouver tous les premiers ramifiés, cependant il assure que tous les premiers ramifiés sont des diviseurs du discriminant de π_α, et cette information est utile en pratique car il est généralement facile de vérifier si π_α est séparable modulo $\mathfrak{p}$.
On va généraliser le théorème précédent 5.45 au cas d'une extension qui n'est pas nécessairement monogène. Pour cela, on a besoin du lemme suivant.

Lemme 5.46. *Soit B/A une extension de Dedekind et soient M, N deux B-modules et $f : M \longrightarrow N$ un morphisme de B-modules. Soit $\mathfrak{p}$ un premier de A. Si pour tout $\mathfrak{q}$ au dessus de $\mathfrak{p}$ on a que $M_\mathfrak{q} \longrightarrow N_\mathfrak{q}$ est un isomorphisme, alors $M_\mathfrak{p} \longrightarrow N_\mathfrak{p}$ est un isomorphisme.*

Démonstration. Il suffit d'utiliser 1.21 pour l'anneau $B_\mathfrak{p}$ en constatant que les idéaux premiers de $B_\mathfrak{p}$ sont exactement les $\mathfrak{q}_\mathfrak{p}$ avec $\mathfrak{q}$ au dessus de $\mathfrak{p}$ (utiliser 1.19) avec la partie multiplicative $S = A \setminus \mathfrak{p}$. □

Théorème 5.47. *Soit B/A une extension de Dedekind avec A localement parfait de corps des fractions L/K avec $L = K[\alpha_1, \ldots, \alpha_r]$ et les α_i dans A. Soit $\mathfrak{p}$ un premier de A. S'il existe $Q \in A[X]$ séparable modulo $\mathfrak{p}$ (i.e. son discriminant n'est pas divisible par $\mathfrak{p}$) qui annule les α_i, alors $\mathfrak{p}$ est non ramifié dans B et on a :*

$$B_\mathfrak{p} = A_\mathfrak{p}[\alpha_1, \ldots, \alpha_r].$$

Démonstration. On le montre par récurrence sur r. Le cas $r = 0$ est clair. Si on sait que c'est vrai dans le cas $r-1$, on peut poser A' la clôture intégrale dans $K' = K(\alpha_1, \ldots, \alpha_{r-1})$ de $A[\alpha_1, \ldots, \alpha_{r-1}]$, et on a par hypothèse de récurrence :

$$A'_\mathfrak{p} = A_\mathfrak{p}[\alpha_1, \ldots, \alpha_{r-1}].$$

Si $\alpha_r \in K'$, il n'y a rien à faire. Sinon, son polynôme minimal sur K' est séparable modulo tout $\mathfrak{q}$ premier de A' au dessus de $\mathfrak{p}$ et donc par le théorème précédent 5.45 :

$$B_\mathfrak{q} = A'[\alpha_r]_\mathfrak{q}.$$

Par le lemme précédent 5.46, on a donc :

$$B_\mathfrak{p} = A'[\alpha_r]_\mathfrak{p} = A_\mathfrak{p}[\alpha_1, \ldots, \alpha_r].$$

On montre aussi que $\mathfrak{p}$ est non ramifié dans B par ce même argument de récurrence en se basant sur le théorème 5.45. □

Le théorème suivant donne pour presque tout $\mathfrak{p}$ la factorisation de $\mathfrak{p}B$ dans B.

Théorème 5.48. *(Kummer, Dedekind) Soit B/A une extension de Dedekind avec A localement parfait de corps des fractions L/K avec $L = K[\alpha]$ et $\alpha \in B$.*
Soit $\mathfrak{p}$ un premier de A tel que $p \nmid (B : A[\alpha])$ (c'est en particulier le cas si π_α est séparable modulo $\mathfrak{p}$). On factorise π_α dans $(A/\mathfrak{p})[X]$:

$$\overline{\pi_\alpha} = \prod_{i=1}^{r} \overline{P_i}^{e_i}$$

avec $\overline{P_i} \in A/\mathfrak{p}[X]$ irréductible unitaire et $P_i \in A[X]$ unitaire.
Alors on a la factorisation en premiers suivante :

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

avec :

$$\mathfrak{q}_i = \mathfrak{p}B + P_i(\alpha)B.$$

De plus on a :

$$e(\mathfrak{q}_i \mid \mathfrak{p}) = e_i$$

et :

$$f(\mathfrak{q}_i \mid \mathfrak{p}) = \deg P_i.$$

Démonstration. On commence par le cas où $B = A[\alpha]$. On note k le corps $A/\mathfrak{p}$. On a :

$$\prod_i P_i^{e_i} \equiv \pi_\alpha[\mathfrak{p}A[X]].$$

Ainsi :

$$\mathfrak{p}B = \mathfrak{p}B + \pi_\alpha(\alpha)B = \mathfrak{p}B + \prod_i (P_i(\alpha)B)^{e_i} \supseteq \prod_i \mathfrak{q}_i^{e_i}$$

avec $\mathfrak{q}_i = \mathfrak{p}B + P_i(\alpha)B$. Autrement dit, on a établi la relation de divisibilité suivante :

$$\mathfrak{p}B \mid \prod_i \mathfrak{q}_i^{e_i}.$$

Notons que chaque $\mathfrak{q}_i$ est premier, au dessus de $\mathfrak{p}$, et que $f(\mathfrak{q}_i \mid \mathfrak{p}) = \deg P_i$ puisque :

$$B/\mathfrak{q}_i = A[\alpha]/(\mathfrak{p}A[\alpha] + P_i(\alpha)A[\alpha]) \cong k[X]/(\overline{\pi_\alpha}, \overline{P_i}) = k[X]/(\overline{P_i})$$

est une extension de degré $\deg P_i$ de k. De plus, les $\mathfrak{q}_i$ sont distincts : cela revient à dire que les $\overline{P_i(\alpha)}$ sont distincts dans $B/\mathfrak{p}B$, autrement dit que les $\overline{P_i}$ sont distincts dans :

$$A[X]/(\pi_\alpha A[X] + \mathfrak{p}A[X]) \cong k[X]/\left(\prod_i \overline{P_i}^{e_i}\right) \cong \prod_i k[X]/(\overline{P_i}^{e_i})$$

ce qui est clair en regardant les coordonnées : la seule coordonnée nilpotente de $\overline{P_i}$ dans ce quotient est la i-ème.
On peut alors écrire :

$$\mathfrak{p}B = \prod_i \mathfrak{q}_i^{e_i'}$$

avec $e_i' = e(\mathfrak{q}_i \mid \mathfrak{p}_i)$ et on a $e_i' \leq e_i$ d'après la relation de divisibilité établie plus tôt. Rappelons qu'on a :

$$\|\mathfrak{p}B\|_{B/A} = \mathfrak{p}^d$$

avec $d = [L : K] = \deg \pi_\alpha$ d'après le théorème 5.17. De plus on a :

$$\left\| \prod_i \mathfrak{q}_i^{e_i} \right\| = \prod_i \mathfrak{p}^{f_i e_i} = \mathfrak{p}^{\sum_i e_i \deg P_i} = \mathfrak{p}^d = \|\mathfrak{p}B\|$$

ce qui impose $e_i = e_i'$ pour tout i et donc :

$$\mathfrak{p}B = \prod_i \mathfrak{q}_i^{e_i}.$$

Le cas général s'obtient par localisation : si $\mathfrak{p} \nmid (B : A[\alpha])$, alors $B_\mathfrak{p} = A_\mathfrak{p}[\alpha]$ et ce qui précède s'applique :

$$\mathfrak{p}B_\mathfrak{p} = \prod_i (\mathfrak{q}_i)_\mathfrak{p}^{e_i}$$

et donc $\mathfrak{p}B = \prod_i \mathfrak{q}_i^{e_i}$ car ce sont deux idéaux de B contenant $\mathfrak{p}$ qui ont la même localisation par $\mathfrak{p}$.
(En effet, si I et J sont deux idéaux de B contenant $\mathfrak{p}$ et si $I_\mathfrak{p} \subseteq J_\mathfrak{p}$, alors pour tout $x \in I$ on a $x \in J_\mathfrak{p}$ donc il existe $s \in A \setminus \mathfrak{p}$ tel que $sx \in J$, or s est inversible modulo $\mathfrak{p}$ donc il existe $t \in A$ et $p \in \mathfrak{p}$ tels que $st = 1 + p$ et donc $xst = x + xp$, de sorte que $x = xst - xp \in J + \mathfrak{p}B \subseteq J$ donc $I \subseteq J$.) □

5.9 Compositum d'extensions de Dedekind

Le théorème suivant permet sous certaines hypothèses de déterminer la clôture intégrale d'un anneau de Dedekind dans un compositum de deux extensions du corps des fractions.

Théorème 5.49. *Soit A un anneau de Dedekind de corps des fractions K, soit Ω un corps algébriquement clos contenant K et soient E et F deux sous-corps de Ω contenant K. On suppose les extensions E/K et F/K finies et séparables. On suppose aussi que E et F sont complémentaires (voir 2.21) et que $E \cap F = K$, de sorte que :*

$$[EF : K] = [E : K] \cdot [F : K].$$

Notons B, C et D les clôtures intégrales de A dans E, F et EF (notons que EF est encore séparable sur K).
On a alors :

$$BC \subseteq D \subseteq (\mathcal{D}_{B/A} + \mathcal{D}_{C/A})^{-1} BC.$$

En particulier, si les discriminants de B et C sur A sont premiers entre eux, alors :

$$D = BC.$$

De plus, si $D = BC$, alors :

$$\mathcal{D}_{D/A} = \mathcal{D}_{B/A}^{[F:K]}\mathcal{D}_{C/A}^{[E:K]}.$$

Démonstration. On note $\overline{A}$ la clôture intégrale de A dans Ω. Il est clair que $BC \subseteq D$. Puisque l'énoncé est compatible à la localisation, on peut supposer que A est principal (une autre méthode pour prouver cet énoncé est d'utiliser 5.29, dans les deux cas on se ramène à considérer des réseaux plutôt que des quasi-réseaux). Il existe alors $\underline{e}$ une A-base de B, et $\underline{f}$ une A-base de C. Par complémentarité de E et F et puisque $E \cap F = K$, on a un isomorphisme de K-algèbres canonique :

$$EF \cong E \otimes_K F$$

donc $(e_i f_j)_{i,j}$ est une K-base de EF et :

$$\mathrm{Hom}_K(EF, \Omega) \cong \mathrm{Hom}_K(E, \Omega) \times \mathrm{Hom}_K(F, \Omega) \quad (*)$$

par propriété universelle du produit tensoriel de K-algèbres.
Soit $d \in D$. On écrit d dans la E-base $\underline{f}$ de EF :

$$d = \sum_i x_i f_i$$

avec $x_i \in E$. Pour chaque $\sigma \in \mathrm{Hom}_K(F, \Omega)$, d'après l'isomorphisme $(*)$, on a $\mathrm{id}_E \otimes \sigma \in \mathrm{Hom}_K(EF, \Omega)$. On a alors :

$$(\mathrm{id} \otimes \sigma)(d) = \sum_i x_i \sigma(f_i)$$

et ce système s'inverse pour donner :

$$x_i = \sum_{\sigma \in \mathrm{Hom}_K(F,\Omega)} u_{i,\sigma} \cdot (\mathrm{id} \otimes \sigma)(d)$$

avec, par la formule de Cramer :

$$u_{i,\sigma} \in \frac{1}{\det(\sigma(f_i))_{i,\sigma}} \overline{A}$$

et puisque $(\mathrm{id} \otimes \sigma)(d) \in \overline{A}$, on obtient :

$$x_i \in \frac{1}{\det(\sigma(f_i))_{i,\sigma}} \overline{A}.$$

Ainsi, puisque $\det(\sigma(f_i))_{i,\sigma}^2 = D_{F/K}(\underline{f})$:

$$D_{F/K}(\underline{f}) \cdot x_i \in \det(\sigma(f_i))_{i,\sigma} \overline{A} \subseteq \overline{A}.$$

Cet élément est donc dans $E \cap \overline{A} = B$. On a donc :

$$D_{F/K}(\underline{f}) \cdot d \in BC$$

et comme $\mathcal{D}_{C/A} = D_{F/K}(\underline{f})A$:

$$d\mathcal{D}_{C/A} \subseteq BC.$$

Par symétrie, on a aussi :

$$d\mathcal{D}_{B/A} \subseteq BC$$

et donc finalement :

$$d \in (\mathcal{D}_{B/A} + \mathcal{D}_{C/A})^{-1} BC$$

comme souhaité.
Supposons $D = BC$ et montrons :

$$\mathcal{D}_{D/A} = \mathcal{D}_{B/A}^{[F:K]} \mathcal{D}_{C/A}^{[E:K]}.$$

On peut encore supposer A principal puisque c'est un énoncé local. On se donne $\underline{e}$ une A-base de B et $\underline{f}$ une A-base de C. Ainsi $(e_i f_j)_{i,j}$ est une A-base de $BC = D$ et on a, par 2.16 :

$$\begin{aligned} D_{EF/K}((e_i f_j)_{i,j}) &= N_{E/K}\left(D_{EF/E}(\underline{f})\right) \cdot D_{E/K}(\underline{e})^{[EF:E]} = N_{E/K}\left(D_{F/K}(\underline{f})\right) \cdot D_{E/K}(\underline{e})^{[F:K]} \\ &= D_{F/K}(\underline{f})^{[E:K]} \cdot D_{E/K}(\underline{e})^{[F:K]} \end{aligned}$$

car les matrices qui donnent $D_{F/K}(\underline{f})$ et $D_{EF/E}(\underline{f})$ sont les mêmes donc ont le même déterminant. □

Chapitre 6

L'anneau des entiers d'un corps de nombres

> Au reste, tant les vraies racines que les fausses ne sont pas toujours réelles, mais quelquefois seulement imaginaires, c'est-à-dire qu'on peut bien toujours en imaginer autant que j'ai dit en chaque équation, mais qu'il n'y a quelquefois aucune quantité qui corresponde à celles qu'on imagine.
>
> René Descartes, La Géométrie

6.1 Généralités

Définition 6.1. *Un corps de nombres est une extension finie de $\mathbb{Q}$. On considérera toujours qu'un corps de nombres est contenu dans $\mathbb{C}$, bien que cela nécessite un choix. Si K est un corps de nombres, on note $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K$ son anneau des entiers : ici $\overline{\mathbb{Z}}$ désigne l'anneau des entiers algébriques de $\mathbb{C}$. Ainsi $\mathcal{O}_K$ est la clôture intégrale de $\mathbb{Z}$ dans K et puisque l'extension $K/\mathbb{Q}$ est finie et séparable et $\mathbb{Z}$ est un anneau de Dedekind, $\mathcal{O}_K/\mathbb{Z}$ est une extension de Dedekind.*
En particulier $\mathcal{O}_K$ est un $\mathbb{Z}$-réseau de K et donc un groupe abélien libre de rang d, ce qui n'était pas du tout évident a priori. On appelle base intégrale de K une $\mathbb{Z}$-base de $\mathcal{O}_K$. C'est en particulier une base de K.
Si $\mathfrak{p}$ est un premier de $\mathcal{O}_K$, il est au dessus d'un idéal premier non nul de $\mathbb{Z}$ qui est donc de la forme $p\mathbb{Z}$ avec p un nombre premier. Pour simplifier les notations, on écrira donc $e(\mathfrak{p} \mid p)$ et $f(\mathfrak{p} \mid p)$ plutôt que $e(\mathfrak{p} \mid p\mathbb{Z})$ et $f(\mathfrak{p} \mid p\mathbb{Z})$.
Le groupe $\mathcal{F}(\mathbb{Z})^\times$ est isomorphe à $\mathbb{Q}^\times/\{\pm 1\} \cong \mathbb{Q}_+^\times$ car $\mathbb{Z}$ est principal.
On pourra donc identifier les idéaux fractionnaires non nuls de $\mathbb{Z}$ à des rationnels strictement positifs quand le contexte est clair.

Remarque 6.2. Toutes les extensions de Dedekind de $\mathbb{Z}$ sont d'ailleurs de cette forme, et on pourrait renommer ce chapitre "extensions de Dedekind de $\mathbb{Z}$", mais c'est bien moins concret.

On rappelle qu'en vertu du théorème 4.15, on a pour tout idéal non nul I contenu dans $\mathcal{O}_K$:

$$\|I\| = [\mathcal{O}_K : I]\mathbb{Z}$$

que l'on notera simplement, sous l'identification mentionnée plus haut $\|I\| = [\mathcal{O}_K : I]$.

Définition 6.3. *On définit le discriminant de K, noté* $\mathrm{Disc}(K)$ *comme :*

$$D_{K/\mathbb{Q}}(\underline{b})$$

pour une base intégrale $\underline{b}$ quelconque de K. Cet entier ne dépend pas de la base choisie puisque en changeant de base le discriminant est multiplié par le carré du déterminant d'une matrice de $\mathrm{GL}_d(\mathbb{Z})$*, c'est à dire par* 1.
On a bien entendu :

$$\mathrm{Disc}(K) \cdot \mathbb{Z} = \mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}$$

d'après 5.27. Cependant $\mathrm{Disc}(K)$ *contient plus d'information puisqu'il possède un signe, que l'on pourra déterminer par des méthodes géométriques (voir 6.17).*

Proposition 6.4. *(Critère de Stickelberger) Soit K un corps de nombres de degré $n \geq 1$ et $x_1, \ldots, x_n \in \mathcal{O}_K$. Alors on a :*

$$D_{K/\mathbb{Q}}(\underline{x}) \equiv 0 \text{ ou } 1 \ [4]$$

et en particulier :

$$\mathrm{Disc}(K) \equiv 0 \text{ ou } 1 \ [4].$$

Démonstration. Sans perte de généralité on peut supposer $n \geq 2$. On choisit L une extension finie de K normale sur $\mathbb{Q}$, de groupe de Galois $G = \mathrm{Gal}(L/\mathbb{Q})$. On numérote $\sigma_1, \ldots, \sigma_n$ les plongements de K dans $\mathbb{C}$.
Par 2.14 et par la formule explicite du déterminant, on a :

$$D_{K/\mathbb{Q}}(\underline{x}) = \left(\sum_{\alpha \in \mathfrak{S}_n} \varepsilon(\alpha) \prod_{i=1}^{n} \sigma_{\alpha(i)}(x_i) \right)^2 = (A - B)^2 = (A + B)^2 - 4AB$$

avec :

$$A = \sum_{\alpha \in \mathfrak{A}_n} \prod_{i=1}^{n} \sigma_{\alpha(i)}(x_i)$$

et :

$$B = \sum_{\alpha \in \mathfrak{S}_n \setminus \mathfrak{A}_n} \prod_{i=1}^{n} \sigma_{\alpha(i)}(x_i)$$

où $\mathfrak{A}_n$ est le groupe des permutations paires. Pour tout $g \in G$, on a $gA = A$ et $gB = B$ ou $gA = B$ et $gB = A$ selon la signature de la permutation $\sigma \mapsto g \circ \sigma$ de l'ensemble $\{\sigma_1, \ldots, \sigma_n\}$.
Ainsi :

$$g(A + B) = A + B$$

et :

$$g(AB) = AB$$

donc $A + B$ et AB sont rationnels. De plus ce sont des entiers algébriques, et $\overline{\mathbb{Z}}$ est intégralement clos donc $A+B$ et AB sont des entiers. Ainsi $(A+B)^2$ est un carré parfait donc congru à 0 ou 1 modulo 4. Ceci conclut la preuve. □

6.2 Corps quadratiques

L'exemple le plus simple de corps de nombres, après $\mathbb{Q}$, est celui des *corps quadratiques*, c'est à dire des extensions de degré 2 de $\mathbb{Q}$. Dans ce cas là, on peut donner une base intégrale explicitement. Dans ce qui suit, si $d \in \mathbb{Z}$, $\sqrt{d}$ est une racine carrée quelconque de d dans $\mathbb{C}$.

Proposition 6.5. *Les corps quadratiques sont les $\mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteur carré (i.e. sans diviseur de la forme p^2 avec p premier). De plus ces corps sont deux à deux distincts et deux à deux non-isomorphes.*

Démonstration. Ces corps $\mathbb{Q}(\sqrt{d})$ sont clairement des corps quadratiques car $\sqrt{d}$ est un entier algébrique de degré au plus 2 qui n'est pas un entier, puisque d est sans facteur carré et différent de 0 et 1, donc il est de degré exactement 2 car $\mathbb{Z}$ est intégralement clos. Soit K un corps quadratique. En invoquant le théorème de l'élément primitif, ou plus simplement en prenant un élément α de $K \setminus \mathbb{Q}$, on a :

$$K = \mathbb{Q}(\alpha)$$

avec α algébrique de degré 2. En mettant le polynôme minimal de α sous forme canonique, on obtient :

$$a(\alpha + b)^2 + c = 0$$

avec $a, b, c \in \mathbb{Z}$ et $a \neq 0$. On a ainsi $(a\alpha + ab)^2 = -ac$ donc :

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}(a\alpha + ab) = \mathbb{Q}(\sqrt{-ac})$$

Ainsi K est de la forme $\mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z} \setminus \{0,1\}$ et on peut clairement supposer d sans facteur carré puisque pour tout p premier on a $\mathbb{Q}(\sqrt{p^2 d}) = \mathbb{Q}(\sqrt{d})$.
Voyons que si d, d' sont deux tels entiers, les corps $\mathbb{Q}(\sqrt{d})$ et $\mathbb{Q}(\sqrt{d'})$ sont distincts. Sinon, on pourrait écrire $\sqrt{d} = a + b\sqrt{d'}$ avec $a, b \in \mathbb{Q}$ et donc :

$$d = a^2 + d'b^2 + 2ab\sqrt{d'}$$

ce qui impose $ab = 0$. Ainsi, ou bien $\sqrt{d} = a$, ce qui est impossible, ou bien $a = 0$ et :

$$d = d'b^2$$

ce qui contredit le fait que d est sans facteur carré (à moins que $b = 0$ ou $b = 1$ mais c'est impossible).
Puisque ces corps sont galoisiens et distincts, ils ne sont pas isomorphes (un isomorphisme entre deux corps de nombres galoisiens $K_1 \longrightarrow K_2$ a son image contenue dans K_1 car l'extension $K_1/\mathbb{Q}$ est normale). □

On fixe à présent $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique, avec $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteur carré. On va déterminer une base intégrale de $\mathcal{O}_K$. Procédons par analyse-synthèse. Soit $z \in \mathcal{O}_K$, on écrit $z = a + \sqrt{d}b$ avec $a, b \in \mathbb{Q}$. La trace de z est un entier, donc :

$$2a \in \mathbb{Z}$$

De même, la norme de z est un entier donc :

$$a^2 - db^2 \in \mathbb{Z}$$

De même, $a - \sqrt{d}b$ est aussi un entier algébrique car $z \in \overline{\mathbb{Z}}$ et $\sqrt{d} \in \overline{\mathbb{Z}}$ donc $\sqrt{d}(z - (a - \sqrt{d}b)) \in \overline{\mathbb{Z}}$, c'est à dire :

$$2db \in \mathbb{Z}$$

puisque c'est un élément de $\overline{\mathbb{Z}} \cap \mathbb{Q}$. Ces contraintes arithmétiques permettent la disjonction de cas suivante :

Lemme 6.6. *Si a est entier, alors b est entier.*
Si $a \in \mathbb{Z} + 1/2$ alors $b \in \mathbb{Z} + 1/2$ et $d \equiv 1$ [4].

Démonstration. Supposons a entier. Puisque $a^2 - db^2$ est entier, db^2 est entier. Ainsi pour tout nombre premier p, on a :

$$v_p(d) + 2v_p(b) \geq 0$$

donc $v_p(b) \geq -v_p(d)/2 \geq -1/2$ car d est *sans facteur carré*. Ainsi $v_p(b) \geq 0$, et ce pour tout p premier, donc b est entier.
Supposons maintenant $a = k + 1/2$ avec k entier. Ainsi $a^2 - db^2 = k^2 + k + 1/4 - db^2$ donc :

$$db^2 \in \mathbb{Z} + 1/4$$

Pour p premier *différent de* 2, on a donc :

$$v_p(d) + 2v_p(b) \geq 0$$

et comme précedemment $v_p(b) \geq 0$. Enfin on a :

$$v_2(d) + 2v_d(b) = -2$$

donc $v_2(d)$ est pair, et puisque d est sans facteur carré, $v_2(d) = 0$. On a donc $v_2(b) = -1$. Au total :

$$b \in \mathbb{Z} + 1/2$$

Mais $4(a^2 - db^2) = (2a)^2 - d(2b)^2$ est un multiple de 4, et de plus $2a \equiv 1$ [2], donc $(2a)^2 \equiv 1$ [4], donc finalement $d(2b)^2 \equiv 1$ [4]. Mais $(2b)^2 \equiv 1$ [4] donc $d \equiv 1$ [4].
□

Ce lemme permet de donner une base intégrale de $\mathcal{O}_K$ selon si d est congru à 1 modulo 4 ou non.

Théorème 6.7. *L'anneau des entiers de $K = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteur carré est donné par :*

$$\mathcal{O}_K = \mathbb{Z}[\omega] = \mathbb{Z} \oplus \mathbb{Z}\omega$$

avec :

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & si\ d \equiv 1\ [4] \\ \sqrt{d} & sinon \end{cases}$$

Démonstration. Si d n'est pas congru à 1 modulo 4, le lemme 6.6 montre que :

$$\mathcal{O}_K \subseteq \mathbb{Z} \oplus \sqrt{d}\mathbb{Z}$$

L'autre inclusion est claire car $\sqrt{d} \in \mathcal{O}_K$.
Si d est congru à 1 modulo 4, alors $\omega = \frac{1+\sqrt{d}}{2}$ est un élément de $\mathcal{O}_K$ puisqu'il vérifie :

$$\omega^2 = \omega + \frac{d-1}{4}$$

On a donc $\mathbb{Z}[\omega] = \mathbb{Z} \oplus \mathbb{Z}\omega \subseteq \mathcal{O}_K$. Réciproquement, si $z = a + \sqrt{d}b = a - b + 2b\omega \in \mathcal{O}_K$, ou bien a est entier et par le lemme 6.6 b est aussi entier donc $z \in \mathbb{Z} \oplus \mathbb{Z}\omega$, ou bien $a \in \mathbb{Z} + 1/2$ et par le lemme 6.6 b est aussi dans $\mathbb{Z} + 1/2$ donc $a - b \in \mathbb{Z}$ et $2b \in \mathbb{Z}$, donc encore une fois $z \in \mathbb{Z} \oplus \mathbb{Z}\omega$. □

Remarque 6.8. Dans le cas des corps quadratiques, l'anneau des entiers est donc toujours engendré par un seul élément. Il est naturel de se demander s'il existe une forme du théorème de l'élément primitif pour les anneaux d'entiers de corps de nombres, cependant c'est faux en général : $\mathcal{O}_K$ n'est pas toujours engendé par un seul élément.

Proposition 6.9. *Le discriminant du corps quadratique $K = \mathbb{Q}(\sqrt{d})$ est donné par :*

$$\mathrm{Disc}(K) = \begin{cases} d & si\ d \equiv 1\ [4] \\ 4d & sinon \end{cases}$$

L'idéal différent $\mathrm{Diff}(K) = \mathrm{Diff}_{\mathcal{O}_K/\mathbb{Z}}$ *de K est :*

$$\mathrm{Diff}(K) = \begin{cases} \sqrt{d} \cdot \mathcal{O}_K & si\ d \equiv 1\ [4] \\ 2\sqrt{d} \cdot \mathcal{O}_K & sinon \end{cases}.$$

Démonstration. On a $\mathcal{O}_K = \mathbb{Z}[\omega]$ avec ω comme dans le théorème 6.7.
Si $d \equiv 1\ [4]$, le polynôme minimal de $\omega = \frac{1+\sqrt{d}}{2}$ est :

$$\pi_\omega = X^2 - X + \frac{1-d}{4}$$

de sorte que :

$$\pi'_\omega(\omega) = 2\omega - 1 = \sqrt{d}.$$

Ainsi, par le théorème 2.15 et le théorème 5.32, on a dans ce cas :

$$\mathrm{Disc}(K) = (-1)^{\binom{2}{2}} N_{K/\mathbb{Q}}(\sqrt{d}) = d$$

et :

$$\mathrm{Diff}(K) = \sqrt{d} \cdot \mathcal{O}_K.$$

Si d est congru à 2 ou 3 modulo 4, alors $\omega = \sqrt{d}$ et $\pi'_\omega(\omega) = (X^2 - d)'(\omega) = 2\sqrt{d}$ et donc $\mathrm{Disc}(K) = 4d$ et $\mathrm{Diff}(K) = 2\sqrt{d} \cdot \mathcal{O}_K$.
On peut aussi calculer le discriminant de façon directe avec la proposition 2.14. □

6.3 Algèbre réelle d'un corps de nombres

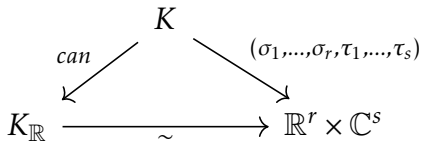
On fixe K un corps de nombres de degré d et on note Σ l'ensemble des plongements de K dans $\mathbb{C}$. Parmi ces plongements, certains sont *réels* (au sens où leur image est contenue dans $\mathbb{R}$, on les note $\sigma_1, \ldots, \sigma_r$, et les autres, non réels, vont par deux : si τ est un plongement non réel, $\overline{\tau}$ (qui à x associe le conjugué de $\tau(x)$) est un plongement non réel différent de τ. On note alors $\tau_1, \overline{\tau_1}, \ldots, \tau_s\overline{\tau_s}$ ces plongements non réels. Ainsi on a :

$$d = r + 2s$$

On conserve ces notations dans la suite.

Définition 6.10. *On associe à K l'algèbre réelle $K \otimes_{\mathbb{Q}} \mathbb{R}$, notée dans la suite $K_{\mathbb{R}}$. C'est donc un espace vectoriel de dimension d sur $\mathbb{R}$. D'après 4.7, $\mathcal{O}_K$ est encore un réseau du $\mathbb{R}$-espace vectoriel $K_{\mathbb{R}}$. On préfèrera travailler dans cet espace pour les considérations géométriques et pour pouvoir utiliser la théorie de la mesure.*

Proposition 6.11. *Une fois la numérotation $\sigma_1, \ldots, \sigma_r, \tau_1, \ldots, \tau_s$ choisie, on a un isomorphisme de $\mathbb{R}$-algèbres canonique entre $K_{\mathbb{R}}$ et $\mathbb{R}^r \times \mathbb{C}^s$ qui fait commuter le diagramme suivant :*



Démonstration. Par le théorème de l'élément primitif, on peut supposer que $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/(\pi)$ avec $\alpha \in \mathbb{C}$, $\pi \in \mathbb{Q}[X]$ unitaire et $\pi(\alpha) = 0$. Le polynôme $\pi = \prod_{f \in \Sigma}(X - f(\alpha))$ se factorise de la façon suivante dans $\mathbb{R}[X]$:

$$\pi = \prod_i (X - \sigma_i(\alpha)) \prod_j (X - 2\,\mathrm{Re}(\tau_j(\alpha)) + \left|\tau_j(\alpha)\right|^2)$$

On a donc :

$$K_{\mathbb{R}} \cong \mathbb{R}[X]/(\pi) \cong \prod_i \mathbb{R}[X]/(X - \sigma_i(\alpha)) \times \prod_j \mathbb{R}[X]/(X - 2\,\mathrm{Re}(\tau_j(\alpha)) + \left|\tau_j(\alpha)\right|^2)$$

par le théorème des restes chinois (les facteurs étant premiers entre eux deux à deux). Or l'application d'évaluation en $\sigma_i(\alpha)$, $\mathbb{R}[X]/(X - \sigma_i(\alpha)) \longrightarrow \mathbb{R}$ est un isomorphisme et de même l'application $P \mapsto P(\tau_j(\alpha))$, $\mathbb{R}[X]/(X - 2\,\mathrm{Re}(\tau_j(\alpha)) + \left|\tau_j(\alpha)\right|^2) \longrightarrow \mathbb{C}$ est un isomorphisme. Ainsi on peut identifier $K_{\mathbb{R}}$ et $\mathbb{R}^r \times \mathbb{C}^s$ et on vérifie immédiatement que le diagramme de la proposition commute.

□

Remarque 6.12. Grâce à la proposition 6.11, on identifiera $K_{\mathbb{R}}$ et $\mathbb{R}^r \times \mathbb{C}^s$ en identifiant l'inclusion canonique avec le morphisme $\iota = (\sigma_1, \ldots, \sigma_r, \tau_1, \ldots, \tau_s)$.

On peut définir la norme et la trace sur la $\mathbb{R}$-algèbre de dimension finie $K_{\mathbb{R}}$ exactement comme pour les extensions de corps en considèrant la norme et la trace de l'endomorphisme de multiplication. Avec le plongement $K \longrightarrow K_{\mathbb{R}}$, les applications norme et trace prolongent les applications norme et trace de K sur $\mathbb{Q}$. On a alors :

Proposition 6.13. *Soit $a = (x_1, \ldots, x_r, y_1, \ldots, y_s) \in K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$. On a :*

$$N(a) = \prod_i x_i \times \prod_j y_j \overline{y_j}$$

et :

$$\mathrm{Tr}(a) = \sum_i x_i + \sum_j (y_j + \overline{y_j})$$

Démonstration. La multiplication par a se fait coordonnée par coordonnée, donc sa matrice est diagonale et le résultat en découle immédiatement. □

6.4 Borne de Minkowski

Soit K un corps de nombres de degré d, on rappelle que $K \xrightarrow{\iota} K_{\mathbb{R}}$ est l'application $(\sigma_1, \ldots, \sigma_r, \tau_1, \ldots, \tau_s)$ dans les notations de 6.3.

Théorème 6.14. *(Existence d'une borne de Minkowski) Il existe une constante $M > 0$ dépendant seulement de K telle que tout idéal non nul I de $\mathcal{O}_K$ contient un élément a vérifiant :*

$$0 < |N(a)| \leq M \|I\|$$

Une telle constante s'appelle une borne de Minkowski de K.

Démonstration. On munit $K_{\mathbb{R}}$ d'une norme $|\bullet|$ et d'une mesure de Lebesgue μ et on note $\overline{B}$ la boule unité fermée de $K_{\mathbb{R}}$ pour cette norme.
Soit I un idéal non nul de $\mathcal{O}_K$. D'après la proposition 5.3, $\iota(I)$ est un sous-réseau de $\iota(\mathcal{O}_K)$ et on a :

$$\mathrm{covol}(\iota(I)) = \mathrm{covol}(\iota(\mathcal{O}_K)) \|I\|$$

Par le *théorème de Minkowski* 4.36, il existe $a \in I$ *non nul* tel que :

$$|a| \leq 2 \left(\frac{\mathrm{covol}(\iota(I))}{\mu(\overline{B})} \right)^{1/d} = 2 \left(\frac{\mathrm{covol}(\iota(\mathcal{O}_K))}{\mu(\overline{B})} \right)^{1/d} \|I\|^{1/d}$$

Or $|N|$ est continue sur $\overline{B}$ qui est compacte, donc atteint son maximum S sur $\overline{B}$, et donc on a :

$$|N(a)| \leq S\,|a|^d \leq 2^d S \frac{\mathrm{covol}(\iota(\mathcal{O}_K))}{\mu(\overline{B})} \|I\|$$

ce qui permet de poser :

$$M = 2^d S \frac{\mathrm{covol}(\iota(\mathcal{O}_K))}{\mu(\overline{B})}.$$

□

Une propriété fondamentale de la borne de Minkowski est la suivante :

Théorème 6.15. *Chaque élément de* $\mathrm{Cl}(\mathcal{O}_K)$ *contient un idéal de* $\mathcal{O}_K$ *de norme inférieure ou égale à* M*. Autrement dit, en notant* $\pi : \mathcal{F}(\mathcal{O}_K) \longrightarrow \mathrm{Cl}(\mathcal{O}_K)$ *le morphisme surjectif canonique, on a :*

$$\pi(\{I \trianglelefteq \mathcal{O}_K \mid 0 < \|I\| \leq M\}) = \mathrm{Cl}(\mathcal{O}_K)$$

Démonstration. Soit J un idéal fractionnaire non nul de $\mathcal{O}_K$. Il s'agit de montrer que J est équivalent à un idéal de A de norme inférieure ou égale à M. Quitte à multiplier J par un élément de $\mathrm{Princ}(\mathcal{O}_K)$, on peut supposer $J \trianglelefteq \mathcal{O}_K$. Le théorème précédent assure qu'il existe $a \in J \setminus \{0\}$ vérifiant :

$$|N(a)| \leq M \|J\|$$

Ainsi $\left\|aJ^{-1}\right\| \leq M$, et donc J^{-1} est équivalent à un idéal de A de norme inférieure ou égale à M. En appliquant le résultat à J^{-1} on conclut. □

Il est utile en pratique d'avoir une borne M explicite.
On va démontrer simultanément les deux théorèmes suivants :

Théorème 6.16. *(Borne de Minkowski explicite) Dans le théorème 6.14, on peut prendre :*

$$M = \frac{d!}{d^d}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{Disc}\, K|}$$

Théorème 6.17. *(Signe du discriminant) Le signe du discriminant de* K *est donné par* $(-1)^s$.

Remarque 6.18. La borne du théorème 6.16 n'est a priori pas optimale.

Démonstration. En reprenant la preuve de 6.14, on prend :

$$M = 2^d S \frac{\mathrm{covol}(\iota(\mathcal{O}_K))}{\mu(B)}$$

avec B la boule unité de $K_{\mathbb{R}}$ pour une norme $|\bullet|$ à choisir, μ une mesure de Lebesgue sur $K_{\mathbb{R}}$ à choisir et $S = \sup_{a \in B} |N(a)|$. On considère alors la norme suivante sur $K_{\mathbb{R}}$:

$$\left|(x_1, \ldots, x_r, y_1, \ldots, y_s)\right| = \sum_i |x_i| + 2 \sum_j \left|y_j\right|$$

Par inégalité arithmético-géométrique, on a :

$$\left|N((x_1, \ldots, x_r, y_1, \ldots, y_s))\right|^{1/d} \leq \frac{1}{d}\left|(x_1, \ldots, x_r, y_1, \ldots, y_s)\right|$$

et le cas d'égalité peut avoir lieu pour un point non nul, par exemple $(1, \ldots, 1, 1, \ldots, 1)$, donc :

$$S = d^{-d}$$

On note $(b_1, \ldots, b_d)$ la base canonique de $\mathbb{R}^r \times \mathbb{C}^s$ identifié à $\mathbb{R}^r \times (\mathbb{R}^2)^s$. On choisit la mesure de Lebesgue μ sur $K_{\mathbb{R}}$ qui donne un covolume unitaire au réseau $\bigoplus_i \mathbb{Z} b_i$. On

calcule à présent le covolume de $\iota(\mathcal{O}_K)$. Pour cela, prenons $(e_1,\dots,e_d)$ une base intégrale de K. Ainsi les $\iota(e_i)$ forment une $\mathbb{R}$-base de $K_{\mathbb{R}}$. On note $\theta_1,\dots,\theta_d$ les plongements *complexes* de K, numérotés de la façon suivante : $\theta_1=\sigma_1,\dots,\theta_r=\sigma_r$, puis $\theta_{r+1}=\tau_1$, $\theta_{r+2}=\overline{\tau_1}$ et ainsi de suite. On a alors :

$$\begin{aligned}\det_{(b_1,\dots,b_d)}(\iota(e_1),\dots,\iota(e_d)) &= \begin{vmatrix} \sigma_1(e_1) & \dots & \sigma_1(e_d) \\ \vdots & \ddots & \vdots \\ \sigma_r(e_1) & \dots & \sigma_r(e_d) \\ \operatorname{Re}\tau_1(e_1) & \dots & \operatorname{Re}\tau_1(e_d) \\ \operatorname{Im}\tau_1(e_1) & \dots & \operatorname{Im}\tau_1(e_d) \\ \vdots & \ddots & \vdots \\ \operatorname{Re}\tau_s(e_1) & \dots & \operatorname{Re}\tau_s(e_d) \\ \operatorname{Im}\tau_s(e_1) & \dots & \operatorname{Im}\tau_s(e_d) \end{vmatrix} = \left(\frac{i}{2}\right)^s \begin{vmatrix} \theta_1(e_1) & \dots & \theta_1(e_d) \\ \vdots & \ddots & \vdots \\ \theta_d(e_1) & \dots & \theta_d(e_d) \end{vmatrix} \\ &= \left(\frac{i}{2}\right)^s \sqrt{\operatorname{Disc}(K)}\end{aligned}$$

car pour tout vecteur $u\in\mathbb{C}^s$, on a l'égalité suivante dans $\Lambda_{\mathbb{C}}\mathbb{C}^s$:

$$\operatorname{Re}u\wedge\operatorname{Im}u=\frac{i}{2}u\wedge\overline{u}$$

Ici, $\sqrt{\operatorname{Disc}(K)}$ désigne une racine carrée arbitraire de $\operatorname{Disc}(K)$. Notons que ce déterminant doit être *réel*, donc son carré doit être un réel positif, ce qui signifie que :

$$(-1)^s\operatorname{Disc}(K)>0$$

puisqu'on sait déjà que c'est non nul. Ainsi le signe de $\operatorname{Disc}(K)$ est donné par $(-1)^s$, ce qui démontre le théorème 6.17. En passant au module on obtient l'égalité suivante :

$$\operatorname{covol}(\iota(\mathcal{O}_K))=\left|\det_{(b_1,\dots,b_d)}(\iota(e_1),\dots,\iota(e_d))\right|=\frac{\sqrt{|\operatorname{Disc}(K)|}}{2^s}$$

Il reste enfin à calculer le volume de la boule unité $\mu(B)$. On adopte les notations suivantes : x désigne une variable réelle et y une variable complexe. On a :

$$\mu(B)=\int_{\sum_i|x_i|+2\sum_j|y_j|\leq 1} dx_1\dots dx_r\,d\operatorname{Re}y_1\,d\operatorname{Im}y_1\dots d\operatorname{Re}y_s\,d\operatorname{Im}y_s$$

On pose alors :

$$I_{r,s}(t)=\int_{\sum_i|x_i|+\sum_j|y_j|\leq t} x_1\dots dx_r\,d\operatorname{Re}y_1\,d\operatorname{Im}y_1\dots d\operatorname{Re}y_s\,d\operatorname{Im}y_s$$

(on notera l'absence du 2 dans cette définition) de sorte que :

$$\mu(B)=\frac{I_{r,s}(1)}{4^s}$$

en effectuant le changement de variable $y_j' = 2y_j$. On va à présent calculer $I_{r,s}(t)$ par récurrence. On a, par Fubini :

$$I_{r,s+1}(t) = \int_{|y_1|\leq t} I_{r,s}(t - |y_1|)d\,\mathrm{Re}\,y_1\,d\,\mathrm{Im}\,y_1$$

Un changement de coordonnées polaires $y_1 = \rho e^{i\alpha}$ donne alors :

$$I_{r,s+1}(t) = 2\pi \int_0^t I_{r,s}(t-\rho)\rho d\rho = 2\pi \int_0^t I_{r,s}(\rho)(t-\rho)d\rho$$

donc $I'_{r,s+1}(t) = 2\pi \int_0^t I_{r,s}(\rho)d\rho + 2\pi I_{r,s}(t)t - 2\pi t I_{r,s}(t) = 2\pi \int_0^t I_{r,s}(\rho)d\rho$, et ainsi :

$$I''_{r,s+1} = 2\pi I_{r,s}$$

On peut prendre la convention $I_{0,0}(t) = 1$ pour que cette formule soit valable avec $r = s = 0$: en effet, dans ce cas, il faut prendre $I_{0,0} = 1$ pour le calcul de l'intégrale précédente. On a de plus les conditions limites $I_{0,s}(0) = 0$ et $I'_{0,s}(0) = 0$ d'après le calcul précédent. Une récurrence permet alors d'obtenir :

$$I_{0,s}(t) = \frac{(2\pi)^s}{(2s)!}t^{2s}$$

Ensuite on observe que :

$$I_{r+1,s}(t) = \int_{|x_1|\leq t} I_{r,s}(t - |x_1|)dx_1 = 2\int_0^t I_{r,s}(u)du$$

de sorte que $I'_{r+1,s} = 2I_{r,s}$. Avec la condition au limite $I_{r,s}(0) = 0$, on obtient :

$$I_{r,s}(t) = \frac{(2\pi)^s 2^r t^{2s+r}}{(2s+r)!} = \frac{(2\pi)^s 2^r t^d}{d!}$$

pour $d = r + 2s$. On a donc :

$$\mu(B) = \frac{\pi^s 2^{r-s}}{d!}$$

Au final on a :

$$M = 2^d d^{-d}\frac{\sqrt{|\mathrm{Disc}(K)|}}{2^s} \times \frac{d!}{\pi^s 2^{r-s}} = \frac{d!}{d^d}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{Disc}\,K|}$$

□

Une première application simple de cette estimation est le résultat suivant.

Corollaire 6.19. *On a toujours :*

$$|\mathrm{Disc}(K)| \geq \left(\frac{d^d}{d!}\left(\frac{\pi}{4}\right)^s\right)^2 \geq \left(\frac{d^d}{d!}\right)^2\left(\frac{\pi}{4}\right)^d \sim_{d\to\infty} \frac{1}{2\pi d}\left(\frac{\pi e^2}{4}\right)^d$$

En particulier le discriminant de K tend vers l'infini quand d tend vers l'infini. De plus, si $K \neq \mathbb{Q}$, alors $|\mathrm{Disc}(K)| \geq 3$ et ainsi le seul corps de nombres de discriminant 1 est $\mathbb{Q}$.

Démonstration. On applique le théorème 6.14 à l'idéal non nul $I = \mathcal{O}_K$. Il existe donc $a \in \mathcal{O}_K \setminus \{0\}$ tel que :

$$0 < |N(a)| \leq M$$

On a donc :

$$M \geq 1$$

Ainsi $|\mathrm{Disc}(K)| \geq \left(\frac{d^d}{d!}\left(\frac{\pi}{4}\right)^s\right)^2$. Ensuite, $\pi/4 < 1$ et puisque $r + 2s = d$, on a $2s \leq d$, d'où la seconde inégalité. Une étude de fonction permet d'établir que la suite $\left(\left(\frac{d^d}{d!}\right)^2\left(\frac{\pi}{4}\right)^d\right)_{d\geq 1}$ est croissante. Ainsi, si $K \neq \mathbb{Q}$, on a $d \geq 2$ et donc :

$$|\mathrm{Disc}(K)| \geq \left(\frac{2^2}{2!}\right)^2\left(\frac{\pi}{4}\right)^2 \geq \frac{\pi^2}{4} > 2$$

et le discriminant est entier donc $|\mathrm{Disc}(K)| \geq 3$. Enfin, on obtient facilement l'équivalent annoncé avec la formule de Stirling :

$$d! \sim_{d\longrightarrow\infty} \left(\frac{d}{e}\right)^d \sqrt{2\pi d}$$

□

Mentionnons enfin la valeur de M pour les corps quadratiques.

Proposition 6.20. *Pour $K = \mathbb{Q}(\sqrt{d})$ avec d différent de 0 et 1 et sans facteur carré, on a :*

$$M = \begin{cases} \frac{2}{\pi}\sqrt{|d|} & \text{si } d \equiv 1\ [4] \\ \frac{4}{\pi}\sqrt{|d|} & \text{sinon} \end{cases}$$

Démonstration. Il suffit d'utiliser la proposition 6.9. □

6.5 Finitude du groupe des classes

Un des résultats majeurs de la géométrie des nombres est la finitude du groupe des classes d'un anneau d'entiers de corps de nombres. Tous les anneaux de Dedekind n'ont pas un groupe de classe fini et on va utiliser la borne de Minkowski, propre aux anneaux d'entiers de corps de nombres, pour obtenir ce résultat.
Soit K un corps de nombres de degré d.

Proposition 6.21. *Soit $R > 0$. Il n'y a qu'un nombre fini d'idéaux de $\mathcal{O}_K$ de norme inférieure ou égale à R.*

Démonstration. On note E l'ensemble des idéaux non nuls de $\mathcal{O}_K$ de norme inférieure ou égale à R.
Prenons un entier $k \geq 1$ divisible par tous les entiers de l'intervalle $[1, R]$ (par exemple le ppcm de ces entiers). Ainsi, pour tout $I \in E$, on a $k(\mathcal{O}_K/I) = 0$ par le théorème de Lagrange. On a donc $k\mathcal{O}_K \subseteq I$, et ainsi E est contenu dans l'ensemble F des sous-groupes de $\mathcal{O}_K$ contenant $k\mathcal{O}_K$, lui même en bijection avec l'ensemble *fini* des sous-groupes du groupe *fini* $\mathcal{O}_K/k\mathcal{O}_K$. □

Théorème 6.22. *(Finitude du groupe des classes) Le groupe des classes de K, $\mathrm{Cl}(\mathcal{O}_K)$ est fini.*

Démonstration. Comme précedemment, M désigne une *borne de Minkowski* pour K. D'après le théorème 6.15, il suffit de montrer que l'ensemble :

$$E = \{I \trianglelefteq \mathcal{O}_K \mid 0 < \|I\| \leq M\}$$

est fini. Cela découle de la proposition 6.21. □

6.6 Groupe des inversibles de l'anneau des entiers

Soit K un corps de nombres de degré $d = r + 2s$ avec les notations précédentes (voir 6.3). L'objectif de ce paragraphe est de déterminer la structure du groupe des inversibles de $\mathcal{O}_K$, que l'on notera $\mathcal{O}_K^\times$.

Proposition 6.23. *On a l'égalité suivante :*

$$\mathcal{O}_K^\times = \{z \in \mathcal{O}_K \mid |N(z)| = 1\}$$

Démonstration. Si $z \in \mathcal{O}_K^\times$, sa norme est un entier inversible donc c'est ± 1. Réciproquement, si $z \in \mathcal{O}_K$ vérifie $N(z) = \pm 1$, alors l'idéal (z) est de norme 1, et donc $(z) = \mathcal{O}_K$ et z est inversible dans $\mathcal{O}_K$. □

Définition 6.24. *On note S_K le sous-groupe de Lie de $K_\mathbb{R}^\times$ constitué des éléments $a \in K_\mathbb{R}$ tels que $|N(a)| = 1$. Ainsi S_K est de dimension $d-1$. On a par construction $\iota(\mathcal{O}_K^\times) \subseteq S_K \subseteq K_\mathbb{R}^\times$.*

On aura besoin du théorème suivant sur les sous-groupes discrets des groupes de Lie abéliens connexes. On utilise la notation $\mathbb{U}$ pour le cercle unité de $\mathbb{C}$.

Théorème 6.25. *Soit A un groupe de Lie abélien isomorphe à $\mathbb{R}^k \times \mathbb{U}^\ell \times F$ avec k, ℓ des entiers naturels et F un groupe abélien fini et soit G un sous-groupe discret de A. Alors G est un groupe abélien de type fini de rang inférieur ou égal à k, et G est de rang k si et seulement si il est cocompact, au sens où A/G est compact.*
Ici le rang de G désigne la dimension du $\mathbb{Q}$-espace vectoriel $G \otimes_\mathbb{Z} \mathbb{Q}$.

Remarque 6.26. Ce théorème couvre le cas de tous les groupes de Lie abéliens connexes, puisqu'il sont tous de la forme $\mathbb{R}^k \times \mathbb{U}^\ell$: en effet, si G est un groupe de Lie abélien connexe, alors son algèbre de Lie $\mathfrak{g}$ a un crochet de Lie nul et l'exponentielle

$$\mathfrak{g} \longrightarrow G$$

est alors un morphisme de groupes qui est un difféomorphisme local (car de rang constant et c'est un difféomorphisme local en 0 par théorème d'inversion locale). L'image de ce morphisme est donc un sous-groupe ouvert (et donc fermé) de G et donc ce morphisme est surjectif (car G est connexe) et son noyau est un sous-groupe fermé de $\mathfrak{g}$ de dimension 0, c'est à dire un sous-groupe discret, donc libre de rang d inférieur ou égal à la dimension de G d'après le théorème 4.27. On a donc un isomorphisme de groupes de Lie :

$$G \cong \mathfrak{g}/\ker(\exp) \cong \mathbb{R}^k/\mathbb{Z}^d \cong \mathbb{R}^{k-d} \times \mathbb{U}^d$$

avec $k = \dim G$.

Démonstration. On traite d'abord le cas où F est le groupe trivial. On peut alors supposer $A = \mathbb{R}^k \times \mathbb{U}^\ell$. Soit G un sous-groupe discret de A. Le revêtement universel de A est $\mathbb{R}^{k+\ell} \xrightarrow{p} A$ et $p^{-1}(G)$ est un sous-groupe discret de ce revêtement universel. Le théorème 4.27 assure alors que $p^{-1}(G)$ est un groupe abélien libre de rang $q \leq k+\ell$. On a une suite exacte :

$$0 \longrightarrow \ker p = \{0\}^k \times \mathbb{Z}^\ell \longrightarrow p^{-1}(G) \xrightarrow{p} G \longrightarrow 0$$

puisque $\ker p \subseteq p^{-1}(G)$. Ainsi G est de type fini et de rang $q - \ell \leq k$ (on peut tensoriser la suite exacte par $\mathbb{Q}$ qui est plat sur $\mathbb{Z}$). Montrons ensuite que G est cocompact si et seulement si il est de rang k. On a un isomorphisme de groupes de Lie :

$$\mathbb{R}^{k+\ell}/p^{-1}(G) \cong A/G$$

donc G est cocompact si et seulement si $p^{-1}(G)$ est cocompact dans $\mathbb{R}^{k+\ell}$, i.e. (par la proposition 4.28) si $p^{-1}(G)$ est de rang $k+\ell$. Or $\operatorname{Rg} G + \ell = \operatorname{Rg} p^{-1}(G)$ d'après la suite exacte précédente, donc finalement G est cocompact si et seulement si il est de rang k. Ensuite, traitons le cas général où $A = F \times \mathbb{R}^k \times \mathbb{U}^\ell$. On note $\pi : A \longrightarrow A/F$ la surjection canonique, qui est un revêtement à fibres finies, de sorte que si G est un sous-groupe discret de A, alors $\pi(G)$ est un sous-groupe discret de A/F, et donc $\pi(G)$ est de type fini et de rang inférieur ou égal à k par ce qui précède. Or on a une suite exacte :

$$0 \longrightarrow F \cap G \longrightarrow G \longrightarrow \pi(G) \longrightarrow 0$$

donc G est de type fini et de rang au plus k puisque $F \cap G$ est fini.
Enfin, G est cocompact si et seulement si $\pi(G)$ est cocompact dans A/F
car $(A/F)/\pi(G) \cong A/(F+G) \cong (A/G)/$ et on utilise le cas précédent pour conclure. □

Proposition 6.27. *On a un isomorphisme de groupes de Lie :*

$$S_K \cong \{\pm 1\}^r \times \mathbb{U}^s \times \mathbb{R}^{r+s-1}$$

Démonstration. Avec l'identification $K_\mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$, on a :

$$K_\mathbb{R}^\times = (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$$

On peut alors "redresser" $K_\mathbb{R}$ via l'isomorphisme de groupes de Lie suivant :

$$\ell : \begin{cases} K_\mathbb{R}^\times \longrightarrow \{\pm 1\}^r \times \mathbb{U}^s \times \mathbb{R}^{r+s} \\ (x_1, \dots, x_r, y_1, \dots, y_s) \mapsto \left(\frac{x_1}{|x_1|}, \dots, \frac{x_r}{|x_r|}, \frac{y_1}{|y_1|}, \dots, \frac{y_s}{|y_s|}, \log|x_1|, \dots, \log|x_r|, 2\log\left|y_1\right|, \dots, 2\log\left|y_s\right| \right) \end{cases}$$

On note alors H l'hyperplan de $\mathbb{R}^{r+s}$ qui est le noyau de la forme linéaire $(1 \ \dots 1)$, de sorte que :

$$\ell(S_K) = \{\pm 1\}^r \times \mathbb{U}^s \times H$$

ce qui conclut.

□

Pour étudier le groupe $\mathcal{O}_K^\times$, on l'identifie à son image dans S_K qui lui est isomorphe via ι.

Lemme 6.28. *Le groupe $\mathcal{O}_K^\times$ est cocompact dans S_K.*

Démonstration. On note ici $G = \mathcal{O}_K^\times$. Soit $a \in S_K$. Puisque $|N(a)| = 1$, on a :

$$\mathrm{covol}(a\iota(\mathcal{O}_K)) = \mathrm{covol}(\iota(\mathcal{O}_K))$$

en fixant une mesure de Lebesgue sur $K_\mathbb{R}$. Par le théorème de Minkowski 4.36, il existe donc un élément $z \in \mathcal{O}_K \setminus \{0\}$ dépendant de a tel que :

$$|a\iota(z)| \leq R$$

avec $R > 0$ une constante *indépendante* de a. Si on pose $u = a\iota(z)$ On a ainsi $|u| \leq R$ et $|N(u)| = |N(z)|$.

$$S_K = \bigcup_{z \in \mathcal{O}_K \setminus \{0\}} \frac{1}{\iota(z)} \{u \in K_\mathbb{R} \mid |u| \leq R,\ |N(u)| = |N(z)|\}$$

On note S le maximum de $|N|$ sur la boule unité fermée de $K_\mathbb{R}$ de sorte que, si $|u| \leq R$, alors $|N(u)| \leq SR^d$. De plus la norme d'un élément de $\mathcal{O}_K$ est un entier, donc :

$$S_K = \bigcup_{k=1}^{\lfloor SR^d \rfloor} \{u \in K_\mathbb{R} \mid |u| \leq R,\ |N(u)| = k\} \cdot \iota\Big(\{z \in \mathcal{O}_K \mid |N(z)| = k\}^{-1}\Big)$$

On pose $X_k = \{z \in \mathcal{O}_K \mid |N(z)| = k\}$, qui est stable par l'action de $\mathcal{O}_K^\times$. Le quotient $X_k/\mathcal{O}_K^\times$ se plonge injectivement dans l'ensemble des idéaux de $\mathcal{O}_K$ de norme k (via l'application $z \mapsto (z)$). Par la proposition 6.21, le quotient $X_k/\mathcal{O}_K^\times$ est donc fini. Ainsi on a :

$$S_K/G = \bigcup_{k=1}^{\lfloor SR^d \rfloor} \pi\left(\{u \in K_\mathbb{R} \mid |u| \leq R,\ |N(u)| = k\}\right) \cdot (\iota(X_k)/G)^{-1}$$

avec $\pi : S_K \longrightarrow S_K/G$ la surjection canonique. Dans cette réunion finie, $\iota(X_k)/G$ est un ensemble fini car $X_k/\mathcal{O}_K^\times$ est un ensemble fini, et $\pi(\{u \in K_\mathbb{R} \mid |u| \leq R,\ |N(u)| = k\})$ est compact car π est continue et le quotient S_K/G est séparé (puisque G est fermé dans S_K). Ainsi S_K/G est compact comme réunion finie de compacts dans un espace séparé. □

Le résultat suivant, dû à Dirichlet, donne la structure du groupe $\mathcal{O}_K^\times$.

Théorème 6.29. *(des Unités de Dirichlet) Le groupe $\mathcal{O}_K^\times$ est produit direct interne de son groupe de torsion qui est cyclique et d'un sous-groupe abélien libre F de rang $r + s - 1$, i.e. :*

$$\mathcal{O}_K^\times = \mathbb{U}_\infty(K) \odot F$$

avec $\mathbb{U}_\infty(K)$ est l'ensemble des racines de l'unité de K (c'est exactement le sous-groupe de torsion de $\mathcal{O}_K^\times$). Ici la notation $\odot$ signifie "produit direct interne" pour un groupe dont la loi est notée multiplicativement.

Démonstration. Le groupe G est discret et cocompact dans S_K donc le théorème 6.25 et la proposition 6.27 assurent que G est de type fini et de rang $r + s - 1$. On conclut alors avec le théorème de structure des groupes abéliens de type fini en observant que la torsion de $\mathcal{O}_K^\times \subseteq \mathbb{C}^\times$ est simplement $\mathbb{U}_\infty(K)$ qui est cyclique. □

Remarque 6.30. Il n'y a pas unicité d'un tel sous-groupe F en général, et en exhiber une base est un problème très difficile, même pour les corps quadratiques réels. Pour un tel corps $\mathbb{Q}(\sqrt{d})$ avec $d \geq 2$ sans facteur carré, on a $r = 2$ et $s = 0$ donc F est libre de rang 1, et un générateur de F est appelé une unité fondamentale de K.
Si $d \not\equiv 1$ [4], trouver les unités revient à résoudre l'équation $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a+b\sqrt{d}) = \pm 1$, i.e. une équation dite de Pell-Fermat :

$$a^2 - db^2 = \pm 1.$$

Par exemple, pour $d = 2$, $1+\sqrt{2}$ est une unité fondamentale et le groupe des unités de $K = \mathbb{Q}(\sqrt{2})$ est donné par :

$$\mathcal{O}_K^\times = (1+\sqrt{2})^{\mathbb{Z}} \odot \{\pm 1\}.$$

On déduit du théorème de Dirichlet une preuve (loin d'être la plus élémentaire) du théorème de Kronecker.

Théorème 6.31. *(de Kronecker) Soit $z \in \overline{\mathbb{Z}}$ un entier algébrique dont tous les conjugués (dont z lui même) sont de module inférieur ou égal à 1. Alors z est une racine de l'unité.*

Démonstration. Notons $K = \mathbb{Q}(z)$. C'est un corps de nombres. Notons π le polynôme minimal de z sur $\mathbb{Q}$. Puisque $\pi(0)$ est (au signe près) le produit des conjugués de z et qu'il s'agit d'un entier, les conjugués de z sont de module *exactement* 1. De plus $z \in \mathcal{O}_K^\times$ car tous les conjugués de z sont de module 1 et donc $|N(z)| = 1$. Ainsi $z \in \mathcal{O}_K^\times$. Puisque les conjugués de z sont de module 1, on a $\ell \circ \iota(z) \in \{\pm 1\}^r \times \mathbb{U}^s \times \{0\}$. Or le sous-groupe de $\{\pm 1\}^r \times \mathbb{U}^s$ engendré par $\ell \circ \iota(z)$ est *discret* donc il est fini d'après le théorème 6.25. Ainsi z est d'ordre fini : c'est une racine de l'unité. □

6.7 Régulateur d'un corps de nombres

Le théorème des unités de Dirichlet 6.29 permet de définir un invariant d'un corps de nombres K, *le régulateur de K*, qui mesure en quelque sorte la densité de $\mathcal{O}_K^\times$ dans $\mathcal{O}_K$. On reprend les mêmes notations que dans le paragraphe précédent. On a notamment un isomorphisme de groupes de Lie :

$$\ell : \begin{cases} K_{\mathbb{R}}^\times \longrightarrow \{\pm 1\}^r \times \mathbb{U}^s \times \mathbb{R}^{r+s} \\ (x_1, \dots, x_r, y_1, \dots, y_s) \mapsto \left(\frac{x_1}{|x_1|}, \dots, \frac{x_r}{|x_r|}, \frac{y_1}{|y_1|}, \dots, \frac{y_s}{|y_s|}, \log|x_1|, \dots, \log|x_r|, 2\log|y_1|, \dots, 2\log|y_s| \right) \end{cases}$$

qui envoie S_K sur $\{\pm 1\}^r \times \mathbb{U}^s \times H$. On munit $\mathbb{R}^{r+s}$ du produit scalaire canonique, qui se retreint à H pour faire de H un espace euclidien qui est alors muni d'une mesure de Lebesgue canonique μ, celle qui donne mesure 1 à un hypercube de dimension $r+s-1$ orthonormé.
On choisit F un sous-groupe libre de rang $r+s-1$ de $\mathcal{O}_K^\times$ tel que :

$$\mathcal{O}_K^\times = \mathbb{U}_\infty(K) \odot F$$

donné par le théorème des unités. On note $\pi : \{\pm 1\}^r \times \mathbb{U}^s \times \mathbb{R}^{r+s} \longrightarrow \mathbb{R}^{r+s}$ la projection sur les dernières coordonnées, et $\hat{\ell} = \pi \circ \ell$, qui est un morphisme de groupes de Lie de

rang $r+s$. Pour simplifier les notations, on considère que $K \subseteq K_{\mathbb{R}}$ et ainsi on omettra de noter le morphisme $\iota : K \longrightarrow K_{\mathbb{R}}$. Notons que :

$$\hat{\ell}(F) \subseteq H$$

car les éléments de $\mathcal{O}_K^\times$ sont de norme ± 1. Notons de plus que $\hat{\ell}(F)$ est indépendant de F car :

$$\hat{\ell}(F) = \hat{\ell}(\mathcal{O}_K^\times)$$

puisque les éléments de torsion sont envoyés par ℓ dans $\{\pm 1\}^r \times \mathbb{U}^s$. On note Λ ce groupe, qu'on appelle *réseau des unités*. La proposition suivante justifie cette terminologie.

Proposition 6.32. *Le groupe Λ est un réseau de H et $\hat{\ell}$ réalise un isomorphisme de groupes entre F et Λ.*

Démonstration. D'abord, le morphisme $\hat{\ell}$ est injectif sur F :

$$\ker \hat{\ell} = \ell^{-1}(\{\pm 1\}^r \times \mathbb{U}^s)$$

Ainsi on a :

$$\ker \hat{\ell} \cap \mathcal{O}_K^\times = \mathbb{U}_\infty(K).$$

En effet l'inclusion de droite à gauche est claire, et si $z \in \ker \hat{\ell} \cap \mathcal{O}_K^\times$, le sous-groupe de $\{\pm 1\}^r \times \mathbb{U}^s$ engendré par $\ell(z)$ est discret et donc fini. Or $F \cap \mathbb{U}_\infty(K) = \{1\}$ donc $\hat{\ell}$ est injectif sur F, et induit un isomorphisme :

$$F \cong \Lambda$$

Ensuite Λ est un sous-groupe *discret* de $\mathbb{R}^{r+s}$ et donc de H : il suffit de montrer que 0 est isolé dans Λ. Puisque F est discret dans $K_{\mathbb{R}}$, $\ell(F)$ est discret dans $\{\pm 1\}^r \times \mathbb{U}^s \times \mathbb{R}^{r+s}$ donc il existe un voisinage ouvert V du neutre $(1,\dots,1,0,\dots,0)$ dont l'intersection avec $\ell(F)$ est réduite au neutre. Par définition de la topologie produit et quitte à rétrécir V, on peut supposer que $V = W \times W'$ avec W un ouvert de $\{\pm 1\}^r \times \mathbb{U}^s$ contenant le neutre et W' un ouvert de $\mathbb{R}^{r+s}$ contenant 0. Par locale compacité de $\{\pm 1\}^r \times \mathbb{U}^s \times \mathbb{R}^{r+s}$ on peut aussi supposer $\overline{W'}$ compact. On pose alors :

$$U = \pi^{-1}(W') = \{\pm 1\}^r \times \mathbb{U}^s \times W'$$

qui est un ouvert d'adhérence compacte contenant le neutre. Ainsi $U \cap \ell(F)$ est fini (car contenu dans quelque chose de discret et compact) et donc $\pi(U \cap \ell(F))$ est un ensemble fini contenu dans W'. Quitte à encore rétrécir W', on peut donc supposer que :

$$\pi(U \cap \ell(F)) = \{0\}$$

Or on a :

$$\hat{\ell}(F) \cap W' = \pi(U \cap \ell(F)) = \{0\}$$

et $\hat{\ell}(F)$ est donc discret dans H. Par le théorème des unités de Dirichlet 6.29, c'est aussi un sous-groupe de H de rang $r+s-1$ qui est aussi la dimension de H, et donc par 4.28 c'est un réseau de H (car discret et de rang la dimension de H). □

Définition 6.33. *On définit le régulateur de K par la formule suivante :*

$$\mathrm{Reg}(K) = \frac{1}{\sqrt{r+s}}\mathrm{covol}(\Lambda)$$

où le covolume est pris avec la mesure μ sur H définie plus haut. Ainsi, plus le régulateur est petit, plus le réseau Λ est dense et donc plus les unités sont denses dans S_K.

On souhaite donner une formule plus directe pour calculer le régulateur. Pour cela on commence par observer le fait suivant.

Lemme 6.34. *Soit V un $\mathbb{R}$-espace vectoriel de dimesnion n et $x_1, \dots, x_{n+1}$ des vecteurs de V tels que :*

$$\sum_{i=1}^{n+1} x_i = 0.$$

Soit ω une n-forme alternée (par exemple le déterminant dans une base de V). Alors pour tout i, la quantité :

$$|\omega(x_1, \dots, \widehat{x_i}, \dots, x_n)|$$

est indépendante de i. Ici le chapeau désigne une omission.
En particulier, si M est une matrice rectangulaire à $n+1$ lignes et n colonnes telle que la somme des coefficients de chaque colonne est nulle, ce qui précède s'applique aux lignes de M et implique que pour tout i entre 1 et $n+1$, le déterminant de la matrice obtenue en retirant la i-ème ligne de M ne dépend pas au signe près de i.

Démonstration. Par caractère antisymétrique de ω, il suffit de montrer que :

$$\omega(x_1, x_3, \dots, x_{n+1}) = \pm\omega(x_2, x_3, \dots, x_{n+1}).$$

Or on a :

$$\omega(x_1, x_3, \dots, x_{n+1}) = \omega\left(-\sum_{i\geq 2} x_i, x_3, \dots, x_{n+1}\right) = -\omega(x_2, x_3, \dots, x_{n+1})$$

par caractère multilinéaire et alterné de ω. □

La proposition suivante donne une définition calculatoire pour le régulateur, et justifie le choix du facteur $(r+s)^{-1/2}$.

Proposition 6.35. *Soit $(u_1, \dots, u_{r+s-1})$ une base du $\mathbb{Z}$-module libre F (i.e. tout élément de F s'écrit de manière unique $\prod_i u_i^{a_i}$ avec $a_i \in \mathbb{Z}$). Alors la matrice rectangulaire à $r+s$ lignes et $r+s-1$ colonnes suivante :*

$$M = \begin{pmatrix} \log|\sigma_1(u_1)| & \dots & \log|\sigma_1(u_{r+s-1})| \\ \vdots & \ddots & \dots \\ \log|\sigma_r(u_1)| & \dots & \log|\sigma_r(u_{r+s-1})| \\ 2\log|\tau_1(u_1)| & \dots & 2\log|\tau_s(u_1)| \\ \vdots & \ddots & \vdots \\ 2\log|\tau_s(u_1)| & \dots & 2\log|\tau_s(u_{r+s-1})| \end{pmatrix}$$

est telle que la somme des coefficients de chaque colonne est nulle, et en en retirant une ligne quelconque on obtient une matrice carrée M' de taille $r+s-1$ dont la valeur absolue du déterminant est égale au régulateur de K :

$$\mathrm{Reg}(K) = \left|\det(M')\right|.$$

Démonstration. D'après le lemme 6.34, la ligne retirée n'a pas d'influence sur R. On peut supposer que l'on retire la dernière ligne de M pour obtenir M'. On note $\underline{e}$ la base canonique de $\mathbb{R}^{r+s}$ et $\underline{e}^*$ sa base duale. On note aussi $v_i = \hat{\ell}(u_i) \in H$ de sorte que M est la matrice de la famille $\underline{v}$ dans la base $\underline{e}$ de $\mathbb{R}^{r+s}$. Pour une famille $\underline{w}$ de $r+s-1$ vecteurs de H, on pose :

$$\alpha(\underline{w}) = \det\left((e_i^*(w_j))_{i,j\leq r+s-1}\right)$$

On fixe aussi $\underline{h}$ une base orthonormée de H et on pose :

$$\beta(\underline{w}) = \det_{\underline{h}}(\underline{w}).$$

On va comparer ces deux formes $r+s-1$-linéaires alternées sur H au signe près. On considère la base de H suivante :

$$w_i = e_i - e_{r+s}$$

pour $1 \leq i \leq r+s-1$. On a ainsi :

$$\alpha(\underline{w}) = \begin{vmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{vmatrix} = 1$$

tandis que, par la formule de Gram :

$$\left|\beta(\underline{w})\right| = \sqrt{\det\left(\left(\langle w_i, w_j\rangle\right)_{i,j}\right)}$$

et on a $\langle w_i, w_j\rangle = \delta_{ij} + 1$. Le déterminant de cette matrice se calcule facilement par récurrence, il vaut $r+s$, et ainsi on a :

$$\beta(\underline{w}) = \pm\sqrt{r+s}\cdot\alpha(\underline{w}).$$

Ceci est valable pour toute base $\underline{w}$ de H car les $r+s-1$-formes sur H forment un espace vectoriel de dimension 1. Ainsi on a :

$$\beta(\underline{v}) = \pm\sqrt{r+s}\alpha(\underline{v}) = \pm\sqrt{r+s}\det(M')$$

Or par définition :

$$\beta(\underline{v}) = \pm\det_{\underline{h}}(\underline{v}) = \pm\mathrm{covol}(\Lambda).$$

Ceci conclut la preuve. □

La proposition suivante donne le calcul du régulateur pour les corps quadratiques. Notons d'ailleurs que $\mathrm{Reg}(\mathbb{Q}) = 1$ car un déterminant de taille 0 vaut 1.

Proposition 6.36. *Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique avec d entier sans facteur carré différent de 0 et 1.*
Si $d < 0$, alors $\mathrm{Reg}(K) = 1$, et si $d > 0$:

$$\mathrm{Reg}(K) = |\log|\alpha||$$

avec α une unité fondamentale de K, c'est à dire un générateur de $\mathcal{O}_K^\times$ modulo $\mathbb{U}_\infty(K)$.

Démonstration. Si $d < 0$, alors $r = 0$ et $s = 1$ donc le régulateur vaut 1. Sinon on a $r = 2$ et $s = 0$ et la proposition 6.35 donne :

$$\mathrm{Reg}(K) = |\det(\log|\alpha|)| = |\log|\alpha||.$$

□

Chapitre 7

Théorie de Galois des extensions de Dedekind

> Sauter des passages est un point important. Il faut le faire chaque fois qu'une démonstration semble trop difficile, ou lorsqu'un théorème ou même tout un paragraphe ne parle pas au lecteur. Dans la plupart des cas, il pourra continuer malgré tout, et revenir plus tard aux parties qu'il a laissées de côté.
>
> Emil Artin

7.1 Factorisation dans une extension galoisienne

On considère ici une extension de Dedekind B/A *galoisienne*, au sens où l'extension des corps de fractions associés L/K est une extension *galoisienne* dont on note G le groupe de Galois. On suppose aussi A localement parfait (voir 5.38), au sens où tous ses corps résiduels $A/\mathfrak{p}$ avec $\mathfrak{p}$ premier non nul sont parfaits.

Proposition 7.1. *Soit $\mathfrak{p}$ un premier de A. Le groupe de Galois G agit transitivement sur les premiers au dessus de $\mathfrak{p}$.*

Démonstration. Premièrement, l'action est bien définie puisque si $\mathfrak{q}$ est un premier au dessus de $\mathfrak{p}$ et $\sigma \in G$, alors on a bien $\mathfrak{p} \subseteq \sigma(\mathfrak{q})$ car $\sigma(\mathfrak{p}) = \mathfrak{p}$, et $\sigma(\mathfrak{q})$ est un idéal premier car :

$$B/\sigma(\mathfrak{q}) = \sigma(B)/\sigma(\mathfrak{q}) \cong B/\mathfrak{q}$$

qui est intègre. De plus $\sigma(\mathfrak{q}) \neq 0$. Le fait que $\sigma(B) = B$ vient du fait que tout élément de σB est encore entier sur A et l'autre inclusion s'obtient en utilisant σ^{-1}.
L'action est transitive : soient $\mathfrak{q}, \mathfrak{q}'$ au dessus de $\mathfrak{p}$. On suppose par l'absurde que pour

tout $\sigma \in G$, on a $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$. Par le théorème des restes chinois, il existe alors $x \in B$ tel que $x \equiv 0\ [\mathfrak{q}']$ et $x \equiv 1\ [\sigma^{-1}(\mathfrak{q})]$ pour tout $\sigma \in G$, puisque $\mathfrak{q}'$ est premier à tous les $\sigma^{-1}(\mathfrak{q})$ car ce sont des idéaux maximaux distincts. Ainsi on a :

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \equiv 1\ [\mathfrak{q}]$$

mais $x \in \mathfrak{q}'$ donc $N_{L/K}(x) \in \mathfrak{q}' \cap K$, et ainsi $N_{L/K}(x) \in \mathfrak{p}$. En particulier $N_{L/K}(x) \in \mathfrak{q}$, ce qui est en contradiction avec $N_{L/K}(x) \equiv 1\ [\mathfrak{q}]$. □

Proposition 7.2. *Soit $\mathfrak{p}$ un premier de A. Alors les indices $e(\mathfrak{q} \mid \mathfrak{p})$ et $f(\mathfrak{q} \mid \mathfrak{p})$ avec $\mathfrak{q}$ au dessus de $\mathfrak{p}$ ne dépendent que de $\mathfrak{p}$. On les note alors $e(\mathfrak{p})$ et $f(\mathfrak{p})$ et on note aussi $r(\mathfrak{p})$ le nombre de premiers de B au dessus de $\mathfrak{p}$. On a de plus :*

$$e(\mathfrak{p})f(\mathfrak{p})r(\mathfrak{p}) = [L : K].$$

Démonstration. Puisque G agit transitivement sur les premiers au dessus de $\mathfrak{p}$ d'après la proposition 7.1, il suffit de montrer que pour tout $\sigma \in G$ et $\mathfrak{q}$ au dessus de $\mathfrak{p}$, on a :

$$e(\mathfrak{q} \mid \mathfrak{p}) = e(\sigma\mathfrak{q} \mid \mathfrak{p})$$

et :

$$f(\mathfrak{q} \mid \mathfrak{p}) = f(\sigma\mathfrak{q} \mid \mathfrak{p}).$$

On a :

$$\mathfrak{p}B = \prod_{\mathfrak{q} \supseteq \mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}$$

et $\sigma^{-1}\mathfrak{p} = \mathfrak{p}$ donc :

$$\mathfrak{p}B = \sigma^{-1}(\mathfrak{p}B) = \prod_{\mathfrak{q} \supseteq \mathfrak{p}} (\sigma^{-1}\mathfrak{q})^{e(\mathfrak{q}|\mathfrak{p})} = \prod_{\mathfrak{q} \supseteq \mathfrak{p}} \mathfrak{q}^{e(\sigma\mathfrak{q}|\mathfrak{p})}$$

en faisant le changement de variable $\mathfrak{q} \leftarrow \sigma^{-1}\mathfrak{q}$. On a donc $e(\mathfrak{q} \mid \mathfrak{p}) = e(\sigma\mathfrak{q} \mid \mathfrak{p})$. Ensuite on a :

$$B/\sigma\mathfrak{q} = \sigma B/\sigma\mathfrak{q} \cong B/\mathfrak{q}$$

en tant que $A/\mathfrak{p}$-espaces vectoriels (car σ agit trivialement sur $\mathfrak{p}$) donc $f(\sigma\mathfrak{q} \mid \mathfrak{p}) = f(\mathfrak{q} \mid \mathfrak{p})$. Enfin, la formule des degrés 5.17 donne $e(\mathfrak{p})f(\mathfrak{p})r(\mathfrak{p}) = [L : K]$.

□

Définition 7.3. *Soit $\mathfrak{q}$ un premier de B au dessus de $\mathfrak{p}$ un premier de A. On appelle groupe de Galois local de $\mathfrak{q}$ au dessus de $\mathfrak{p}$ le groupe de Galois noté $\overline{G}(\mathfrak{q} \mid \mathfrak{p})$ de l'extension $A/\mathfrak{p} \subseteq B/\mathfrak{q}$. Cette extension est galoisienne car A est localement parfait et L/K est normale (si $b \in B$, le polynôme minimal π_b de b sur K est unitaire et à coeffients dans A et est scindé car L/K est normale, et ainsi $\overline{b}$ est annulé par $\overline{\pi_b}$ qui est non nul, à coefficients dans $A/\mathfrak{p}$ et scindé dans $B/\mathfrak{p}$).*
Ainsi $\overline{G}(\mathfrak{q} \mid \mathfrak{p})$ est un groupe fini d'ordre $f(\mathfrak{p})$.
On appelle groupe de décomposition de $\mathfrak{q}$ au dessus de $\mathfrak{p}$, noté $D(\mathfrak{q} \mid \mathfrak{p})$, le sous-groupe de G constitué des $\sigma \in G$ qui stabilisent $\mathfrak{q}$, au sens $\sigma\mathfrak{q} = \mathfrak{q}$ (ou de manière équivalente $\sigma\mathfrak{q} \subseteq \mathfrak{q}$ car ce sont des idéaux maximaux).

Proposition 7.4. *Dans le contexte précédent, le groupe $D(\mathfrak{q} \mid \mathfrak{p})$ agit par automorphismes de $A/\mathfrak{p}$-algèbre sur $B/\mathfrak{q}$. On a donc un morphisme naturel :*

$$D(\mathfrak{q} \mid \mathfrak{p}) \longrightarrow \overline{G}(\mathfrak{q} \mid \mathfrak{p}).$$

Démonstration. Si $\sigma \in D(\mathfrak{q} \mid \mathfrak{p})$, puisque $\sigma(\mathfrak{q}) = \mathfrak{q}$, le morphisme σ se factorise en un morphisme de corps $\overline{\sigma} : B/\mathfrak{q} \longrightarrow B/\mathfrak{q}$ qui est un automorphisme car σ^{-1} se factorise de la même façon. De plus $\overline{\sigma}$ fixe $A/\mathfrak{p}$ car σ fixe $\mathcal{O}_K$. Il est clair que $\sigma \mapsto \overline{\sigma}$ est un morphisme de groupes. □

Définition 7.5. *On appelle groupe d'inertie de $\mathfrak{q}$ au dessus de $\mathfrak{p}$, le noyau du morphisme $D(\mathfrak{q} \mid \mathfrak{p}) \longrightarrow \overline{G}(\mathfrak{q} \mid \mathfrak{p})$, et on le note $E(\mathfrak{q} \mid \mathfrak{p})$. De manière équivalente, $E(\mathfrak{q} \mid \mathfrak{p})$ est l'ensemble des $\sigma \in G$ tels que pour tout $x \in \mathcal{O}_L$, on a $\sigma(x) \equiv x\ [\mathfrak{q}]$.*

Remarque 7.6. Pour tout premier $\mathfrak{p}$ de A, les groupes $D(\mathfrak{q} \mid \mathfrak{p})$ avec $\mathfrak{q}$ au dessus de $\mathfrak{p}$ sont conjugués et les groupes $E(\mathfrak{q} \mid \mathfrak{p})$ avec $\mathfrak{q}$ au dessus de $\mathfrak{p}$ sont aussi conjugués : en effet l'action de G sur les premiers au dessus de $\mathfrak{p}$ est transitive et on a pour tout $\sigma \in G$ et $\mathfrak{q}$ au dessus de $\mathfrak{p}$:

$$E(\sigma\mathfrak{q} \mid \mathfrak{p}) = \sigma E(\mathfrak{q} \mid \mathfrak{p})\sigma^{-1}$$

et

$$D(\sigma\mathfrak{q} \mid \mathfrak{p}) = \sigma D(\mathfrak{q} \mid \mathfrak{p})\sigma^{-1}.$$

En particulier, si G est abélien (on dit alors que l'extension est abélienne), les groupes de décomposition et d'inertie $D(\mathfrak{q} \mid \mathfrak{p})$ et $E(\mathfrak{q} \mid \mathfrak{p})$ ne dépendent que de $\mathfrak{p}$.

Le théorème suivant est fondamental : il donne le lien entre les cardinaux des groupes G, $D(\mathfrak{q} \mid \mathfrak{p})$ et $E(\mathfrak{q} \mid \mathfrak{p})$ et les indices de ramification et d'inertie.

Théorème 7.7. *On considère toujours $\mathfrak{q}$ un premier de B au dessus de $\mathfrak{p}$ un premier de A. Pour plus de simplicité, on note simplement D le groupe de décomposition $D(\mathfrak{q} \mid \mathfrak{p})$ et on note E le groupe d'inertie $E(\mathfrak{q} \mid \mathfrak{p})$. On note aussi e pour $e(\mathfrak{p})$, f pour $f(\mathfrak{p})$ et r pour $r(\mathfrak{p})$. Enfin, la notation avec un exposant désigne l'ensemble des éléments fixés, par exemple $\mathfrak{q}^E$ est l'ensemble des éléments de $\mathfrak{q}$ fixés par E, (c'est aussi $\mathfrak{q} \cap L^E$). On a alors les indices suivants :*

$$\begin{array}{ccccc}
G & & L & \supseteq & \mathfrak{q} \\
{\scriptstyle r}\big| & & {\scriptstyle e}\big| & & {\scriptstyle e}\big\{ \\
D & & L^E & \supseteq & \mathfrak{q}^E \\
{\scriptstyle f}\big| & & {\scriptstyle f}\big| & & 1\big\{ \\
E & & L^D & \supseteq & \mathfrak{q}^D \\
{\scriptstyle e}\big| & & {\scriptstyle r}\big| & & 1\big\{ \\
1 & & K & \supseteq & \mathfrak{p}
\end{array}
\qquad
\begin{array}{c}
\\
\big|\,1 \\
\\
\big|\,f \\
\\
\big|\,1 \\
\\

\end{array}$$

Au niveau des idéaux, le trait en vague représente l'indice de ramification et le trait droit représente l'indice d'inertie.

Démonstration. Puisque L/K est galoisienne, on peut écrire :

$$\mathfrak{p}B = (\mathfrak{q}_1 \dots \mathfrak{q}_r)^e$$

avec $\mathfrak{q} = \mathfrak{q}_1$. On sait que G agit transitivement sur $\{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ (proposition 7.1) et le stabilisateur de $\mathfrak{q}$ pour cette action est D. Ainsi la formule orbite-stabilisateur donne :

$$[G : D] = r$$

Ensuite on montre que $e(\mathfrak{q} \mid \mathfrak{q}^D) = e$ et $f(\mathfrak{q} \mid \mathfrak{q}^D) = f$. Pour cela on constate que $\mathfrak{q}$ est le seul premier de B au dessus de $\mathfrak{q}^D$: en effet, $D = \mathrm{Gal}(L/L^D)$ agit transitivement sur les premiers de B au dessus de $\mathfrak{q}^D$, or il agit aussi trivialement par définition de D. Ainsi $\mathfrak{q}^D$ n'a qu'un seul idéal de B au dessus de lui et la formule des degrés 5.17 donne :

$$e(\mathfrak{q} \mid \mathfrak{q}^D) f(\mathfrak{q} \mid \mathfrak{q}^D) = [L : L^D] = |D| = |G|/r = efr/r = ef$$

d'après la proposition 7.2. Par la proposition 5.8 sur les indices dans les tours d'extensions, on a $e(\mathfrak{q} \mid \mathfrak{q}^D) \leq e$ et $f(\mathfrak{q} \mid \mathfrak{q}^D) \leq f$. Il y a donc égalité :

$$e(\mathfrak{q} \mid \mathfrak{q}^D) = e$$

et

$$f(\mathfrak{q} \mid \mathfrak{q}^D) = f.$$

Ensuite montrons que $f(\mathfrak{q} \mid \mathfrak{q}^E) = 1$. Il s'agit de montrer que l'extension $B^E/\mathfrak{q}^E \subseteq B/\mathfrak{q}$ est triviale. Soit $\alpha \in B$. On considère le polyôme :

$$g(X) = \prod_{\sigma \in E} (X - \sigma\alpha) \in B[X]$$

Le polynôme g est fixé par l'action de E donc ses coefficients aussi et donc $g \in B^E[X]$. On note $\overline{g}$ la réduction de g dans $B/\mathfrak{q}[X]$ de sorte que :

$$\overline{g} = (X - \overline{\alpha})^{|E|}$$

car tous les $\sigma\alpha$ sont congrus à α modulo $\mathfrak{q}$ (pour $\sigma \in E$). Le polynôme $\overline{g}$ est alors un polynôme à coefficients dans $B^E/\mathfrak{q}^E$, non nul, qui annule $\overline{\alpha}$. Le polynôme minimal de $\overline{\alpha}$ pour l'extension $B/\mathfrak{q} \supseteq B^E/\mathfrak{q}^E$ divise $\overline{g}$ et est séparable car l'extension est séparable, donc c'est $X - \overline{\alpha}$ et $\overline{\alpha} \in B^E/\mathfrak{q}^E$ comme souhaité.
Obervons à présent que l'on a une suite exacte :

$$1 \longrightarrow E \longrightarrow D \longrightarrow \overline{G}$$

et donc $[D : E] \leq \left|\overline{G}\right| = f$. Par correspondance de Galois $[L^E : L^D] \leq f$, or $e(\mathfrak{q}^E \mid \mathfrak{q}^D) f(\mathfrak{q}^E \mid \mathfrak{q}^D) = [L^E : L^D]$ car $\mathfrak{q}^D$ n'a qu'un seul premier au dessus de lui dans L^E (car il n'en a qu'un seul dans L). Mais $f = f(\mathfrak{q} \mid \mathfrak{q}^D) = f(\mathfrak{q} \mid \mathfrak{q}^E) f(\mathfrak{q}^E \mid \mathfrak{q}^D) = f(\mathfrak{q}^E \mid \mathfrak{q}^D)$ car $f(\mathfrak{q} \mid \mathfrak{q}^E) = 1$. Donc $e(\mathfrak{q}^E \mid \mathfrak{q}^D) f \leq f$ et cela impose :

$$e(\mathfrak{q}^E \mid \mathfrak{q}^D) = 1$$

On peut alors finir de compléter tous les indices à l'aide de la correspondance de Galois et de la proposition 5.8. □

On en déduit une formule qui relie la norme d'un idéal fractionnaire au produit de ses conjugués.

Corollaire 7.8. *Pour tout idéal fractionnaire I de B, on a :*

$$\prod_{\sigma\in G}\sigma I = \|I\|_{B/A}\, B$$

Démonstration. On a :

$$\begin{aligned}\|I\|_{B/A}\, B &= \prod_{\mathfrak{p}} (\mathfrak{p}B)^{\left(\sum_{\mathfrak{q}\supseteq\mathfrak{p}} f(\mathfrak{p})v_{\mathfrak{q}}(I)\right)} = \prod_{\mathfrak{p}}\left(\prod_{\mathfrak{q}\supseteq\mathfrak{p}}\mathfrak{q}^{e(\mathfrak{p})}\right)^{\left(\sum_{\mathfrak{q}\supseteq\mathfrak{p}} f(\mathfrak{p})v_{\mathfrak{q}}(I)\right)}\\ &= \prod_{\mathfrak{p}}\prod_{\mathfrak{q}\supseteq\mathfrak{p}}\mathfrak{q}^{\left(\sum_{\mathfrak{q}'\supseteq\mathfrak{p}} e(\mathfrak{p})f(\mathfrak{p})v_{\mathfrak{q}'}(I)\right)}\end{aligned}$$

Or on a :

$$\sum_{\sigma\in G} v_{\sigma(\mathfrak{q})}(I) = \sum_{\mathfrak{q}'\supseteq\mathfrak{q}} v_{\mathfrak{q}'}(I)\,|D(\mathfrak{q}:\mathfrak{p})| = \sum_{\mathfrak{q}'\supseteq\mathfrak{p}} e(\mathfrak{p})f(\mathfrak{p})v_{\mathfrak{q}'}(I)$$

car G agit transitivement sur les premiers au dessus de $\mathfrak{p}$ et le stabilisateur de $\mathfrak{q}$ pour cette action est $D(\mathfrak{q}:\mathfrak{p})$. On en déduit :

$$\begin{aligned}\|I\|_{B/A}\, B &= \prod_{\mathfrak{p}}\prod_{\mathfrak{q}\supseteq\mathfrak{p}}\mathfrak{q}^{\left(\sum_{\sigma\in G} v_{\sigma(\mathfrak{q})}(I)\right)} = \prod_{\mathfrak{q}}\mathfrak{q}^{\left(\sum_{\sigma\in G} v_{\sigma(\mathfrak{q})}(I)\right)} = \prod_{\mathfrak{q}}\prod_{\sigma\in G}\mathfrak{q}^{v_{\sigma(\mathfrak{q})}(I)}\\ &= \prod_{\mathfrak{q}}\prod_{\sigma\in G}(\sigma(\mathfrak{q}))^{v_{\mathfrak{q}}(I)} = \prod_{\sigma\in G}\sigma(I).\end{aligned}$$

□

Enfin, le corollaire suivant permet de construire des éléments du groupe de Galois. On en verra un cas particulier fondamental dans la suite (théorème 7.15).

Corollaire 7.9. *On a une suite exacte :*

$$0 \longrightarrow E(\mathfrak{q}\mid\mathfrak{p}) \longrightarrow D(\mathfrak{q}\mid\mathfrak{p}) \longrightarrow \overline{G}(\mathfrak{q}\mid\mathfrak{p}) \longrightarrow 1$$

Dans le cas où A est localement fini (i.e. les corps résiduels de A, mis à part le corps des fractions de A, sont finis), l'extension résiduelle est une extension finie de corps finis et donc $D(\mathfrak{q}\mid\mathfrak{p})/E(\mathfrak{q}\mid\mathfrak{p})$ est un groupe cyclique d'ordre $f(\mathfrak{p})$. Un générateur de cette extension est donné par le Frobenius $x\mapsto x^{|A/\mathfrak{p}|}$.

Démonstration. Il suffit de montrer que $D\longrightarrow\overline{G}$ est surjective, mais on a $|D| = ef = |E|\times\left|\overline{G}\right|$ donc c'est bien surjectif. □

7.2 Spécialisation du groupe de Galois et symbole d'Artin

On considère toujours B/A une extension de Dedekind galoisienne de corps des fractions L/K et de groupe de Galois G, avec A localement parfait. On reformule le théorème 7.7 et son corollaire 7.9 dans le cas d'un premier $\mathfrak{p}$ *non ramifié* de A.

Théorème 7.10. *Soit $\mathfrak{p}$ un premier de A et $\mathfrak{q}$ un premier de B au dessus de $\mathfrak{p}$. Si $\mathfrak{p}$ n'est pas ramifié dans B, alors on a $E(\mathfrak{q} \mid \mathfrak{p}) = \{\mathrm{id}\}$ et donc :*

$$G \supseteq D(\mathfrak{q} \mid \mathfrak{p}) \cong \overline{G}(\mathfrak{q} \mid \mathfrak{p})$$

et ainsi, dans le cas où A est localement fini (5.38), G contient un élément d'ordre $f(\mathfrak{p})$ qui agit comme $x \mapsto x^{|A/\mathfrak{p}|}$ modulo $\mathfrak{q}$, avec p le seul nombre premier contenu dans $\mathfrak{p}$. Un tel élement est appelé Frobenius modulo $\mathfrak{p}$.
Enfin on a les indices suivants (avec les mêmes conventions que pour le théorème 7.7) :

$$\begin{array}{ccccc} G & & L & \supseteq & \mathfrak{q} \\ {\scriptstyle r}\big| & & {\scriptstyle f}\big| & & e\big\{\ \big|f \\ D & & L^D & \supseteq & \mathfrak{q}^D \\ {\scriptstyle f}\big| & & {\scriptstyle r}\big| & & 1\big\{\ \big|1 \\ 1 & & K & \supseteq & \mathfrak{p} \end{array}$$

Démonstration. Cela découle directement de 7.7 et de 7.9 puisqu'on a $e = 1$ et $E = \{1\}$. □

Définition 7.11. *Dans le cas où A est localement fini (5.38) et $\mathfrak{p}$ n'est pas ramifié, pour $\mathfrak{q}$ au dessus de $\mathfrak{p}$, le Frobenius modulo $\mathfrak{p}$ est noté :*

$$\left(\frac{B/A}{\mathfrak{q}}\right) \in G.$$

C'est un élément de G d'ordre $f(\mathfrak{q} \mid \mathfrak{p})$.

Voyons tout de suite une application de ce concept.

Proposition 7.12. *Supposons A localement fini. S'il existe un premier $\mathfrak{p}$ de A inerte dans B (au sens où $\mathfrak{p}A$ est un premier de B), alors l'extension L/K est cyclique.*

Démonstration. Un tel premier n'est pas ramifié donc ce qui précède s'applique, et on a d'ailleurs $r(\mathfrak{p}) = 1$ (il n'y a qu'un seul premier au dessus de $\mathfrak{p}$) donc $f(\mathfrak{p}) = [L : K]$ par la formule $ref = [L : K]$ (5.17) et ainsi le Frobenius modulo $\mathfrak{p}$ engendre le groupe de Galois de L/K. □

Proposition 7.13. *On suppose A localement fini. Soit $\mathfrak{p}$ un premier non ramifié. Les Frobenius $\left(\frac{B/A}{\mathfrak{q}}\right)$ avec $\mathfrak{q}$ au dessus de $\mathfrak{p}$ forment une classe de conjugaison dans G. Plus précisément, on a pour tout $\sigma \in G$ et tout $\mathfrak{q}$ au dessus de $\mathfrak{p}$:*

$$\left(\frac{B/A}{\sigma\mathfrak{q}}\right) = \sigma\left(\frac{B/A}{\mathfrak{q}}\right)\sigma^{-1}.$$

Démonstration. D'après la remarque 7.6 :

$$D(\sigma\mathfrak{q} \mid \mathfrak{p}) = \sigma D(\mathfrak{q} \mid \mathfrak{p})\sigma^{-1}$$

et on a pour tout $x \in B$:

$$\left(\frac{B/A}{\mathfrak{q}}\right)(x) \equiv x^{|A/\mathfrak{p}|} \ [\mathfrak{q}]$$

donc :

$$\sigma\left(\frac{B/A}{\mathfrak{q}}\right)\sigma^{-1}(x) \equiv x^{|A/\mathfrak{p}|} \ [\sigma\mathfrak{q}]$$

et par injectivité de $D(\sigma\mathfrak{q} \mid \mathfrak{p}) \longrightarrow \overline{G}(\mathfrak{q} \mid \mathfrak{p})$, on a donc nécessairement :

$$\sigma\left(\frac{B/A}{\mathfrak{q}}\right)\sigma^{-1} = \left(\frac{B/A}{\sigma\mathfrak{q}}\right).$$

Puisque G agit transitivement sur les premiers au dessus de $\mathfrak{q}$, on a bien le résultat voulu. □

Définition 7.14. *On suppose A localement fini. Soit $\mathfrak{p}$ un premier non ramifié. Les Frobenius $\left(\frac{B/A}{\mathfrak{q}}\right)$ pour $\mathfrak{q}$ au dessus de $\mathfrak{p}$ forment une classe de conjugaison de G et s'envoie donc sur un seul élément de l'abélianisé G^{ab}, que l'on note avec le symbole d'Artin :*

$$\left(\frac{B/A}{\mathfrak{p}}\right) \in G^{ab}$$

Dans le cas où G est abélien, cela définit un élément de G.
On étend le symbole d'Artin par linéarité pour définir un morphisme de groupes $\left(\frac{B/A}{\bullet}\right)$:

$$\mathcal{F}(A)_0^{\times} \longrightarrow G^{ab}$$

où $\mathcal{F}(A)_0^{\times}$ désigne le groupe des idéaux fractionnaires non nuls de A pour lesquels les premiers apparaissant dans leur décomposition en facteurs premiers sont non ramifiés.

Voyons tout de suite une application frappante du symbole d'Artin pour calculer des groupes de Galois.

Théorème 7.15. *(Spécialisation du groupe de Galois) On suppose A localement fini. Soit P un polynôme unitaire à coefficients dans A, et $\mathfrak{p}$ un premier de A tel que P est séparable modulo $\mathfrak{p}$ (i.e. dans le corps $A/\mathfrak{p}$). On note G le groupe de Galois de P, c'est à dire le groupe de Galois du corps de décomposition de P sur K. G est naturellement vu comme un sous-groupe du groupe des permutations des racines de P dans le corps de décomposition. La réduction $\overline{P}$ de P modulo $\mathfrak{p}$ se factorise en produit d'irréductibles :*

$$\overline{P} = \prod_{i=1}^{s} P_i$$

avec les P_i deux à deux distincts.
Le premier $\mathfrak{p}$ est alors non ramifié dans le corps de décomposition L de P et pour tout

$\mathfrak{q}$ *au dessus de* $\mathfrak{p}$ *dans le corps de décomposition, le Frobenius* $\left(\frac{B/A}{\mathfrak{q}}\right)$ *est de type cyclique* $(\deg P_1, \deg P_2, \ldots, \deg P_s)$ *dans le groupe symétrique.*
De plus, si $x_1, \ldots, x_d$ *sont les racines de* P *dans* L*, et si* B *est la clôture normale de* A *dans* L*, on a :*

$$B_{\mathfrak{p}} = A[x_1, \ldots, x_d]_{\mathfrak{p}}.$$

Démonstration. Notons L un corps de décomposition de P sur K et B la clôture intégrale de A dans L de sorte que B/A est une extension de Dedekind galoisienne de groupe G. On factorise P dans $K[X]$:

$$P = \prod_i (X - x_i).$$

Notons que les x_i sont distincts car, P étant séparable modulo $\mathfrak{p}$, il est séparable. On choisit ensuite $\mathfrak{q}$ un premier de B au dessus de $\mathfrak{p}$. Puisque P est séparable modulo $\mathfrak{p}$, la réduction $B \longrightarrow B/\mathfrak{q}$ induit une bijection entre l'ensemble $V(P)$ des racines de P et l'ensemble $V(\overline{P})$ des racines de $\overline{P}$ dans $B/\mathfrak{q}$.
Cette bijection est compatible à l'action du groupe $D(\mathfrak{q} \mid \mathfrak{p})$ et fournit donc un isomorphisme de $D(\mathfrak{q} \mid \mathfrak{p})$-ensembles.
On a donc un diagramme commutatif :

$$\begin{array}{ccc} D(\mathfrak{q} \mid \mathfrak{p}) & \twoheadrightarrow & \overline{G}(\mathfrak{q} \mid \mathfrak{p}) \\ \downarrow & & \downarrow \\ \mathfrak{S}_{V(P)} & \xrightarrow{\sim} & \mathfrak{S}_{V(\overline{P})} \end{array}$$

qui assure l'injectivité de $D(\mathfrak{q} \mid \mathfrak{p}) \longrightarrow \overline{G}(\mathfrak{q} \mid \mathfrak{p})$ et donc $E(\mathfrak{q} \mid \mathfrak{p}) = 1$ et $\mathfrak{p}$ n'est pas ramifié.
Pour tout i, le groupe de Galois $\overline{G}(\mathfrak{q} \mid \mathfrak{p})$ agit transitivement sur les racines de P_i car P_i est irréductible.
En particulier le Frobenius qui le génère agit transitivement sur les racines de chaque P_i et donc son type cylique est $(\deg P_1, \deg P_2, \ldots, \deg P_s)$. C'est donc aussi le cas pour $\left(\frac{B/A}{\mathfrak{q}}\right)$. □

Remarque 7.16. Sans changer la preuve, on peut même supposer simplement que P est à coefficients dans $A_{\mathfrak{p}}$ plutôt que dans A.

7.3 Factorisation dans un compositum

Remarque 7.17. Si C/A est une extension de Dedekind de corps de fractions M/K et si L est un corps intermédiaire, alors $B = C \cap L$ est la clôture intégrale de A dans L, faisant de $C/B/A$ une tour d'extensions de Dedekind.

Proposition 7.18. *Soit* $C/B/A$ *une tour d'extensions de Dedekind de corps de fractions* $M/L/K$*, avec* A *localement parfait. On suppose* M/K *galoisienne de groupe de Galois* G*. Soit* $\mathfrak{q}$ *un premier de* C *au dessus de* $\mathfrak{p}$ *un premier de* A*. On a alors les équivalences suivantes :*

— *Le corps* L *est contenu dans* $M^{D(\mathfrak{q}|\mathfrak{p})}$ *si et seulement si* $e(\mathfrak{q} \cap L \mid \mathfrak{p}) = f(\mathfrak{q} \cap L \mid \mathfrak{p}) = 1$.

— *Le corps L est contenu dans $M^{E(\mathfrak{q}|\mathfrak{p})}$ si et seulement si $e(\mathfrak{q} \cap L \mid \mathfrak{p}) = 1$.*

Démonstration. On renvoie au théorème 7.7 pour les notations. Si $L \subseteq M^E$, alors on a $1 = e(\mathfrak{q}^E \mid \mathfrak{p}) = e(\mathfrak{q}^E \mid \mathfrak{q} \cap L)e(\mathfrak{q} \cap L \mid \mathfrak{p})$ donc $e(\mathfrak{q} \cap L \mid \mathfrak{p}) = 1$. Si $e(\mathfrak{q} \cap L \mid \mathfrak{p}) = 1$, on peut considérer l'extension galoisienne de Dedekind C/B et le groupe d'inertie de $\mathfrak{q}$ au dessus de $\mathfrak{q} \cap L$ dans cette extension :

$$E(\mathfrak{q} \mid \mathfrak{q} \cap L) = \{\sigma \in \mathrm{Gal}(M/L) \mid \sigma\mathfrak{q} = \mathfrak{q} \text{ et } \forall x \in C\ \sigma x - x \in \mathfrak{q}\} = \mathrm{Gal}(M/L) \cap E(\mathfrak{q} \mid \mathfrak{p}).$$

Or $|E(\mathfrak{q} \mid \mathfrak{q} \cap L)| = e(\mathfrak{q} \mid \mathfrak{q} \cap L) = e(\mathfrak{q} \mid \mathfrak{p}) = |E(\mathfrak{q} \mid \mathfrak{p})|$ car $e(\mathfrak{q} \cap L \mid \mathfrak{p}) = 1$. Ainsi :

$$E(\mathfrak{q} \mid \mathfrak{p}) = E(\mathfrak{q} \mid \mathfrak{q} \cap L) \subseteq \mathrm{Gal}(M/L)$$

donc $L \subseteq M^E$.
Le raisonnement est le même pour le groupe D. Il s'agit de constater que :

$$D(\mathfrak{q} \mid \mathfrak{q} \cap L) = \mathrm{Gal}(M/L) \cap D$$

et ainsi, si $e(\mathfrak{q} \cap L \mid \mathfrak{p}) = f(\mathfrak{q} \cap L \mid \mathfrak{p}) = 1$, les groupes D et $D(\mathfrak{q} \mid \mathfrak{q} \cap L)$ ont le même cardinal ef et l'un est inclus dans l'autre donc ils sont égaux, et donc $D \subseteq \mathrm{Gal}(M/L)$ et $L \subseteq M^D$. □

Corollaire 7.19. *Soit C/A une extension de Dedekind avec A localement parfait, de corps des fractions M/K, et soient L_1, L_2 des extensions intermédiaires telles que :*

$$L_1 L_2 = M.$$

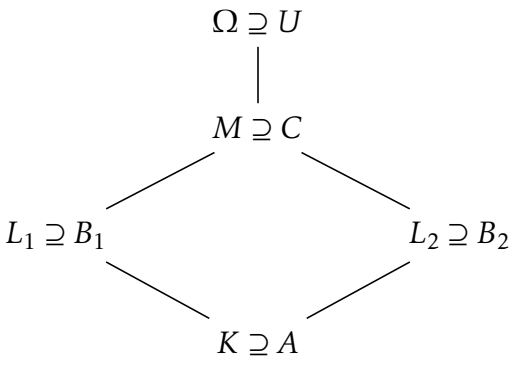
On note B_1 et B_2 les anneaux de Dedekind correspondant : $B_1 = C \cap L_1$ et $B_2 = C \cap L_2$. Soit $\mathfrak{q}$ un premier de C au dessus de $\mathfrak{p}$ un premier de A. On note $\mathfrak{q}_i = \mathfrak{q} \cap B_i$. On a alors les équivalences suivantes :

— *$\mathfrak{q} \mid \mathfrak{p}$ est non ramifié si et seulement si les $\mathfrak{q}_i \mid \mathfrak{p}$ sont non ramifiés.*

— *$\mathfrak{q} \mid \mathfrak{p}$ a pour indices d'inertie et de ramification 1 si et seulement si $e(\mathfrak{q}_i \mid \mathfrak{p}) = f(\mathfrak{q}_i \mid \mathfrak{p}) = 1$ pour chaque i.*

En particulier, $\mathfrak{p}$ est non ramifié dans C si et seulement si il est non ramifié dans chaque B_i et $\mathfrak{p}$ est totalement décomposé (i.e. les indices d'inertie et de ramification des premiers au dessus de $\mathfrak{p}$ valent 1) si et seulement si $\mathfrak{p}$ est totalement décomposé dans chaque B_i.

Démonstration. On choisit Ω une extension galoisienne de M et on note U la clôture intégrale de C dans Ω. On choisit ensuite $\mathfrak{r}$ un premier de Ω au dessus de $\mathfrak{q}$.



On a alors, d'après la proposition précédente 7.18 et puisque $M = L_1 L_2$:

$$e(\mathfrak{q} \mid \mathfrak{p}) = 1 \iff M \subseteq \Omega^{E(\mathfrak{r}|\mathfrak{p})} \iff L_1 \subseteq \Omega^{E(\mathfrak{r}|\mathfrak{p})} \text{ et } L_2 \subseteq \Omega^{E(\mathfrak{r}|\mathfrak{p})} \iff \forall i \; e(\mathfrak{q}_i \mid \mathfrak{p}) = 1$$

et la preuve est similaire pour la deuxième équivalence, en utilisant le corps $\Omega^{D(\mathfrak{r}|\mathfrak{p})}$. □

Le corollaire suivant permet de décider de la ramification ou de la totale décomposition d'un premier dans la clôture normale d'une extension.

Corollaire 7.20. *Soit B/A une extension de Dedekind de corps de fractions L/K avec A localement parfait. Soit M une clôture normale de L, c'est à dire une extension finie normale de L engendrée par les images de L par les éléments de $\mathrm{Gal}(M//K)$ (par exemple, si Ω est une clôture algébrique de L on peut considérer le compositum dans Ω des $\sigma(L)$ avec $\sigma \in \mathrm{Hom}_K(L, \Omega)$). On note C la clôture intégrale de A dans M de sorte que C/A est une extension de Dedekind galoisienne.*
Soit $\mathfrak{p}$ un premier de A. Alors $\mathfrak{p}$ est ramifié dans B si et seulement si il l'est dans C.
De plus $\mathfrak{p}$ est totalement décomposé dans B si et seulement si il l'est dans C.
En particulier, $\mathcal{D}_{C/A}$ et $\mathcal{D}_{B/A}$ ont les mêmes diviseurs premiers.

Démonstration. Notons que M/K est encore séparable car M s'obtient comme corps de décomposition d'un polynôme séparable en appliquant le théorème de l'élément primitif à L/K. C'est une application directe de 7.19 (qui s'applique aussi à un compositum d'un nombre fini d'extensions avec la même preuve).
En effet on utilise que :

$$M = \prod_{\sigma \in \mathrm{Gal}(M/K)} \sigma(L)$$

où la notation produit désigne un compositum. On utilise aussi le fait que pour tout σ, les extensions de Dedekind B/A et $\sigma B/A$ sont isomorphes et donc $\mathfrak{p}$ est ramifié (resp. totalement décomposé) dans l'une si et seulement si il l'est dans l'autre.
La remarque sur les diviseurs premiers des discriminants provient du théorème de Dedekind 5.41. □

7.4 Théorème 90 de Hilbert pour les idéaux

Définition 7.21. *Un idéal fractionnaire J de B est dit divisible si pour tout $\mathfrak{q} \supseteq \mathfrak{p}$, on a :*

$$e(\mathfrak{q} \mid \mathfrak{p}) \mid v_{\mathfrak{q}}(J)$$

Ces idéaux forment un sous-groupe $\mathcal{F}(B)^{\times}_{\mathrm{div}} \subseteq \mathcal{F}(B)^{\times}$.

Proposition 7.22. *En général, même si L/K n'est pas supposée normale, l'application :*

$$\mathcal{F}(A)^{\times} \longrightarrow \mathcal{F}(B)^{\times}$$

donnée par $I \mapsto IB$ est injective. Dans le cas où L/K est galoisienne, son image est le sous-groupe des idéaux fractionnaires divisibles de B fixés par l'action de G sur ldes idéaux fractionnaires :

$$\mathcal{F}(A)^{\times} \cong \left(\mathcal{F}(B)^{\times}_{\mathrm{div}}\right)^{G}.$$

Démonstration. C'est injectif puisque si $IB = B$, alors pour tout premier $\mathfrak{p}$ et tout premier $\mathfrak{q}$ au dessus de $\mathfrak{p}$:

$$0 = v_{\mathfrak{q}}(IB) = v_{\mathfrak{p}}(I)e(\mathfrak{q} \mid \mathfrak{p})$$

donc $v_{\mathfrak{p}}(I) = 0$ puisqu'il existe toujours au moins un premier au dessus de $\mathfrak{p}$. La formule précédente montre aussi que l'image d'un idéal fractionnaire de A est toujours divisible.
Supposons maintenant L/K galoisienne. Clairement, pour tout $I \in \mathcal{F}(A)^\times$ et tout $g \in G$, on a $gI = I$ donc $gIB = IB$.
Réciproquement, soit $J \in \mathcal{F}(B)^\times$ divisible fixé par l'action de G. Pour tout $\mathfrak{p}$ premier, tout $\mathfrak{q}$ au dessus de $\mathfrak{p}$ et tout $g \in G$, on a alors :

$$v_{\mathfrak{q}}(J) = v_{\mathfrak{q}}(g^{-1}J) = v_{g\mathfrak{q}}(J)$$

donc par transitivité de l'action de G sur les premiers au dessus de $\mathfrak{p}$, les valuations $\mathfrak{q}$-adiques de J pour $\mathfrak{q}$ au dessus de $\mathfrak{p}$ sont toutes égales à un nombre $w_{\mathfrak{p}}e(\mathfrak{p})$ car J est divisible. On pose alors :

$$I = \prod_{\mathfrak{p}} \mathfrak{p}_{\mathfrak{p}}^{w}$$

et on a bien $IB = J$. □

On prouve le théorème suivant, analogue à 2.28 mais plus facile à démontrer car on dispose de la factorisation en produit de premiers.

Théorème 7.23. *(Hilbert 90 pour les idéaux) On suppose L/K cyclique d'ordre n et on note σ un générateur de G. On a une suite exacte :*

$$1 \longrightarrow (\mathcal{F}(B)^\times)^G \longrightarrow \mathcal{F}(B)^\times \xrightarrow{\sigma/\mathrm{id}} \mathcal{F}(B)^\times \xrightarrow{\|\bullet\|_{B/A}} \mathcal{F}(A)^\times$$

où la flèche σ/id est définie par $I \mapsto \sigma(I)I^{-1}$.

Démonstration. Le seul point qui mérite un argument est le suivant : étant donné un idéal fractionnaire J de B de norme triviale, on souhaite trouver un idéal fractionnaire I de B tel que :

$$J = \sigma(I)I^{-1}$$

ce qui se traduit en un problème d'algèbre linéaire sur le groupe abélien libre $\mathcal{F}(B)^\times$. On a en effet :

$$\|J\|_{B/A}\, B = B$$

et ainsi, par le corollaire 7.8 :

$$\prod_{g \in G} gJ = B$$

donc pour tout premier $\mathfrak{p}$, en choisissant $\mathfrak{q}(\mathfrak{p})$ un premier quelconque au dessus de $\mathfrak{p}$:

$$\sum_{g \in G} v_{g\mathfrak{q}(\mathfrak{p})}(J) = 0.$$

On note alors Q l'ensemble des $G\cdot\mathfrak{q}(\mathfrak{p})$ des premiers au dessus de $\mathfrak{p}$, et on a, en divisant l'égalité précédente par $r(\mathfrak{p})$:

$$\sum_{\mathfrak{q}\in Q} v_{\mathfrak{q}}(J) = 0$$

Ce qui va permettre de trouver une "primitve" à la suite des $v_{\mathfrak{q}}(J)$ (de la même façon qu'une fonction périodique continue de moyenne nulle admet une primitive périodique). Mettons cela en oeuvre : on définit un idéal fractionnaire I de la façon suivante :

$$I = \prod_{\mathfrak{p}} \prod_{k=0}^{r(\mathfrak{p}-1)} (\sigma^k \mathfrak{q}(\mathfrak{p}))^{v_{\mathfrak{p},k}}$$

avec :

$$v_{\mathfrak{p},k} = \sum_{i=0}^{k-1} v_{\sigma^k \mathfrak{q}(\mathfrak{p})}(J)$$

et on laisse au lecteur le soin de vérifier que :

$$\sigma^{-1}(I)I^{-1} = J$$

et quitte à remplacer σ par σ^{-1} dans notre choix de générateur, on obtient ce qu'on souhaitait. □

Chapitre 8

Corps cyclotomiques

> Si un polygone régulier possède n côtés et si n est une puissance de 2 ou est le produit d'une puissance de 2 et de k nombres de Fermat premiers différents alors ce polygone est constructible.
>
> Carl Friedrich Gauss,
> Disquisitiones arithmeticae

Un corps cyclotomique est une extension de $\mathbb{Q}$ engendrée par une racine de l'unité. De façon équivalente, c'est un corps de la forme $\mathbb{Q}(\mathbb{U}_n)$ avec $n \geq 1$ un entier, et $\mathbb{U}_n$ le groupe des racines n-èmes de l'unité. Dans la suite, φ désigne l'indicatrice d'Euler. On note aussi $m \wedge n$ le pgcd et $m \vee n$ le ppcm de deux entiers m et n. On rappelle que φ est multiplicative, au sens où si m et n sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.
Dans ce chapitre, on souhaite décrire le groupe de Galois des corps cyclotomiques, donner la forme de l'anneau des entiers d'un tel corps et étudier la factorisation des nombres premiers dans une extension cyclotomique.
On retrouvera le résultat bien connu selon lequel les polynômes cyclotomiques sont irréductibles, autrement dit que $[\mathbb{Q}(\mathbb{U}_n) : \mathbb{Q}] = \varphi(n)$, par une simple application de la spécialisation du groupe de Galois (via le théorème 7.15).

8.1 Polynômes cyclotomiques

Définition 8.1. *Soit $n \geq 1$. On définit le n-ème polynôme cyclotomique sur $\mathbb{Q}$ comme :*

$$\Phi_n = \prod_{\langle\omega\rangle = \mathbb{U}_n} (X - \omega)$$

où le produit porte sur les $\varphi(n)$ générateurs du groupe $\mathbb{U}_n$. Ainsi :

$$\deg \Phi_n = \varphi(n).$$

Proposition 8.2. *Le n-ème polynôme cyclotomique Φ_n est unitaire et à coefficients entiers.*

Démonstration. Il est clairement unitaire, et on a :

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{d|n} \prod_{\langle \omega \rangle = \mathbb{U}_d} (X - \omega) = \prod_{d|n} \Phi_d \quad (*)$$

ce qui donne, par inversion de Möbius :

$$\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(d)}$$

avec μ la fonction de Möbius, et ceci montre que Φ_n est à coefficients rationnels. Sans utiliser la fonction de Möbius, la formule $(*)$ permet aussi de montrer par récurrence forte que Φ_n est à coefficients rationnels.
De plus, Φ_n est à coefficients dans $\overline{\mathbb{Z}}$ car les racines de l'unité sont des entiers algébriques (ce sont des racines de $X^n - 1$).
Puisque $\mathbb{Z}$ est intégralement clos, Φ_n est bien à coefficients entiers. □

Exemple 8.3. *Par exemple, si p est premier :*

$$\Phi_p = \prod_{\omega \in \mathbb{U}_p \setminus \{1\}} (X - \omega) = \frac{X^p - 1}{X - 1} = 1 + X + \cdots + X^{p-1}$$

et pour tout $k \geq 1$:

$$\Phi_{p^k} = \prod_{\omega \in \mathbb{U}_{p^k} \setminus \mathbb{U}_{p^{k-1}}} (X - \omega) = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \Phi_p(X^{p^{k-1}}).$$

Dans ce cas, le critère d'Eisenstein pour le nombre premier p appliqué à $\Phi_{p^k}(X - 1)$ permet d'obtenir l'irréductibilité sur $\mathbb{Q}$ de Φ_{p^k}. En général, cette méthode ne marche pas et on va avoir recours à la spécialisation du groupe de Galois pour l'obtenir.

8.2 Groupe de Galois des corps cyclotomiques et irréductibilité des polynômes cyclotomiques

Un corps cyclotomique est toujours une extension finie galoisienne de $\mathbb{Q}$ puisque c'est le corps de décomposition du polynôme séparable $X^n - 1$.
On va calculer le groupe de Galois du corps cyclotomique $\mathbb{Q}(\mathbb{U}_n)$, et on verra qu'il est de cardinal $\varphi(n)$, ce qui entraînera l'irréductibilité de Φ_n.

Théorème 8.4. *Soit $n \geq 1$. On note K le n-ème corps cyclotomique $\mathbb{Q}(\mathbb{U}_n)$ et $G = \mathrm{Gal}(K/\mathbb{Q})$. Le groupe G agit sur $\mathbb{U}_n$ par automorphismes de groupes, induisant un isomorphisme de groupes :*

$$G \cong \mathrm{Aut}(\mathbb{U}_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

En particulier $[K : \mathbb{Q}] = \varphi(n)$ et Φ_n est irréductible sur $\mathbb{Q}$. C'est donc le polynôme minimal de n'importe quelle racine n-ème de l'unité.

Démonstration. Il est clair que G agit sur $\mathbb{U}_n$ car c'est l'ensemble des racines de $X^n - 1$. L'action est fidèle car ces racines engendrent K. On a donc un morphisme canonique injectif :

$$G \hookrightarrow \mathrm{Aut}(\mathbb{U}_n)$$

et il s'agit de voir que c'est un isomorphisme. Notons que l'on a un isomorphisme de groupes canonique :

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}(\mathbb{U}_n)$$

qui envoie k sur l'automorphisme $z \mapsto z^k$ car $\mathbb{U}_n$ est un groupe cyclique.
Pour montrer que $G \longrightarrow \mathrm{Aut}(\mathbb{U}_n) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ est surjectif, il suffit de montrer que l'image contient les classes des nombres premiers p qui ne divisent pas n, car ceci génèrent le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ (en effet, si $a \wedge n = 1$, a se décompose en produit de nombres premiers qui ne divisent pas n).
Pour cela, on utilise le théorème 7.15 pour construire un Frobenius modulo p : si $p \nmid n$, $X^n - 1$ est séparable modulo p et puisque $\Phi_n \mid X^n - 1$, le polynôme Φ_n est aussi séparable modulo p.
On en déduit, par le théorème 7.15, qu'il existe un Frobenius modulo p : un élément $\sigma \in G$, tel que :

$$\sigma(x) \equiv x^p \ [\mathfrak{p}]$$

pour tout $x \in K$ et pour $\mathfrak{p}$ un premier quelconque de K au dessus de p. On contemple alors le diagramme commutatif suivant :

$$\begin{array}{ccccc} G & \xhookrightarrow{\ i\ } & \mathrm{Aut}(\mathbb{U}_n) & \xrightarrow[\sim]{\ \eta\ } & (\mathbb{Z}/n\mathbb{Z})^\times \\ & & \downarrow{\scriptstyle \sim}{\scriptstyle r} & & \| \\ & & \mathrm{Aut}(\mathbb{U}_n(\mathcal{O}_K/\mathfrak{p})) & \xrightarrow[\eta]{\ \sim\ } & (\mathbb{Z}/n\mathbb{Z})^\times \ni p \end{array}$$

où la restriction r provient de l'isomorphisme $\mathbb{U}_n \longrightarrow \mathbb{U}_n(\mathcal{O}_K/\mathfrak{p})$ obtenu par réduction modulo $\mathfrak{p}$ (c'est un isomorphisme car $X^n - \overline{1} = \prod_{\omega \in \mathbb{U}_n(\mathcal{O}_K/\mathfrak{p})}(X - \omega) = \overline{X^n - 1} = \prod_{\omega \in \mathbb{U}_n}(X - \overline{\omega})$ dans $\mathcal{O}_K/\mathfrak{p}[X]$). L'élément σ assure que p est dans l'image de $\eta \circ r \circ i$, donc dans l'image de $\eta \circ i$, comme voulu. Ainsi i est un isomorphisme, et si ω est une racine primitive n-ème de l'unité, on a donc :

$$\deg \pi_\omega = [\mathbb{Q}(\omega) : \mathbb{Q}] = [K : \mathbb{Q}] = |G| = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \varphi(n) = \deg \Phi_n$$

et $\pi_\omega \mid \Phi_n$ donc :

$$\pi_\omega = \Phi_n$$

et Φ_n est irréductible. □

Grâce à ça on peut déterminer exactement l'ensemble des racines de l'unité présentes dans un corps cyclotomique.

Proposition 8.5. *Soit $n \geq 1$ et K le n-ème corps cyclotomique. L'ensemble des racines de l'unité présentes dans K est exactement $\mathbb{U}_{2n}$ si n est impair et $\mathbb{U}_n$ si n est pair.*

Démonstration. Notons ℓ le nombre de racines de l'unité présentes dans K. Naturellement, on a $\mathbb{Q}(\mathbb{U}_\ell) \subseteq K$ et puisque $\mathbb{U}_n \subseteq \mathbb{U}_\ell$, on a aussi $K \subseteq \mathbb{Q}(\mathbb{U}_\ell)$. Les corps cyclotomiques K et $K' = \mathbb{Q}(\mathbb{U}_\ell)$ sont donc égaux. On a donc $\varphi(\ell) = \varphi(n)$. En décomposant ℓ et n en facteurs premiers et en utilisant que $n \mid \ell$ et que φ est multiplicative, on obtient que $\ell \mid 2n$ si n est impair et que $\ell = n$ si n est pair. On note alors que si n est impair, on a -1 d'ordre 2 dans $K^\times$ et on a un élément d'ordre n donc on a aussi un élément d'ordre $2n$ puisque 2 et n sont premiers entre eux : ainsi $\ell = 2n$. □

8.3 Compositums et intersections de corps cyclotomiques

La première application que l'on donne de l'irréductibilité des polynômes cyclotomiques (théorème 8.4) est la description des intersections de corps cyclotomiques (le cas des compositums ne nécessite aucune théorie).

Lemme 8.6. *Soit $f : \mathbb{N}^* \longrightarrow \mathbb{C}$ une fonction multiplicative, au sens où pour tous m, n premiers entre eux, on a $f(mn) = f(m)f(n)$. On a alors pour tous $m, n \geq 1$:*

$$f(m)f(n) = f(m \wedge n)f(m \vee n).$$

Démonstration. On note, pour p premier, v_p la valuation p-adique de m et w_p celle de n. On a, par multiplicativité :

$$f(m)f(n) = \prod_p (f(p^{v_p})f(p^{w_p}))$$

et :

$$f(m \wedge n)f(m \vee n) = \prod_p \left(f\left(p^{\min(v_p, w_p)}\right) f\left(p^{\max(v_p, w_p)}\right)\right).$$

Ces deux quantités sont clairement égales. □

Proposition 8.7. *Soient $m, n \geq 1$. On a :*

$$\mathbb{Q}(\mathbb{U}_m) \cap \mathbb{Q}(\mathbb{U}_n) = \mathbb{Q}(\mathbb{U}_{m \wedge n})$$

et :

$$\mathbb{Q}(\mathbb{U}_m)\mathbb{Q}(\mathbb{U}_n) = \mathbb{Q}(\mathbb{U}_{m \vee n}).$$

Démonstration. On a clairement :

$$\mathbb{Q}(\mathbb{U}_m)\mathbb{Q}(\mathbb{U}_n) = \mathbb{Q}(\mathbb{U}_m, \mathbb{U}_n) = \mathbb{Q}(\mathbb{U}_m\mathbb{U}_n) = \mathbb{Q}(\mathbb{U}_{m \vee n}).$$

L'égalité $\mathbb{U}_m\mathbb{U}_n = \mathbb{U}_{m \vee n}$ vient du fait que le seul sous-groupe de $\mathbb{U}_{m \vee n}$ dont l'ordre est divisible par m et n est $\mathbb{U}_{m \vee n}$.
On note ensuite $K = \mathbb{Q}(\mathbb{U}_m) \cap \mathbb{Q}(\mathbb{U}_n)$ et $L = \mathbb{Q}(\mathbb{U}_{m \vee n})$. Les extensions $\mathbb{Q}(\mathbb{U}_m)/K$ et $\mathbb{Q}(\mathbb{U}_n)/K$ étant galoisiennes, le théorème 2.24 s'applique et donne, au niveau des degrés :

$$[\mathbb{Q}(\mathbb{U}_m) : K] \cdot [\mathbb{Q}(\mathbb{U}_n) : K] = [\mathbb{Q}(\mathbb{U}_{m \vee n}) : K]$$

qui se réécrit :

$$[\mathbb{Q}(\mathbb{U}_m):\mathbb{Q}]\cdot[\mathbb{Q}(\mathbb{U}_n):\mathbb{Q}] = [\mathbb{Q}(\mathbb{U}_{m\vee n}):\mathbb{Q}]\cdot[K:\mathbb{Q}]$$

donc :

$$[K:\mathbb{Q}] = \frac{\varphi(m)\varphi(n)}{\varphi(m\vee n)} = \varphi(m\wedge n)$$

par le lemme 8.6. Or on a clairement $\mathbb{Q}(\mathbb{U}_{m\wedge n})\subseteq K$ et ces corps ont le même degré sur $\mathbb{Q}$ donc ils sont égaux. □

8.4 Anneau des entiers d'un corps cyclotomique

8.4.1 Le cas des puissances de nombres premiers

Soit p un nombre premier, $k\geq 1$ un entier et $m = p^k$. On considère le corps cyclotomique $K = \mathbb{Q}(\mathbb{U}_m)$ de degré $\varphi(m) = (p-1)p^{k-1}$. On suppose aussi $m\geq 3$ pour avoir $K\neq\mathbb{Q}$.

Lemme 8.8. *Soit ω une racine primitive m-ème de l'unité. On a :*

$$N_{K/\mathbb{Q}}(1-\omega) = p.$$

Démonstration. Par le théorème 8.4, le groupe de Galois de $K/\mathbb{Q}$ s'identifie au groupe des automorphismes du groupe cyclique $\mathbb{U}_m$, et ainsi :

$$N_{K/\mathbb{Q}}(1-\omega) = \prod_{\langle\alpha\rangle=\mathbb{U}_m}(1-\alpha) = \left(\frac{\prod_{\alpha\in\mathbb{U}_m}(X-\alpha)}{\prod_{\alpha\in\mathbb{U}_{m/p}}(X-\alpha)}\right)(1) = \left(\frac{X^m-1}{X^{m/p}-1}\right)(1) = p$$

comme souhaité. □

Proposition 8.9. *Le nombre premier p est totalement ramifié dans K et on a :*

$$p\mathcal{O}_K = (1-\omega)^{\varphi(m)}$$

pour ω une racine primitive m-ème de l'unité. De plus l'indice d'inertie de p vaut 1.

Démonstration. Puisque $N_{K/\mathbb{Q}}(1-\omega) = p$, d'après la formule 7.8, on a :

$$p\mathcal{O}_K = \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}(1-\sigma(\omega)) = \prod_{\langle\alpha\rangle=\mathbb{U}_m}(1-\alpha)$$

et chaque $(1-\alpha)$ est un premier puisque sa norme est première. Il suffit alors de constater que les $(1-\alpha)$ sont tous égaux. Mais si α,β sont deux générateurs de $\mathbb{U}_m$, on peut écrire :

$$\beta = \alpha^k$$

pour un $k\geq 1$ et ainsi :

$$\frac{1-\beta}{1-\alpha} = 1+\alpha+\cdots+\alpha^{k-1}\in\mathcal{O}_K$$

donc $(1-\alpha)\,|\,(1-\beta)$ et on a l'autre relation de divisibilité par symétrie.
Puisque $e(p)f(p)r(p) = \varphi(m)$ et $r(p) = 1$ et $e(p) = \varphi(m)$, on en déduit que l'indice d'inertie $f(p)$ vaut 1. □

Théorème 8.10. *L'anneau des entiers de K est donné par :*

$$\mathcal{O}_K = \mathbb{Z}[\mathbb{U}_m] = \mathbb{Z}[\omega]$$

avec ω un générateur de $\mathbb{U}_m$. De plus on a :

$$\mathrm{Disc}(K) = \pm p^{p^{k-1}(k(p-1)-1)}$$

où le signe est donné par $(-1)^{\varphi(m)/2}$, puisque $m \geq 3$.
Ainsi p est le seul nombre premier ramifié dans K.
Mentionnons enfin que si $m = p \geq 3$, le discriminant est simplement :

$$\mathrm{Disc}(\mathbb{Q}(\mathbb{U}_p)) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Démonstration. On fixe ω une racine primitive m-ème de l'unité et on considère le sous anneau :

$$\Lambda = \mathbb{Z}[\omega] = \mathbb{Z}[1-\omega] \subseteq \mathcal{O}_K$$

Puisque $\mathbb{Q}\Lambda = K$, Λ est un sous-réseau de $\mathcal{O}_K$ dont une base est $(1, \omega, \ldots, \omega^{\varphi(m)-1})$. Par le théorème 2.15 on a :

$$\mathrm{Disc}_{K/\mathbb{Q}}(\Lambda) = D_{K/\mathbb{Q}}(1, \omega, \ldots, \omega^{\varphi(m)-1})\mathbb{Z} = N_{K/\mathbb{Q}}(\pi'_\omega(\omega))\mathbb{Z}$$

Or π_ω est le m-ème polynôme cyclotomique :

$$\pi_\omega = \frac{X^m - 1}{X^{m/p} - 1}$$

et ainsi par un calcul direct en utilisant que $\omega^m = 1$:

$$\pi'_\omega(\omega) = \frac{m}{\omega(\omega^{m/p} - 1)}$$

ce qui donne :

$$\mathrm{Disc}_{K/\mathbb{Q}}(\Lambda) = \frac{m^{\varphi(m)}}{N_{K/\mathbb{Q}}(\omega^{m/p} - 1)}\mathbb{Z}$$

car les inversibles ont norme ± 1. Par transitivité de la norme 2.10 on a, en posant $F = \mathbb{Q}(\omega^{m/p})$ et en utilisant le lemme 8.8 :

$$N_{K/\mathbb{Q}}(\omega^{m/p} - 1) = N_{F/\mathbb{Q}}(N_{K/F}(\omega^{m/p} - 1)) = N_{F/\mathbb{Q}}(\omega^{m/p} - 1)^{[K:F]} = p^{[K:F]} = p^{\varphi(m)/\varphi(p)} = p^{p^{k-1}}$$

donc :

$$\mathrm{Disc}_{K/\mathbb{Q}}(\Lambda) = p^{k(p-1)p^{k-1} - p^{k-1}}\mathbb{Z} = p^{p^{k-1}(k(p-1)-1)}\mathbb{Z}.$$

On pose alors :

$$d = p^{p^{k-1}(k(p-1)-1)}$$

qui est une puissance de p, notons la p^s. D'après le théorème 5.30 on a alors :

$$\mathcal{O}_K \subseteq \frac{1}{p^s}\Lambda.$$

On montre ensuite que $\Lambda \cap p\mathcal{O}_K \subseteq p\Lambda$. Soit $x \in \Lambda \cap p\mathcal{O}_K \setminus p\Lambda$, on écrit :

$$x = a_k(1-\omega)^k + a_{k+1}(1-\omega)^{k+1} + \cdots + a_{\varphi(m)-1}(1-\omega)^{\varphi(m)-1}$$

avec $a_i \in \mathbb{Z}$, avec $a_k \neq 0$. On peut aussi supposer k maximal pour l'existence d'un tel élément. Notons que cette base est beaucoup plus commode que la base naïve $(1, \omega, \ldots, \omega^{\varphi(m)-1})$ car elle est directement reliée à l'idéal premier $(1-\omega)$. Puisque $x \in p\mathcal{O}_K = (1-\omega)^{\varphi(m)}$, on a :

$$(1-\omega)^{\varphi(m)} \mid x$$

en particulier $(1-\omega)^{k+1} \mid x$ et donc $1-\omega \mid a_k$. Ainsi $a_k \in (1-\omega)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$. En considérant $x - a_k(1-\omega)^k$, on contredit alors la maximalité de k.
On a donc bien $\Lambda \cap p\mathcal{O}_K \subseteq p\Lambda$ puis par récurrence $\Lambda \cap p^s\mathcal{O}_K \subseteq p^s\Lambda$ et donc :

$$\mathcal{O}_K \subseteq \frac{1}{p^s}\Lambda \cap \mathcal{O}_K \subseteq \frac{1}{p^s}(\Lambda \cap p^s\mathcal{O}_K) = \Lambda$$

ce qui conclut la preuve que :

$$\mathcal{O}_K = \mathbb{Z}[\omega]$$

et tout le reste en découle : le discriminant de K est alors bien $\pm d$ et le signe est donné par le théorème 6.17 (ou par un calcul attentif) puisque K n'a que des plongements imaginaires donc $s = \varphi(m)/2$. Par le théorème de Dedekind 5.41, p est le seul premier ramifié. □

On peut en déduire le différent sans aucun calcul (on pourrait aussi utiliser le théorème 5.32).

Corollaire 8.11. *On note* $\mathrm{Diff}(K)$ *le différent* $\mathrm{Diff}_{\mathcal{O}_K/\mathbb{Z}}$ *et* $\mathfrak{p}$ *l'unique premier au dessus de* p*, c'est à dire* $\mathfrak{p} = (1-\omega)\mathcal{O}_K$ *avec* ω *une racine primitive* m*-ème de l'unité. On a alors :*

$$\mathrm{Diff}(K) = \mathfrak{p}^{p^{k-1}(k(p-1)-1)}$$

et dans le cas $m = p \geq 3$ *:*

$$\mathrm{Diff}(K) = \mathfrak{p}^{p-2}.$$

Démonstration. Puisque $\|\mathrm{Diff}(K)\| = |\mathrm{Disc}(K)|$, le seul diviseur premier de $\mathrm{Diff}(K)$ est $\mathfrak{p}$. Si $\mathrm{Diff}(K) = \mathfrak{p}^{\ell}$, comme $f(\mathfrak{p} \mid p) = 1$ (voir proposition 8.9) on a :

$$\ell = v_p(\mathrm{Disc}(K))$$

ce qui conclut. □

8.4.2 Cas général

L'étude des corps cyclotomiques $\mathbb{Q}(\mathbb{U}_{p^n})$ ainsi que le théorème 5.49 sur les compositums d'extensions de Dedekind permet d'établir le théorème général suivant.

Théorème 8.12. *Soit $n \geq 1$ un entier. L'anneau des entiers du corps cyclotomique $\mathbb{Q}(\mathbb{U}_n)$ est simplement :*

$$\mathcal{O}_{\mathbb{Q}(\mathbb{U}_n)} = \mathbb{Z}[\mathbb{U}_n] = \mathbb{Z}[\omega]$$

pour ω une racine primitive n-ème de l'unité. De plus, on a :

$$\mathrm{Disc}(\mathbb{Q}(\mathbb{U}_n)) = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}$$

et le signe est donné par $(-1)^{\varphi(n)/2}$ si $n \geq 3$ (sinon on a $\mathbb{Q}(\mathbb{U}_n) = \mathbb{Q}$).

Démonstration. On montre cela par récurrence forte sur n en constatant que si m et n sont premiers entre eux, et si l'énoncé est connu pour m et n, alors il est vrai pour mn. En effet, les discriminants de m et n sont alors clairement premiers entre eux, les corps $\mathbb{Q}(\mathbb{U}_m)$ et $\mathbb{Q}(\mathbb{U}_n)$ sont complémentaires (d'après 8.7) d'intersection $\mathbb{Q}$ et on conclut alors par le théorème 5.49.
Le signe du discriminant s'obtient avec le théorème 6.17 : si $n \geq 3$, le corps $\mathbb{Q}(\mathbb{U}_n)$ n'a aucun plongement réel car il est galoisien et non contenu dans $\mathbb{R}$. □

8.5 Factorisation des polynômes cyclotomiques dans un corps fini

Les polynômes cyclotomiques Φ_n étant à coefficients dans $\mathbb{Z}$ et unitaires, on peut les voir comme polynômes de $K[X]$ unitaires de degré $\varphi(n)$ pour tout corps K. En revanche ils n'ont pas de raison d'être irréductibles dans K, ni même d'être séparables. Par exemple, si K est un corps de caractéristique 0 contenant n racines n-èmes de l'unité, Φ_n est scindé dans K. Il y a aussi des cas où K ne possède pas n racines n-èmes de l'unité mais où Φ_n se factorise quand même dans K : par exemple $\Phi_8 = 1 + X^4$ se factorise dans $\mathbb{Q}(\mathbb{U}_8) \cap \mathbb{R}$.
On se pose ici la question de déterminer la factorisation de Φ_n dans un corps fini quelconque. Pour K un corps et $n \geq 1$, on note :

$$\mathbb{U}_n(K)$$

l'ensemble des racines de l'unité de K. Elles forment un groupe cyclique (pas nécessairement de cardinal n), d'après le théorème 2.30. On connait le nombre de racines n-èmes de l'unité dans un corps algébriquement clos et dans un corps finis. C'est l'objet des deux propositions suivantes.

Proposition 8.13. *Soit K un corps algébriquement clos et $n \geq 1$ un entier. Si n est non nul dans K, alors :*

$$|\mathbb{U}_n(K)| = n$$

et si K est de caractéristique $p > 0$ et si $n = p^k m$ avec $p \nmid m$, on a :

$$\mathbb{U}_n(K) = \mathbb{U}_m(K)$$

et $|\mathbb{U}_n(K)| = m$.

Démonstration. Si n est non nul dans K, le polynôme $X^n - 1$ est séparable dans K car sa dérivée est nX^{n-1} dont 0 est la seule évetuelle racine, et ce n'est pas une racine de $X^n - 1$, donc $X^n - 1$ a exactement n racines dans K puisque K est algébriquement clos. Si $n = p^k m$ comme dans l'énoncé, on a alors :

$$X^n - 1 = (X^m - 1)^{p^k}$$

donc $X^n - 1$ et $X^m - 1$ ont les mêmes racines, et m n'est pas nul dans K donc on a ce qu'on voulait. □

Proposition 8.14. *Soit K un corps fini de cardinal $q = p^\ell$ avec $\ell \geq 1$ et p premier et soit $n \geq 1$. Le symbole $\wedge$ désigne le* pgcd.
On a :

$$\mathbb{U}_n(K) = \mathbb{U}_{n \wedge (q-1)}(K)$$

et :

$$|\mathbb{U}_n(K)| = n \wedge (q-1).$$

Démonstration. D'après le théorème 2.30, $K^\times$ est un groupe cyclique de cardinal $q-1$. Ainsi $\mathbb{U}_n(K)$ est la n-torsion d'un groupe cyclique de cardinal $q-1$. On a une suite exacte :

$$0 \longrightarrow (\mathbb{Z}/(q-1)\mathbb{Z})(n) \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z} \xrightarrow{\times n} \mathbb{Z}/(q-1)\mathbb{Z} \longrightarrow \mathbb{Z}/(q-1,n)\mathbb{Z} \longrightarrow 0$$

donc :

$$|(\mathbb{Z}/(q-1)\mathbb{Z})(n)| = |\mathbb{Z}/(q-1,n)\mathbb{Z}| = |\mathbb{Z}/((q-1)\wedge n)\mathbb{Z}| = (q-1)\wedge n.$$

Ainsi $\mathbb{U}_n(K)$ est de cardinal $n \wedge (q-1)$ et il n'y a qu'un seul tel sous-groupe de $K^\times$. □

On peut relier les racines de l'unité dans $\overline{\mathbb{Q}}$ et dans un corps algébriquement clos.

Lemme 8.15. *Soit K un corps algébriquement clos et $n \geq 1$. On note $L = \mathbb{Q}(\mathbb{U}_n)$ le n-ème corps cyclotomique.*
Il existe alors un morphisme d'anneaux $\mathcal{O}_L \longrightarrow K$ dont l'image est le sous-corps de K engendré par les racines n-èmes de l'unité, et tout morphisme de ce type induit un morphisme de groupes surjectif :

$$\mathbb{U}_n \longrightarrow \mathbb{U}_n(K).$$

Si n est non nul dans K, c'est un isomorphisme. Sinon, on a une suite exacte :

$$1 \longrightarrow \mathbb{U}_{p^k} \longrightarrow \mathbb{U}_n \longrightarrow \mathbb{U}_m(K) \longrightarrow 1$$

avec $n = p^k m$ et $p \nmid m$ la caractéristique de K.

Démonstration. Le cas où K est de caractéristique nulle est clair. Supposons K de caractéristique $p > 0$, et considérons un plongement :

$$\mathcal{O}_L/\mathfrak{p} \longrightarrow K$$

avec $\mathfrak{p}$ un premier quelconque au dessus de p (un tel plongement existe car K est algébriquement clos et $\mathcal{O}_L/\mathfrak{p}$ est un corps fini). Le morphisme composé $\mathcal{O}_L \longrightarrow K$ envoie alors $X^n - 1 = \prod_{\omega \in \mathbb{U}_n}(X - \omega)$ sur :

$$X^n - 1_K = \prod_{\omega \in \mathbb{U}_n} (X - \overline{\omega})$$

donc le morphisme induit :

$$\mathbb{U}_n \longrightarrow \mathbb{U}_n(K) = \mathbb{U}_m(K)$$

est surjectif. Puisque $|\mathbb{U}_n| = n$ et $|\mathbb{U}_n(K)| = m$, le noyau est de cardinal p^k et $\mathbb{U}_{p^k}$ est le seul sous-groupe de $\mathbb{U}_n$ de cardinal p^k. L'image de $\mathcal{O}_L \longrightarrow K$ est bien F, le sous-corps engendré par les racines de l'unité car $\mathcal{O}_L = \mathbb{Z}[\omega]$ d'après 8.12. Enfin, si $f : \mathcal{O}_L \longrightarrow K$ a pour image F, alors le noyau de f, $\mathfrak{p}$, est un idéal maximal de $\mathcal{O}_L$ car $\mathcal{O}_L/\mathfrak{p} \cong F$, et il est au dessus de p car p est nul dans K. □

Lemme 8.16. *Soient $m, n \geq 1$ avec $m \mid n$. Le morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ de réduction modulo m induit un morphisme de groupes surjectif :*

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow 1.$$

En particulier $\varphi(m) \mid \varphi(n)$.

Démonstration. Il s'agit de montrer que si $k \wedge m = 1$, alors il existe ℓ premier avec n tel que $\ell \equiv k\ [m]$. On écrit $n = dm$. Par le théorème chinois, il existe $\ell \in \mathbb{Z}$ tel que :

$$\ell \equiv k\ [m]$$

et :

$$\ell \equiv 1\ [p]$$

pour tout p premier divisant d et ne divisant pas m. Ainsi ℓ et n n'ont aucun diviseur premier en commun, ce qui conclut. □

De ces deux lemmes, on déduit la proposition suivante qui assure qu'on peut aussi définir Φ_n directement dans un corps algébriquement clos quelconque où n n'est pas nul. Si G est un groupe, on note G^{gen} l'ensemble de ses générateurs. Ainsi $(\mathbb{Z}/n\mathbb{Z})^{\text{gen}} = (\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 8.17. *Soit K un corps algébriquement clos et $n \geq 1$ non nul dans K. Alors le morphisme $\mathbb{Z} \longrightarrow K$ envoie Φ_n sur :*

$$\prod_{\omega \in \mathbb{U}_n(K)^{\text{gen}}} (X - \omega) \in K[X]$$

Dans le cas où K est de caractéristique positive p, si $n = p^k m$ avec $p \nmid m$, alors Φ_n est envoyé sur l'image de $\Phi_m^{\varphi(p^k)}$:

$$\prod_{\omega \in \mathbb{U}_m(K)^{\text{gen}}} (X - \omega)^{\varphi(p^k)}.$$

Démonstration. En caractéristique nulle l'énoncé ne présente pas de difficulté. Supposons K de caractéristique p et $n = p^k m$ avec $p \nmid m$. D'après le lemme 8.15, on a une suite exacte :

$$1 \longrightarrow \mathbb{U}_{p^k} \longrightarrow \mathbb{U}_n \longrightarrow \mathbb{U}_m(K) \longrightarrow 1$$

induit par un certain morphisme d'anneaux $f : \mathcal{O}_L \longrightarrow K$ avec $L = \mathbb{Q}(\mathbb{U}_n)$ dont l'image est un corps.
Par le lemme 8.16 ce morphisme induit une application surjective :

$$g : \mathbb{U}_n^{\text{gen}} \longrightarrow \mathbb{U}_m(K)^{\text{gen}}$$

et ces deux ensembles peuvent être munis d'une structure de groupe en fixant un générateur de $\mathbb{U}_n$ (dont l'image est un générateur de $\mathbb{U}_n(K)$) et ainsi en les identifiant aux groupes $(\mathbb{Z}/n\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z})^\times$, faisant ainsi de g un morphisme de groupes surjectif. Ainsi les fibres ont toutes le même cardinal, $\varphi(n)/\varphi(m) = \varphi(p^k)$ car m et p^k sont premiers entre eux.
Il en résulte que la factorisation dans $L[X]$:

$$\Phi_n = \prod_{\omega \in \mathbb{U}_n^{\text{gen}}} (X - \omega)$$

induit la factorisation suivante dans $K[X]$:

$$f(\Phi_n) = \prod_{\omega \in \mathbb{U}_m(K)^{\text{gen}}} (X - \omega)^{\varphi(p^k)}$$

comme voulu. □

On peut à présent déterminer la factorisation de Φ_n dans les corps finis.

Théorème 8.18. *Soit K un corps fini de cardinal $q = p^\ell$ avec $\ell \geq 1$ et p un nombre premier et soit $n \geq 1$. On écrit $n = p^k m$ avec $p \nmid m$. Le polynôme Φ_n se factorise en produit d'irréductibles dans $K[X]$ de la façon suivante :*

$$\Phi_n = \Phi_m^e = P_1^e \dots P_r^e$$

avec :

$$e = \varphi(p^k)$$

ainsi que :

$$r = \frac{\varphi(m)}{\text{ord}_m(q)}$$

avec $\text{ord}_m(q)$ l'ordre de q dans le groupe $(\mathbb{Z}/m\mathbb{Z})^\times$. De plus les P_i sont tous de degré :

$$f = \text{ord}_m(q)$$

et les ensembles de racines des P_i sont les orbites de $\mathbb{U}_n(K)$ sous l'action du frobenius $x \mapsto x^q$. Enfin, si $\overline{K}$ est une clôture algébrique de K, l'extension $K(\mathbb{U}_n(\overline{K}))/K$ est de degré f.

Démonstration. D'après 8.17, Φ_n est envoyé sur Φ_m^e et on peut donc supposer $k = 0$, et donc $n = m$ non nul dans K. Ainsi, puisque Φ_n divise le polynôme séparable $X^n - 1$ dans $K[X]$, il est aussi séparable.
On note $F = K(\mathbb{U}_n(\overline{K}))$. Le frobenius $\varphi : x \mapsto x^q$ agit sur $\mathbb{U}_n(\overline{K}) = \mathbb{U}_n(F)$, qui est un ensemble de cardinal n puisque $n \neq 0$ dans K, et les orbites (i.e. les orbites sous l'action du groupe de Galois de l'extension galoisienne F/K) sont exactement les ensembles de racines dans F des facteurs irréductibles P_i pour tout i, avec $\Phi_n = P_1 \dots P_r$ (ils sont distincts car Φ_n est séparable).
Par le théorème orbite-stabilisateur, en faisant agir $\mathbb{Z}$ sur $\mathbb{U}_n(F)$ via le frobenius, la taille de l'orbite associée à P_i (i.e. le degré de P_i) est l'indice dans $\mathbb{Z}$ du stabilisateur d'un élément ω de cette orbite. Or ω est une racine primitive n-ème de l'unité, donc on a :

$$\varphi^j(\omega) = \omega \iff \omega^{q^j-1} = 1 \iff n \mid q^j - 1 \iff q^j \equiv 1\ [n] \iff \mathrm{ord}_n(q) \mid j$$

donc ce stabilisateur est exactement $\mathrm{ord}_n(q)\mathbb{Z}$, et ainsi :

$$\deg P_i = \mathrm{ord}_n(q).$$

On a donc $f = \mathrm{ord}_n(q)$ et $rf = \varphi(n)$ donc $r = \frac{\varphi(n)}{\mathrm{ord}_n(q)}$. Puisque F est engendré par ω, le degré de $[F : K]$ est simplement le degré du polynôme minimal de ω, c'est à dire f. □

On en déduit directement le corollaire suivant.

Corollaire 8.19. *Soit K un corps fini de cardinal $q = p^\ell$ et $n \geq 1$ avec $p \geq 3$. Le polynôme cyclotomique Φ_n est irréductible dans K si et seulement si p ne divise pas n et q engendre $(\mathbb{Z}/n\mathbb{Z})^\times$.*
De plus, Φ_n est scindé à racines simples dans K si et seulement si $q \equiv 1\ [n]$.
Pour $p = 2$, on a que Φ_n est irréductible dans K si et seulement si $4 \nmid n$ et q génère $(\mathbb{Z}/m\mathbb{Z})^\times$ avec $m = n$ si n est impair et $m = n/2$ si n est pair. De plus Φ_n est scindé à racines simples dans K si et seulement si $4 \nmid n$ et $q \equiv 1\ [m]$.

8.6 Factorisation des nombres premiers dans une extension cyclotomique

Théorème 8.20. *Soit $n \geq 1$. On note $K = \mathbb{Q}(\mathbb{U}_n)$. Soit p un nombre premier. On adopte les notations du théorème 8.18 :*

$$n = p^k m$$

avec $p \nmid m$. On a alors :

$$e(p) = \varphi(p^k)$$

ainsi que :

$$f(p) = \mathrm{ord}_m(p)$$

et :

$$r(p) = \frac{\varphi(m)}{\mathrm{ord}_m(p)}.$$

En particulier pour $p \geq 3$, p est ramifié si et seulement si $p \mid n$, p est inerte si et seulement si p engendre $(\mathbb{Z}/n\mathbb{Z})^\times$ et p est totalement décomposé (i.e. $e(p) = f(p) = 1$) si et seulement si $p \equiv 1\ [n]$. Pour $p = 2$, on obtient que 2 est ramifié si et seulement si $4 \mid n$, 2 est inerte si et seulement si 2 engendre $(\mathbb{Z}/m\mathbb{Z})^\times$ et 2 est totalement décomposé si te seulement si $p \equiv 1\ [m]$.

Démonstration. C'est une application directe de 8.18 pour le corps fini $\mathbb{F}_p$, en utilisant que $\mathcal{O}_K = \mathbb{Z}[\omega]$ avec ω de polynôme minimal Φ_n, et en utilisant le théorème 5.48 sur la factorisation des idéaux dans une extension de Dedekind engendrée par un élément. □

Remarque 8.21. Pour certaines valeurs impaires de n, le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas toujours cyclique et donc parfois aucun premier n'est inerte dans $\mathbb{Q}(\mathbb{U}_n)$. Par exemple $\mathbb{Z}[\exp(2i\pi/15)]/(p)$ n'est jamais un corps quelque soit le nombre premier p. On précise impaire car le critère pour $p = 2$ est un peu différent si n est pair comme l'indique le théorème précédent.

Chapitre 9

Groupes de ramification supérieure et théorème de Kronecker-Weber

> Nearly everything is really interesting if you go into it deeply enough
>
> Richard Feynman

9.1 Groupes de ramification supérieure

On fixe B/A une extension de Dedekind *galoisienne* de corps des fractions L/K et de groupe G, et on suppose A localement parfait (voir 5.38). On fixe aussi $\mathfrak{q}$ un premier de B au dessus de $\mathfrak{p}$ un premier de A. On adopte les notations du théorème 7.7 :

$$G \supseteq D = D(\mathfrak{q} \mid \mathfrak{p}) \supseteq E = E(\mathfrak{q} \mid \mathfrak{p})$$

et $e = e(\mathfrak{q} \mid \mathfrak{p})$, $f = f(\mathfrak{q} \mid \mathfrak{p})$ et r est le nombre d'idéaux au dessus de $\mathfrak{p}$.

Définition 9.1. *Soit $m \geq 0$. Le groupe D agit sur la B-algèbre $B/\mathfrak{q}^{m+1}$ par automorphismes. On définit le m-ème groupe de ramification $E_m(\mathfrak{q} \mid \mathfrak{p})$ ou plus simplement E_m comme le noyau de cette action, c'est à dire comme l'ensemble des $\sigma \in D$ qui agissent trivialement sur $B/\mathfrak{q}^{m+1}$, i.e. pour tout $b \in B$:*

$$\sigma(b) \equiv b \ [\mathfrak{q}^{m+1}].$$

Par construction E_m est distingué dans D, $E_0 = E$ et on a une filtration décroissante :

$$G \supseteq D \supseteq E_0 \supseteq E_1 \supseteq E_2 \supseteq \dots.$$

Notons que :

$$\bigcap_{m \geq 0} \mathfrak{q}^{m+1} = 0$$

car 0 est le seul élément de valuation $\mathfrak{q}$-adique infinie, et donc si σ est un élément de $\bigcap_{m\geq 0} E_m$, alors pour tout b on a $\sigma(b) - b \in \bigcap_{m\geq 0} \mathfrak{q}^{m+1}$ donc $\sigma(b) = b$ et puisque $L = KB$

on obtient que σ fixe L et $\sigma = \mathrm{id}$. Autrement dit :

$$\bigcap_{m\geq 0} E_m = 1$$

et donc, puisque ce sont des groupes finis, on a $E_m = 1$ pour m assez grand.

On peut alléger la condition $\sigma(b) \equiv b\ [\mathfrak{q}^{m+1}]$ en la vérifiant seulement pour une uniformisante à condition que $\sigma \in E$:

Proposition 9.2. *On considère π une uniformisante de $\mathfrak{q}$, c'est à dire un élément de $\mathfrak{q} \setminus \mathfrak{q}^2$. Soit $m \geq 0$, on a :*

$$E_m = \{\sigma \in E \mid \sigma(\pi) \equiv \pi\ [\mathfrak{q}^{m+1}]\}.$$

Démonstration. Notons E'_m l'ensemble de droite. On a clairement $E_m \subseteq E'_m$ et on montre la deuxième inclusion par récurrence sur m. Pour $m = 0$ c'est clair, supposons maintenant $m \geq 1$ et $E_{m-1} = E'_{m-1}$, et donnons nous $\sigma \in E'_m$. On a naturellement $\sigma \in E'_{m-1}$ donc $\sigma \in E_{m-1}$.
On montre dans un premier temps que pour tout $x \in \mathfrak{q}$ on a :

$$\sigma(x) \equiv x\ [\mathfrak{q}^{m+1}].$$

Soit $x \in \mathfrak{q}$. Par le théorème de spécification finie 3.42, il existe $y \in B$ tel que :

$$v_{\mathfrak{q}}(y) = v_{\mathfrak{q}}(x)$$

et pour tout $\mathfrak{q}' \neq \mathfrak{q}$ divisant x ou divisant π :

$$v'_{\mathfrak{q}}(y) = \max(v'_{\mathfrak{q}}(x), v'_{\mathfrak{q}}(\pi))$$

de sorte que :

$$y \in \pi B \cap xB.$$

Observons alors que $\sigma(y) \equiv y\ [\mathfrak{q}^{m+1}]$: en effet, on peut écrire $y = \pi b$ avec $b \in B$ et cela découle alors du fait que $\sigma(\pi) \equiv \pi\ [\mathfrak{q}^{m+1}]$ et $\sigma(b) \equiv b\ [\mathfrak{q}^m]$ car $\sigma \in E_{m-1}$.
Ainsi, en écrivant $y = x\beta$ avec $\beta \in B$, puisque $v_{\mathfrak{q}}(y) = v_{\mathfrak{q}}(x)$, on a $v_{\mathfrak{q}}(\beta) = 0$ et :

$$\sigma(x)\sigma(\beta) - x\beta \in \mathfrak{q}^{m+1}$$

donc, en posant $t = \sigma(x) - x \in \mathfrak{q}^m$ et $u = \sigma(\beta) - \beta \in \mathfrak{q}^m$:

$$t\beta + ux + tu \in \mathfrak{q}^{m+1}$$

et donc, comme $x \in \mathfrak{q}$ et comme $m \geq 1$:

$$t\beta \in \mathfrak{q}^{m+1}$$

et $t \in \mathfrak{q}^{m+1}$ car β n'est pas divisible par $\mathfrak{q}$, et donc on a bien montré $\sigma(x) \equiv x\ [\mathfrak{q}^{m+1}]$ pour $x \in \mathfrak{q}$.
Cette égalité est clairement vraie pour $x \in B^E = B \cap L^E$ car dans ce cas $\sigma(x) = x$.
C'est donc vrai sur $\mathfrak{q} + B^E$, or on a :

$$B = \mathfrak{q} + B^E.$$

En effet cela revient à dire que le morphisme de corps $B^E/\mathfrak{q}^E \longrightarrow B/\mathfrak{q}$ est surjectif, autrement dit $f(\mathfrak{q}^E \mid \mathfrak{p}) = f$, ce qui découle du théorème 7.7. □

Remarque 9.3. Dans la proposition précédente, on ne prend pas tous les $\sigma \in D$ qui vérifient cette condition mais seulement ceux de E : en effet, pour $m = 0$, $\{\sigma \in D \mid \sigma(\pi) \equiv \pi\ [\mathfrak{q}]\} = D$ et ce n'est pas E_0 en général.

Pour étudier la filtration des E_i, on va plonger les quotients successifs E_i/E_{i+1} dans des groupes abéliens isomorphes à ℓ ou à $\ell^\times$. Dans la suite on note $k = A/\mathfrak{p}$ et $\ell = B/\mathfrak{q}$ les corps résiduels, de sorte que ℓ/k est une extension finie galoisienne de corps parfaits.

Théorème 9.4. *L'action de E_0 sur $\mathfrak{q}/\mathfrak{q}^2$ induit un morphisme de groupes injectif :*

$$E_0/E_1 \xrightarrow{\varphi_0} \mathrm{GL}_\ell(\mathfrak{q}/\mathfrak{q}^2) \cong \ell^\times$$

où $\mathrm{GL}_\ell(\mathfrak{q}/\mathfrak{q}^2)$ est le groupe des automorphismes du ℓ-espace vectoriel de dimension 1 $\mathfrak{q}/\prec^2$. De plus, pour tout $m \geq 1$ on a un morphisme de groupes injectif :

$$E_m/E_{m+1} \xrightarrow{\varphi_m} \mathrm{Hom}_\ell(\mathfrak{q}/\mathfrak{q}^2, \mathfrak{q}^{m+1}/\mathfrak{q}^{m+2})$$

tel que, en omettant de noter les réductions dans les quotients :

$$\varphi_m(\sigma)(x) = \sigma x - x$$

pour $\sigma \in E_m$ et $x \in \mathfrak{q}$.
Enfin, comme $\mathfrak{q}/\mathfrak{q}^2$ et $\mathfrak{q}^m/\mathfrak{q}^{m+1}$ sont tous deux des ℓ-espaces vectoriels de dimension 1, on a un isomorphisme entre $\mathrm{Hom}_\ell(\mathfrak{q}/\mathfrak{q}^2, \mathfrak{q}^{m+1}/\mathfrak{q}^{m+2})$ et ℓ en choisissant une uniformisante de $\mathfrak{q}$ par exemple.
En particulier les quotients E_i/E_{i+1} sont tous des groupes abéliens qui se plongent dans $\ell^\times$ pour $i = 0$ et dans ℓ pour $i \geq 1$.

Démonstration. D'abord $E_0 = E$ stabilise $\mathfrak{q}$ et donc $\mathfrak{q}^2$ et il agit dessus par automorphismes de B-modules. Cette action se factorise en une action de E_0 sur $\mathfrak{q}/\mathfrak{q}^2$ par automorphismes ℓ-linéaires et donne un morphisme de groupes :

$$E_0 \longrightarrow \mathrm{GL}_\ell(\mathfrak{q}/\mathfrak{q}^2)$$

dont le noyau est exactement E_1 d'après la proposition 9.2 (le noyau est formé des $\sigma \in E$ qui agissent trivialement sur $\mathfrak{q}/\mathfrak{q}^2$ et en particulier qui vérifient $\sigma\pi \equiv \pi\ [\mathfrak{q}^2]$ avec π une uniformisante de $\mathfrak{q}$).
On a donc un morphisme injectif :

$$E_0/E_1 \xrightarrow{\varphi_0} \mathrm{GL}_\ell(\mathfrak{q}/\mathfrak{q}^2)$$

et $\mathfrak{q}/\mathfrak{q}^2$ est de dimension 1 comme ℓ-espace vectoriel d'après 3.58, donc son groupe linéaire s'identifie à $\ell^\times$.
Soit maintenant $m \geq 1$ et fixons $\sigma \in E_m$. Par définition de E_m, on a pour tout $x \in B$:

$$\sigma x - x \in \mathfrak{q}^{m+1}$$

et on a donc une application A-linéaire bien définie :

$$\Delta_\sigma : \mathfrak{q} \longrightarrow \mathfrak{q}^{m+1}/\mathfrak{q}^{m+2}$$

qui envoie x sur la classe de $\sigma x - x$. Cette application est même B-linéaire car pour tout $b \in B$ et $x \in \mathfrak{q}$ on a :

$$\sigma(bx) - bx = (\sigma(b) - b)\sigma x + b(\sigma x - x) \equiv b(\sigma x - x) \ [\mathfrak{q}^{m+2}]$$

car $\sigma x \in \mathfrak{q}$ et $\sigma b - b \in \mathfrak{q}^{m+1}$.
Puisque $\mathfrak{q}^{m+1}/\mathfrak{q}^{m+2}$ est un ℓ-espace vectoriel, on obtient par adjonction des scalaires une application ℓ-linéaire :

$$\mathfrak{q}/\mathfrak{q}^2 = \mathfrak{q} \otimes_B \ell \longrightarrow \mathfrak{q}^{m+1}/\mathfrak{q}^{m+2}$$

que l'on note $\psi_m(\sigma)$.
Vérifions que $\sigma \mapsto \psi_m(\sigma)$ est un morphisme de groupes. Pour tous $\sigma, \tau \in E_m$ et $x \in \mathfrak{q}$ on a :

$$\sigma\tau(x) - x = \sigma\tau(x) - \tau(x) + \tau(x) - x$$

et $\tau x \equiv x \ [\mathfrak{q}^2]$ car $m \geq 1$ donc $\psi_m(\sigma)(\tau x) = \psi_m(\sigma)(x)$. On en déduit que :

$$\sigma\tau x - \tau x \equiv \sigma x - x + \tau x - x \ [\mathfrak{q}^{m+2}]$$

comme souhaité. Enfin, le noyau de ψ_m est formé des $\sigma \in E_m$ qui vérifient :

$$\sigma x - x \equiv 0 \ [\mathfrak{q}^{m+2}]$$

pour tout $x \in \mathfrak{q}$ donc en particulier pour une uniformisante de $\mathfrak{q}$. Par la proposition 9.2 c'est exactement E_{m+1}. Cela donne bien le morphisme de l'énoncé et la proposition 3.58 assure que $\mathfrak{q}^{m+1}/\mathfrak{q}^{m+2}$ est un ℓ-espace vectoriel de dimension 1.

□

Corollaire 9.5. *Pour tout $m \geq 0$ le groupe E_m est résoluble. De plus le groupe D est résoluble si et seulement si le groupe de Galois local $\overline{G} = \overline{G}(\mathfrak{q} \mid \mathfrak{p})$ (voir 7.9) est résoluble. Ainsi dans le cas où A est localement fini, le groupe D est toujours résoluble.*

Démonstration. Les quotients successifs E_{m-1}/E_m sont tous abéliens d'après le théorème précédent 9.4. Or pour m assez grand on a $E_m = 1$ donc les E_m sont tous résolubles, et $D/E \cong \overline{G}$ d'après 7.9, donc D est résoluble si et seulement si $\overline{G}$ l'est. Si A est localement fini, $\overline{G}$ est le groupe de Galois d'une extension finie de corps fini, c'est donc un groupe cyclique, qui est en particulier résoluble, donc D est résoluble dans ce cas. □

Corollaire 9.6. *Si A est localement fini et s'il existe un premier de A avec $r = 1$ (c'est à dire qu'il y a un seul premier au dessus de $\mathfrak{p}$), alors le groupe de Galois G de L/K est résoluble.*

Démonstration. Dans ce cas, d'après 7.7, en prenant $\mathfrak{q}$ l'unique premier au dessus de $\mathfrak{p}$ on a $G = D(\mathfrak{q} \mid \mathfrak{p})$ qui est résoluble. □

Dans le cas où A est localement fini, on peut caractériser à quelle condition le groupe E_1 (et par conséquent tous les groupes de ramifications supérieures suivants) est trivial.

Proposition 9.7. *Si A est localement fini, alors $A/\mathfrak{p}$ est un corps fini de caractéristique p et E_1 est l'unique p-Sylow de E. De plus on a l'équivalence suivante :*

$$E_1 \neq 1 \iff p \mid e(\mathfrak{q} \mid \mathfrak{p})$$

et on parle alors de ramification sauvage. Dans le cas contraire on parle de ramification modérée (wild et tame en anglais).

Démonstration. Le groupe $B/\mathfrak{q}$ a pour cardinal une puissance de p et donc, d'après le théorème 9.4 et puisque $E_m = 1$ pour m assez grand, E_1 a pour cardinal une puissance de p (car E_{m-1}/E_m se plonge dans $B/\mathfrak{q}$ pour $m \geq 2$). Ensuite E/E_1 se plonge dans $(B/\mathfrak{q})^\times$ qui est un groupe fini de cardinal $p^r - 1$ avec $r \geq 1$, ce cardinal est donc premier à p. Ainsi E_1 est un p-Sylow de E, et c'est le seul car il est distingué et tous les p-Sylows sont conjugués.
En particulier E_1 est non trivial si et seulement si le cardinal de E est divisible par p, et le théorème 7.7 donne :

$$|E| = e(\mathfrak{q} \mid \mathfrak{p})$$

ce qui conclut. □

Les groupes E_m sont tous distingués dans D et on peut naturellement étudier l'action par conjugaison de D sur E_m au travers de φ_m. Pour $m \geq 1$ ça ne donne rien d'intéressant mais pour $m = 0$ on a le résultat suivant.

Proposition 9.8. *L'action par conjugaison de D sur E descend en une action sur E_0/E_1 et pour tout $\delta \in D$, $\sigma \in E_0$, on a :*

$$\varphi_0(\delta\sigma\delta^{-1}) = \delta(\varphi_0(\sigma))$$

où l'on considère que $\varphi_0(\sigma) \in \ell^\times$.
En particulier, si G est abélien, φ_0 est à valeurs dans $k^\times$ et donc E_0/E_1 se plonge dans $k^\times$.

Démonstration. L'action est bien définie sur E_0/E_1 car si $\sigma \in E_0$, $\tau \in E_1$ et $\delta \in D$, on a :

$$\delta(\sigma\tau)\delta^{-1} = (\delta\sigma\delta^{-1})(\delta\tau\delta^{-1})$$

et $\delta\tau\delta^{-1} \in E_1$.
En identifiant $\mathrm{GL}_\ell(\mathfrak{q}/\mathfrak{q}^2)$ à $\ell^\times$ on a, pour tout $x \in \mathfrak{q}$:

$$\varphi_0(\delta\sigma\delta^{-1}) \cdot x = \delta\sigma\delta^{-1}(x) = \delta\left(\varphi_0(\sigma) \cdot \delta^{-1}x\right) = \delta(\varphi_0(\sigma)) \cdot x$$

dans $\mathfrak{q}/\mathfrak{q}^2$. En appliquant ça à n'importe quel vecteur non nul de la droite $\mathfrak{q}/\mathfrak{q}^2$, on obient bien :

$$\varphi_0(\delta\sigma\delta^{-1}) = \delta(\varphi_0(\sigma)).$$

Si G est abélien, on a alors :

$$\varphi_0(\sigma) = \delta(\varphi_0(\sigma))$$

pour tous $\sigma \in E$ et $\delta \in D$. Ainsi $\varphi_0(\sigma)$ est fixé par le groupe de Galois $\overline{G}$ de l'extension ℓ/k car le morphisme $D \longrightarrow \overline{G}$ est surjectif (voir 7.9). C'est donc un élément de $k^\times$. □

9.2 Formule de Hilbert : factorisation de l'idéal différent

Comme avant, on fixe B/A une extension de Dedekind *galoisienne* de corps des fractions L/K et de groupe G, et on suppose A localement parfait (voir 5.38). On fixe aussi $\mathfrak{q}$ un premier de B au dessus de $\mathfrak{p}$ un premier de A. Le but est de démontrer la formule de Hilbert (théorème 9.11) qui donne la valuation $\mathfrak{q}$-adique de l'idéal différent $\mathrm{Diff}_{B/A}$:

$$v_{\mathfrak{q}}(\mathrm{Diff}_{B/A}) = \sum_{m\geq 0} (|E_m(\mathfrak{q} \mid \mathfrak{p})| - 1).$$

Notons que cette somme est finie car pour m assez grand les $E_m(\mathfrak{q} \mid \mathfrak{p})$ sont triviaux (voir 9.1).

Lemme 9.9. *Il suffit de prouver la formule de Hilbert dans le cas où A est un anneau de valuation discrète. Plus précisément, pour avoir la formule de Hilbert pour l'extension B/A et pour la paire $\mathfrak{q} \mid \mathfrak{p}$, il suffit de l'avoir pour l'extension $B_{\mathfrak{p}}/A_{\mathfrak{p}}$.*

Démonstration. Supposons que l'on connaisse le résultat pour l'extension $B_{\mathfrak{p}}/A_{\mathfrak{p}}$ qui est toujours une extension de Dedekind galoisienne de corps des fractions L/K et de groupe G, avec $A_{\mathfrak{p}}$ localement parfait d'après 5.38. On a alors :

$$v_{\mathfrak{q}}(\mathrm{Diff}_{B/A}) = v_{\mathfrak{q}_{\mathfrak{p}}}((\mathrm{Diff}_{B/A})_{\mathfrak{p}})$$

et donc il suffit de voir que D et les E_m ne sont pas changés en localisant : si σ stabilise $\mathfrak{q}$ alors σ stabilise aussi $\mathfrak{q}_{\mathfrak{p}}$ et la réciproque est vraie car $\mathfrak{q}_{\mathfrak{p}} \cap B = \mathfrak{q}$ (un élément dans cette intersection a une valuation $\mathfrak{q}$-adique d'au moins 1). Ensuite les E_m ne sont pas changés car pour tout $m \geq 0$:

$$B_{\mathfrak{p}}/\mathfrak{q}_{\mathfrak{p}}^{m+1} \cong B/\mathfrak{q}^{m+1}$$

car c'est déjà un $A_{\mathfrak{p}}$-module. □

On traite ensuite le cas particulier suivant.

Lemme 9.10. *On suppose que A un anneau de valuation discrète et que $\mathfrak{p}$ est totalement ramifié (i.e. $e = n$, $f = r = 1$ avec n le degré de l'extension). Alors on a :*

$$B = A[\pi]$$

et la formule de Hilbert est vraie.

Démonstration. Puisque $\mathfrak{p}$ est totalement ramifié, $\mathfrak{q}$ est le seul premier au dessus de $\mathfrak{p}$ et donc c'est le seul premier de B puisque A n'a qu'un seul premier. Donc B est un anneau de valuation discrète, et d'après 7.7, on a :

$$G = D = E$$

et le morphisme $A/\mathfrak{p} \longrightarrow B/\mathfrak{q}$ est un isomorphisme de corps. Il est donc surjectif et ainsi :

$$B = \mathfrak{q} + A$$

et ainsi, en prenant π un générateur de l'idéal principal $\mathfrak{q}$ (une uniformisante de B) :

$$B = A + \pi B = A + \pi(A + \pi B) = A + \pi A + \pi^2 B = A + \pi A + \pi^2 A + \dots \pi^n B$$

donc :

$$B = A[\pi] + \mathfrak{q}^n = A[\pi] + \mathfrak{p}B$$

ce qui donne, d'après le lemme de Nakayama, puisque B est de type fini sur l'anneau local A :

$$B = A[\pi].$$

Le polynôme minimal $g \in A[X]$ (unitaire) de π est donc de degré n et, d'après la proposition 5.32 on a :

$$\mathrm{Diff}_{B/A} = g'(\pi)B.$$

Il reste à montrer que :

$$v_\pi(g'(\pi)) = \sum_{m\geq 0}(|E_m| - 1)$$

Or on a :

$$g'(\pi) = \prod_{\sigma\in G\setminus\{1\}}(\pi - \sigma\pi) = \prod_{m\geq 1}\prod_{\sigma\in E_{m-1}\setminus E_m}(\pi - \sigma\pi)$$

en utilisant la filtration de $G = E$ par les E_m. On a alors :

$$v_\mathfrak{q}(g'(\pi)) = \sum_{m\geq 1}\sum_{\sigma\in E_{m-1}\setminus E_m} v_\mathfrak{q}(\pi - \sigma\pi) = \sum_{m\geq 1}\sum_{\sigma\in E_{m-1}\setminus E_m}(m-1)$$

par définition des E_m. Ainsi, en écrivant des sommes à support fini :

$$\begin{aligned} v_\mathfrak{q}(g'(\pi)) &= \sum_{m\geq 1}(m-1)(|E_{m-1}| - |E_m|) = \sum_{m\geq 1}(m-1)(|E_{m-1}| - 1) - \sum_{m\geq 1}(m-1)(|E_m| - 1) \\ &= \sum_{m\geq 0} m(|E_m| - 1) - \sum_{m\geq 1}(m-1)(|E_m| - 1) = \sum_{m\geq 0}(|E_m| - 1) \end{aligned}$$

ce qui achève la preuve. □

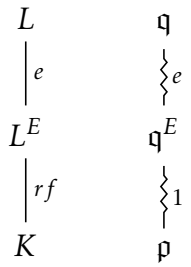
Montrons enfin la formule dans le cas général.

Théorème 9.11. *Dans le cas général (L/K galoisienne et A localement parfait), on a :*

$$v_\mathfrak{q}(\mathrm{Diff}_{B/A}) = \sum_{m\geq 0}(|E_m| - 1)$$

où $E_m = E_m(\mathfrak{q} \mid \mathfrak{p})$.

Démonstration. On considère l'extension intermédiaire associée au groupe E, L^E. Le théorème 7.7 donne le diagramme suivant :



où les traits en vagues représentent les indices de ramification. Remarquons (comme dans la preuve de la proposition 7.18) qu'on a clairement :

$$D(\mathfrak{q} \mid \mathfrak{q}^E) = D \cap \mathrm{Gal}(L/L^E)$$

et pour tout $m \geq 0$:

$$E_m(\mathfrak{q} \mid \mathfrak{q}^E) = E_m \cap \mathrm{Gal}(L/L^E)$$

Or on a $|E| = e$ et $\left|E(\mathfrak{q} \mid \mathfrak{q}^E)\right| = e(\mathfrak{q} \mid \mathfrak{q}^E) = e$ donc :

$$E(\mathfrak{q} \mid \mathfrak{q}^E) = E$$

ce qui entraîne pour tout $m \geq 0$:

$$E_m \subseteq E \subseteq \mathrm{Gal}(L/L^E)$$

et donc :

$$E_m(\mathfrak{q} \mid \mathfrak{q}^E) = E_m.$$

Le premier $\mathfrak{q}^E$ est totalement ramifié dans B car d'indice de ramification e qui est aussi le degré de L/L^E. Par le lemme 9.10, la formule de Hilbert est donc vraie pour $B_{\mathfrak{q}^E}/B^E_{\mathfrak{q}^E}$ et par le lemme 9.9, elle est vraie aussi pour la paire $\mathfrak{q} \mid \mathfrak{q}^E$ dans B/B^E. On a donc :

$$v_{\mathfrak{q}}(\mathrm{Diff}_{B/B^E}) = \sum_{m \geq 0} (\left|E_m(\mathfrak{q} \mid \mathfrak{q}^E)\right| - 1) = \sum_{m \geq 0} (|E_m - 1|)$$

par ce qui précède. On applique alors la transitivité du différent (théorème 5.33) :

$$\mathrm{Diff}_{B/A} = (\mathrm{Diff}_{B^E/A} \cdot B)\, \mathrm{Diff}_{B/B^E}$$

et ainsi :

$$v_{\mathfrak{q}}(\mathrm{Diff}_{B/A}) = \sum_{m \geq 0} (|E_m - 1|) + e \cdot v_{\mathfrak{q}^E}(\mathrm{Diff}_{B^E/A})$$

car $\mathfrak{q}^E B = \mathfrak{q}^e$. Or la paire $\mathfrak{q}^E \mid \mathfrak{p}$ n'est pas ramifiée donc le différent de B^E/A n'est pas divisible par $\mathfrak{q}^E$ d'après le théorème de Dedekind 5.41, et ainsi on a bien la formule de Hilbert dans le cas général. □

Remarque 9.12. Si A est localement fini, on retrouve le théorème de Dedekind : en effet $\sum_{m \geq 0}(|E_m - 1|) \geq e - 1$ avec égalité si et seulement si $E_1 = 1$ autrement dit $p \nmid e(\mathfrak{q} \mid \mathfrak{p})$ (avec p la caractéristique de $A/\mathfrak{p}$) d'après 9.7.

Puisque la formule de Hilbert est valable même si A n'est pas localement fini, on peut en fait améliorer la proposition 9.7.

Proposition 9.13. *Le groupe E_1 est trivial si et seulement si $\mathfrak{p} \nmid e(\mathfrak{q} \mid \mathfrak{p})$.*

Démonstration. D'après la formule de Hilbert 9.11, le groupe E_1 est trivial si et seulement si on a :

$$v_{\mathfrak{q}}(\mathrm{Diff}_{B/A}) = e - 1$$

et ceci se produit si et seulement si $\mathfrak{p} \nmid e$. □

9.3 Théorème de Kronecker-Weber

Le but de cette section est de démontrer le théorème de Kronecker-Weber, qui affirme que toute extension finie abélienne de $\mathbb{Q}$, c'est à dire toute extension finie galoisienne de $\mathbb{Q}$ de groupe de Galois abélien est contenue dans un corps cyclotomique. Ce théorème est une très belle application de la théorie algébrique des nombres et plus précisément de l'étude des groupes de ramification supérieure d'un corps de nombres. On suit la trame du chapitre 4 de [9] (exercices 29 à 36).
Avant toute chose, énonçons quelques propriétés très simples des corps de nombres abéliens et des groupes abéliens finis.

Définition 9.14. *Une extension de corps L/K est dite abélienne si elle est galoisienne, finie et de groupe de Galois abélien (on peut aussi considérer des extensions infinies mais ce ne sera pas le cas ici).*
Elle est dite cyclique si le groupe de Galois est cyclique.
Un corps de nombres abélien est une extension abélienne de $\mathbb{Q}$.
Si G est un groupe abélien fini, on note $\exp(G)$ *son exposant, c'est à dire le* ppcm *des ordres des éléments de G. On rappelle qu'il existe toujours un élément de G dont l'ordre est* $\exp(G)$*, ce qui est clair si l'on dispose du théorème de classification des groupes abéliens finis. D'ailleurs, le théorème de Lagrange impose que l'exposant de G divise l'ordre de G.*

Remarque 9.15. Si L/K est une extension abélienne, toute sous-extension E/K avec $E \subseteq L$ est aussi abélienne. En effet, $\mathrm{Gal}(L/E)$ est distingué dans $\mathrm{Gal}(L/K)$ car ce dernier est abélien, et le groupe quotient $\mathrm{Gal}(E/K)$ est alors abélien.
Si elle est de plus cyclique de degré n, la correspondance de Galois assure que les sous-extensions de L/K sont en bijection croissante avec les diviseurs de n, la bijection étant donnée par $E \mapsto [E : K]$. Ainsi pour chaque $d \mid n$ il y a un unique sous-corps de L de degré d sur K.

On laisse la proposition suivante en exercice.

Proposition 9.16. *Si G et H sont deux groupes abéliens finis, on a*

$$\exp(G \times H) = \mathrm{ppcm}(\exp(G), \exp(H)).$$

Si H est un sous-groupe d'un groupe abélien fini G, alors :

$$\exp(H) \mid \exp(G)$$

et

$$\exp(G/H) \mid \exp(G).$$

Proposition 9.17. *Soit Ω un corps, L_1 et L_2 des sous-corps de Ω et K un sous-corps de L_1 et de L_2 tel que L_1/K et L_2/K sont abéliennes. Alors L_1L_2/K est une extension abélienne et on a un morphisme de groupes injectif :*

$$\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

donné par $\sigma \mapsto (\sigma_{|L_1}, \sigma_{|L_2})$.
On a ainsi :

$$\exp(\mathrm{Gal}(L_1L_2/K)) \mid \mathrm{ppcm}(\exp(\mathrm{Gal}(L_1/K), \exp(\mathrm{Gal}(L_2/K)))).$$

De plus L_1 et L_2 sont complémentaires (voir 2.21) donc on a aussi :

$$[L_1L_2 : K] = \frac{[L_1 : K][L_2 : K]}{[L_1 \cap L_2 : K]}.$$

Démonstration. D'abord l'extension L_1L_2/K est finie et galoisienne avec la même preuve que pour le théorème 2.24. Ensuite le morphisme

$$\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

est injectif car si σ fixe L_1 et L_2 il fixe L_1L_2. Le groupe de Galois de L_1L_2/K est donc abélien et on obtient la relation sur les exposants avec la proposition 9.16.
Enfin L_1 et L_2 sont complémentaires d'après 2.24 et la formule donnée vient d'une des caractérisations de la complémentarité et de la formule de transitivité du degré des extensions de corps. □

On cherche à présent à démontrer le théorème de Kronecker-Weber :

Théorème 9.18. *(Kronecker-Weber) Tout corps de nombres abélien est contenu dans un corps cyclotomique.*

Démontrons le tout d'abord pour les corps quadratiques.

Théorème 9.19. *Soit K un corps quadratique, on note Δ la valeur absolue de son discriminant. Alors K est contenu dans le corps cyclotomique $\mathbb{Q}(\mathbb{U}_\Delta)$.*

Démonstration. D'abord, constatons que :

$$\sqrt{2} = e^{i\pi/4} + e^{-i\pi/4} \in \mathbb{Q}(\mathbb{U}_8).$$

Ensuite, si p est un nombre premier impair, le corps cyclotomique $\mathbb{Q}(\mathbb{U}_p)$ a pour discriminant :

$$\mathrm{Disc}\left(\mathbb{Q}(\mathbb{U}_p)\right) = (-1)^{\frac{p-1}{2}} p^{p-2}$$

d'après 8.10. En utilisant la formule 2.14 du discriminant via les plongements, on voit que ce discriminant est le carré d'un déterminant dont les coefficients sont des éléments de $\mathbb{Q}(\mathbb{U}_p)$ car ce corps est galoisien donc :

$$\sqrt{(-1)^{\frac{p-1}{2}} p^{p-2}} \in \mathbb{Q}(\mathbb{U}_p).$$

Ainsi, si $p \equiv 1\ [4]$, puisque $p-2$ est impair, en sortant tous les facteurs carrés de la racine on obtient que $\sqrt{p} \in \mathbb{Q}(\mathbb{U}_p)$. Si $p \equiv 3\ [4]$, on obtient $\sqrt{-p} \in \mathbb{Q}(\mathbb{U}_p)$.
Soit maintenant $d \neq 0, 1$ un entier relatif sans facteur carré et Δ la valeur absolue du discriminant de $K = \mathbb{Q}(\sqrt{d})$. Il s'agit de montrer que :

$$\sqrt{d} \in \mathbb{Q}(\mathbb{U}_\Delta).$$

Si d est pair, écrivons $d = \pm 2p_1 \dots p_r$ avec les p_j des nombres premiers impairs distincts (car d est sans facteur carré). Puisque d est pair on a $\Delta = 4|d|$ par 6.9. On a alors, par ce qui précède pour tout j :

$$\sqrt{p_j} \in \mathbb{Q}(\mathbb{U}_{p_j}, i)$$

peu importe la congruence de p_j modulo 4. De plus $\sqrt{\pm 2} \in \mathbb{Q}(\mathbb{U}_8)$ et $\mathbb{Q}(\mathbb{U}_8)$ contient i, donc :

$$\sqrt{d} \in \mathbb{Q}(\mathbb{U}_8)\mathbb{Q}(\mathbb{U}_{p_1})\dots\mathbb{Q}(\mathbb{U}_{p_r}) = \mathbb{Q}(\mathbb{U}_{4|d|})$$

d'après la proposition 8.7.
Supposons maintenant d impair. On écrit $d = (-1)^k p_1 \dots p_r$ avec les p_j impairs, et $k \in \{0,1\}$.
Si $d \equiv 3\ [4]$, on a $\Delta = 4|d|$ et par ce qui précède :

$$\sqrt{d} \in \mathbb{Q}(i)\mathbb{Q}(\mathbb{U}_{p_1})\dots\mathbb{Q}(\mathbb{U}_{p_r}) = \mathbb{Q}(\mathbb{U}_{4|d|}).$$

Si $d \equiv 1\ [4]$, on a $\Delta = |d|$. Notons s le nombre de p_j qui sont congrus à 3 modulo 4. Sans perte de généralité, ce sont $p_1, \dots, p_s$. On a donc :

$$1 \equiv d \equiv (-1)^k(-1)^s\ [4]$$

donc $k+s$ est pair, i.e. $k \equiv s\ [2]$. Ainsi :

$$d = \prod_{j=1}^{s}(-p_j)\prod_{j=s+1}^{r} p_j$$

de sorte que :

$$\sqrt{d} = \prod_{j=1}^{s}\sqrt{-p_j}\prod_{j=s+1}^{r}\sqrt{p_j} \in \mathbb{Q}(\mathbb{U}_{p_1})\dots\mathbb{Q}(\mathbb{U}_{p_r}) = \mathbb{Q}(\mathbb{U}_{|d|})$$

comme voulu. □

On va ensuite réduire la preuve du théorème de Kronecker-Weber au cas des corps de type p que l'on définit ainsi.

Définition 9.20. *Soit p un nombre premier. Un corps de type p est un corps de nombres abélien dont le degré est une puissance de p et dont le discriminant est une puissance de p au signe près (cette deuxième condition équivaut à ce que seul p puisse être éventuellement ramifié dans K).*

La famille des corps de type p est stable par sous-corps et par compositum.

Proposition 9.21. *Le compositum de deux corps de type p est un corps de type p et tout sous-corps d'un corps de type p est un corps de type p.*

Démonstration. Si $K \subseteq L$ avec L un corps de type p, alors la remarque 9.15 assure que K est abélien et son groupe de Galois est un quotient d'un groupe dont le cardinal est une puissance de p donc le degré de K est une puissance de p. Enfin si q est un nombre premier ramifié dans K, la transitivité de l'indice de ramificaiton assure que q est ramifié dans L donc que $q = p$.
Si K et L sont deux corps de type p, le groupe de Galois $\mathrm{Gal}(KL/\mathbb{Q})$ se plonge dans $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ donc son ordre est une puissance de p, et le corollaire 7.19 assure que seul p peut être ramifié dans KL. □

Dans un corps de type p, le nombre premier p est toujours totalement ramifié.

Proposition 9.22. *Soit K un corps de type p. Alors p est totalement ramifié, c'est à dire qu'il n'a qu'un seul premier $\mathfrak{p}$ au dessus de lui et que $f(\mathfrak{p} \mid p) = 1$. De plus, on a :*

$$E_1(\mathfrak{p} \mid p) = E(\mathfrak{p} \mid p) = G$$

avec $G = \mathrm{Gal}(K/\mathbb{Q})$.

Démonstration. Notons p^m le degré de $K/\mathbb{Q}$. Considérons $\mathfrak{p}$ un premier quelconque au dessus de p : on verra dans la suite qu'il n'y en a qu'un. Le calcul des indices, avec les notations du théorème 7.7, montre que :

$$e(\mathfrak{p}^E \mid p) = 1$$

et donc que p n'est pas ramifié dans K^E. Or K est de type p donc tout nombre premier $q \neq p$ est aussi non ramifié dans K et donc dans K^E. Ainsi aucun nombre premier ne se ramifie dans K^E, et donc $\left|\mathrm{Disc}(K^E)\right| = 1$ ce qui impose, par le théorème 6.19 que ;

$$K^E = \mathbb{Q}$$

autrement dit que $f(p) = r(p) = 1$ et que $e(p) = p^m$. Ainsi p est totalement ramifié dans K.
En particulier on a $E = G$ qui est de cardinal p^m, donc son seul p-Sylow, à savoir E_1 (d'après 9.7) est E :

$$E_1 = E.$$

□

9.3.1 Réduction au cas des corps de type p

Lemme 9.23. *Il suffit de montrer le théorème de Kronecker-Weber pour les corps abéliens dont le degré est une puissance de p.*

Démonstration. Si K est un corps de nombres abélien de groupe de Galois G, le théorème de classification des groupes abéliens finis permet d'écrire :

$$G = \bigoplus_p G_p$$

avec G_p un groupe abélien fini d'ordre une puissance de p. On considère alors les sous-groupes $H_p = \bigoplus_{q \neq p} G_q$ de G de sorte que :

$$\bigcap_p H_p = 0.$$

Ainsi par la correspondance de Galois 2.17 on a :

$$K = \prod_p K^{H_p}$$

et si on sait plonger les K^{H_p} dans des corps cyclotomiques, on sait plonger K dans un corps cyclotomique puisque la famille des corps cyclotomiques est stable par compositum (voir 8.7). Or pour tout p le corps K^{H_p} est un corps de degré $\left|G/H_p\right| = \left|G_p\right|$ qui est une puissance de p. Il suffit donc de démontrer le théorème de Kronecker-Weber pour les corps abéliens de degré une puissance d'un nombre premier. □

Lemme 9.24. *Soit p un nombre premier et K un corps de nombres abélien de degré p^m avec $m \geq 0$ et $q \neq p$ un nombre premier ramifié dans K. Alors il existe K' un corps de nombres abélien dont le degré est une puissance de p, avec q non ramifié dans K' et tous les premiers non ramifiés dans K qui restent non ramifiés dans K', tel que, si K' est contenu dans un corps cyclotomique, alors K aussi.*

Démonstration. Puisque q est ramifié, on a $m \geq 1$. Choisissons $\mathfrak{q}$ un premier de K au dessus de q et remarquons que l'indice de ramification $e(q)$ (indépendant de $\mathfrak{q}$ car l'extension est galoisienne) n'est pas divisible par q, sans quoi on aurait $q \mid e(q) \mid [K : \mathbb{Q}] = p^m$. On est donc dans un cas de ramification modérée (voir 9.7).
Ainsi $E_1(\mathfrak{q} \mid q) = 1$ et la proposition 9.8 donne un plongement :

$$E = E/E_1 \hookrightarrow \mathbb{F}_q^\times$$

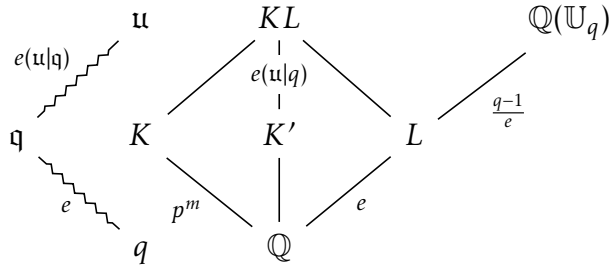
car le groupe de Galois de $K/\mathbb{Q}$ est abélien. Ainsi on a :

$$e(q) \mid q - 1.$$

On considère à présent le corps cyclotomique $\mathbb{Q}(\mathbb{U}_q)$ dont le groupe de Galois est cyclique d'ordre $q-1$ puisqu'il est isomorphe à $(\mathbb{Z}/q\mathbb{Z})^\times$. D'après la remarque 9.15, il existe donc un unique sous-corps L de $\mathbb{Q}(\mathbb{U}_q)$ de degré $e(q)$ sur $\mathbb{Q}$ puisque $e(q) \mid q-1$.
On choisit alors $\mathfrak{u}$ un premier de KL au dessus de $\mathfrak{q}$ et on considère le corps :

$$K' = (KL)^{E(\mathfrak{u}|q)}$$

où q désigne bien le nombre premier q et non l'idéal premier $\mathfrak{q}$. Dans la suite on pose $e = e(\mathfrak{q} \mid q)$. On a la situation suivante, où les traits en vague désignent les indices de ramification :



D'après le théorème 7.7, q n'est pas ramifié dans K' (l'extension est galoisienne donc il suffit de voir que $e\left(\mathfrak{u}^{E(\mathfrak{u}|q)} \mid q\right) = 1$).
De plus, tout nombre premier ℓ non ramifié dans K est non ramifié dans K' : en effet un tel ℓ est nécessairement différent de q car q est ramifié dans K donc ℓ est non ramifié dans $\mathbb{Q}(\mathbb{U}_q)$ (le seul premier ramifié dans $\mathbb{Q}(\mathbb{U}_q)$ étant q d'après 8.10) et donc il n'est pas ramifié dans KL d'après 7.19 et il ne l'est pas non plus dans $K' \subseteq KL$ par la formule

de transitivité des indices de ramification.
On montre maintenant que :

$$K'L = KL.$$

Remarquons d'abord que le plongement $\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ envoie $E(\mathfrak{u} \mid q)$ dans $E(\mathfrak{q} \mid q) \times \mathrm{Gal}(L/\mathbb{Q})$ de sorte que :

$$e(\mathfrak{u} \mid q) \mid e^2 \mid p^{2m}$$

donc $e(\mathfrak{u} \mid q)$ est une puissance de p. Ainsi on a $q \nmid e(\mathfrak{u} \mid q)$ et donc la ramificaiton $\mathfrak{u} \mid q$ est modérée et $E_1(\mathfrak{u} \mid q) = 1$. Encore une fois cela donne un plongement de $E(\mathfrak{u} \mid q)$ dans $\mathbb{F}_q^\times$, ce qui implique que $E(\mathfrak{u} \mid q)$ est un groupe cyclique, dont le cardinal est donc égal à l'exposant. Or par le plongement :

$$E(\mathfrak{u} \mid q) \hookrightarrow E(\mathfrak{q} \mid q) \times \mathrm{Gal}(L/\mathbb{Q})$$

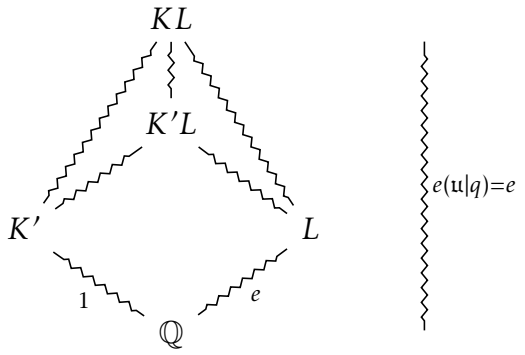
cet exposant divise le ppcm des exposants de $E(\mathfrak{q} \mid q)$ et de $\mathrm{Gal}(L/\mathbb{Q})$ qui divisent tous les deux e (par le théorème de Lagrange). On a donc :

$$e(\mathfrak{u} \mid q) \mid e$$

et d'autre part la formule de transitivité des indices de ramification donne $e \mid e(\mathfrak{u} \mid q)$ donc :

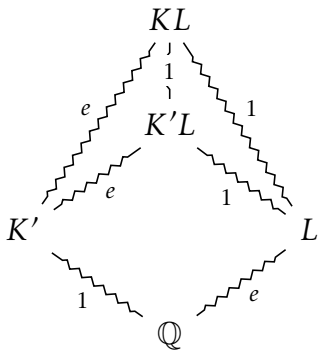
$$e(\mathfrak{u} \mid q) = e.$$

Rappelons que q est totalement ramifié dans $\mathbb{Q}(\mathbb{U}_q)$, d'indice de ramification $q-1$ (théorème 8.9), et donc son indice d'inertie dans l'extension $\mathbb{Q}(\mathbb{U}_q)/\mathbb{Q}$ vaut 1. C'est donc aussi le cas dans l'extension $L/\mathbb{Q}$ et il y a toujours un seul premier au dessus de q dans L (sinon il y en aurait plusieurs dans $\mathbb{Q}(\mathbb{U}_q)$). Ainsi q est totalement ramifié dans L, d'indice $[L : \mathbb{Q}] = e$ et on a donc la situation suivante au niveau des indices de ramification des idéaux au dessus de q (pour KL, on prend $\mathfrak{u}$ et on le tire en arrière dans les autres corps qui apparaissent sur le diagramme) :



car on avait montré que q n'est pas ramifié dans K'. Par multiplicativité des indices on

peut compléter ce diagramme :



en utilisant que le seul diviseur de 1 est 1. Par construction on a :

$$[KL : K'] = |E(\mathfrak{u} \mid \mathfrak{q})| = e$$

et $[K'L : K'] \geq e$ car le degré est divisible par l'indice de ramification, donc :

$$[KL : K'L] \leq \frac{e}{e} = 1$$

donc $KL = K'L$ comme souhaité.
Le degré de K' est une puissance de p car c'est le cas de KL puisque le degré de KL divise $[K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$ et que e est une puissance de p. Enfin, si K' est contenu dans un corps cyclotomique $\mathbb{Q}(\mathbb{U}_t)$, alors on a :

$$K \subseteq KL = K'L \subseteq \mathbb{Q}(\mathbb{U}_t)\mathbb{Q}(\mathbb{U}_q) \subseteq \mathbb{Q}\left((\mathbb{U}_{\text{ppcm}(t,q)}\right)$$

ce qui achève la preuve. □

En appliquant le lemme 9.23 puis le lemme 9.24 autant de fois qu'il y a de nombres premiers différents de p ramifiés dans K, on se ramène au cas où K est de type p. On a donc prouvé le lemme suivant :

Lemme 9.25. *Il suffit de prouver le théorème de Kronecker-Weber pour les corps de type p pour tout nombre premier p.*

9.3.2 Cas des corps de type p impair

Soit p un nombre premier impair. On rappelle que, par la proposition 9.22, p est totalement ramifié dans tout corps de type p.
On va faire mieux que de démontrer le théorème de Kronecker-Weber pour les corps de type p : on va montrer qu'il existe un unique corps de type p de degré p^m pour tout $m \geq 1$, et que cet unique corps est contenu dans $\mathbb{Q}(\mathbb{U}_{p^{m+1}})$ (théorème 9.28).
On commence par étudier le cas $m = 1$.

Lemme 9.26. *Soit K un corps de type p de degré p. On note $\mathfrak{p}$ l'unique premier au dessus de p. On a alors :*

$$\text{Diff}_{\mathcal{O}_K/\mathbb{Z}} = \mathfrak{p}^{2p-1}.$$

Démonstration. Puisque $\mathfrak{p}$ est le seul premier ramifié de K, l'idéal différent est une puissance de $\mathfrak{p}$ et il suffit de déterminer la valuation $\mathfrak{p}$-adique du différent, que l'on noté v. Or on a :

$$v = \sum_{m \geq 0} (|E_m| - 1)$$

avec $E_m = E_m(\mathfrak{p} \mid p)$ d'après la formule de Hilbert 9.11. Puisque les E_m sont des sous-groupes du groupe de Galois qui est d'ordre p, on a $|E_m| \in \{1, p\}$ et donc :

$$p - 1 \mid v.$$

On choisit à présent ϖ une uniformisante de $\mathfrak{p}$, c'est à dire un élément de $\mathfrak{p} \setminus \mathfrak{p}^2$. Si ϖ était dans $\mathbb{Q}$, on aurait :

$$1 = v_{\mathfrak{p}}(\varpi) = e(\mathfrak{p} \mid p) v_p(\varpi) = p v_p(\varpi)$$

ce qui est impossible, donc $\varpi \notin \mathbb{Q}$. On considère f le polynôme minimal de ϖ :

$$f = \sum_{i=0}^{p} a_i X^i$$

avec $a_i \in \mathbb{Z}$ et $a_p = 1$ car ϖ est un entier algébrique irrationnel dont le degré divise p (car il appartient à K). Ce polynôme s'écrit aussi, en notant $G = \mathrm{Gal}(K/\mathbb{Q})$:

$$f = \prod_{\sigma \in G} (X - \sigma(\varpi))$$

et sa réduction dans $\mathcal{O}_K/\mathfrak{p}[X]$ donne donc :

$$\overline{f} = X^p$$

car les $\sigma(\varpi)$ sont tous dans $\mathfrak{q}$ (ici $D(\mathfrak{p} \mid p) = G$ car p est totalement ramifié). Ainsi les a_i pour $i < p$ sont divisibles par p (c'est un raisonnement qu'on retrouvera dans l'étude des extensions totalement ramifiées de corps locaux, voir 14.34).
On a alors :

$$f'(\varpi) = \sum_{i=1}^{p} a_i i \varpi^{i-1}$$

et on remarque que :

$$v_{\mathfrak{p}}(a_i i \varpi^{i-1}) = p v_p(a_i) + p v_p(i) + i - 1 \equiv i - 1 \ [p]$$

donc ces valuations sont deux à deux distinctes et ainsi :

$$v_{\mathfrak{p}}(f'(\varpi)) = \min_{1 \leq i \leq p} (p v_p(a_i) + p v_p(i) + i - 1)$$

On peut donc encadrer cette valuation (en utilisant que $a_p = 1$ et que les autres a_i sont divisibles par p) :

$$p \leq v_{\mathfrak{p}}(f'(\varpi)) \leq 2p - 1.$$

D'après le lemme 9.10, puisque p est totalement ramifié, les localisations suivantes sont égales :

$$\mathbb{Z}[\varpi]_{\mathfrak{p}} = (\mathcal{O}_K)_{\mathfrak{p}}.$$

Ainsi, par la proposition 5.32 on a :

$$v = v_{\mathfrak{p}}(f'(\varpi))$$

et le seul multiple de $p-1$ entre p et $2p-1$ est $2p-2$ (c'est ici qu'on utilise que p est impair). On a donc bien :

$$v = 2p-2.$$

□

Dans le cas $m = 2$, on montre qu'une telle extension est toujours cyclique.

Lemme 9.27. *Soit K un corps de type p de degré p^2. Alors le groupe de Galois* $\mathrm{Gal}(K/\mathbb{Q})$ *est cyclique.*

Démonstration. Pour montrer que l'extension $K/\mathbb{Q}$ est cyclique, la correspondance de Galois assure qu'il suffit de montrer qu'il n'y a qu'une seule sous-extension de degré p : en effet cela revient à montrer qu'il n'y a qu'un seul sous-groupe de $G = \mathrm{Gal}(K/\mathbb{Q})$ de degré p, et le seul groupe abélien d'ordre p^2 qui vérifie cela est $\mathbb{Z}/p^2\mathbb{Z}$. On va donc montrer qu'il n'y a qu'un seul sous-corps de K de degré p.
Pour cela, on fait l'observation suivante : Soit L un sous-corps de K de degré p. La formule de transitivité de l'idéal différent 5.33 donne :

$$\mathrm{Diff}_{\mathcal{O}_K/\mathbb{Z}} = \mathrm{Diff}_{\mathcal{O}_K/\mathcal{O}_L} \cdot \left(\mathrm{Diff}_{\mathcal{O}_L/\mathbb{Z}} \cdot \mathcal{O}_K\right)$$

et le lemme précédent 9.26 assure que $\mathrm{Diff}_{\mathcal{O}_L/\mathbb{Z}} = (\mathfrak{p} \cap L)^{2(p-1)}$. Or on a $e(\mathfrak{p} \cap L \mid p) = p$ car p est totalement ramifié dans L et donc $e(\mathfrak{p} \mid \mathfrak{p} \cap L) = p$ et :

$$\mathrm{Diff}_{\mathcal{O}_L/\mathbb{Z}} \cdot \mathcal{O}_K = \mathfrak{p}^{2p(p-1)}$$

de sorte que :

$$\mathrm{Diff}_{\mathcal{O}_K/\mathcal{O}_L} = \mathfrak{p}^{-2p(p-1)} \mathrm{Diff}_{\mathcal{O}_K/\mathbb{Z}}.$$

Ainsi cet idéal différent est indépendant de l'extension L choisie.
Ensuite, notons qu'on a pour tout $m \geq 0$:

$$E_m(\mathfrak{p} \mid \mathfrak{p} \cap L) = E_m(\mathfrak{p} \mid p) \cap \mathrm{Gal}(K/L).$$

La formule de Hilbert 9.11 donne alors :

$$v_{\mathfrak{p}}(\mathrm{Diff}_{\mathcal{O}_K/\mathcal{O}_L}) = \sum_{m \geq 0} (|E_m(\mathfrak{p} \mid \mathfrak{p} \cap L)| - 1) = \sum_{m \geq 0} (|E_m(\mathfrak{p} \mid p) \cap \mathrm{Gal}(K/L)| - 1)$$

D'après la proposition 9.22, on a $E_1(\mathfrak{p} \mid p) = G$ et puisque pour m assez grand, $E_m(\mathfrak{p} \mid p) = 1$, il existe $r \geq 2$ minimal tel que $E_r(\mathfrak{p} \mid p) \neq G$. Ainsi on a :

$$G = E_0(\mathfrak{p} \mid p) = E_1(\mathfrak{p} \mid p) = \cdots = E_{r-1}(\mathfrak{p} \mid p) \supsetneq E_r(\mathfrak{p} \mid p).$$

De plus, le quotient E_{r-1}/E_r se plonge dans un $\mathcal{O}_K/\mathfrak{p}$-espace vectoriel de dimension 1 d'après 9.4 puisque $r-1 \geq 1$, et on a $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$ car $f(\mathfrak{p} \mid p) = 1$. Donc E_{r-1}/E_r est de cardinal divisant p, et ainsi :

$$|E_r(\mathfrak{p} \mid p)| = p.$$

Ainsi on a :

$$\begin{aligned} v_{\mathfrak{p}}(\mathrm{Diff}_{\mathcal{O}_K/\mathcal{O}_L}) &= \sum_{m=0}^{r-1} (|\mathrm{Gal}(K/L)| - 1) + \sum_{m \geq r} (|E_m(\mathfrak{p} \mid p) \cap \mathrm{Gal}(K/L)| - 1) \\ &= r(p-1) + \sum_{m \geq r} (|E_m(\mathfrak{p} \mid p) \cap \mathrm{Gal}(K/L)| - 1). \end{aligned}$$

Or cette valuation est indépendante de L comme vu plus haut, donc la quantité :

$$C(L) = \sum_{m \geq r} (|E_m(\mathfrak{p} \mid p) \cap \mathrm{Gal}(K/L)| - 1)$$

est aussi indépendante de L. Or pour $L = K^{E_r}$, cette quantité est strictement maximale. En effet on a :

$$C\left(K^{E_r}\right) = p - 1 + \sum_{m > r} (|E_m| - 1)$$

et pour $L \neq K^{E_r}$ on a :

$$C(L) = 0$$

car l'intersection de deux sous-groupes d'ordre divisant p distincts est le groupe trivial. Puisque $C(L)$ ne dépend pas de L, on en déduit que K^{E_r} est le seul sous-corps de K de degré p, ce qui conclut la preuve. □

On peut à présent classifier les corps de type p impair par leur degré.

Théorème 9.28. *Soit $p \geq 3$ un nombre premier et $m \geq 0$ un entier. Il existe un unique corps de type p de degré p^m, que l'on note $K_{p,m}$. C'est une extension cyclique de $\mathbb{Q}$, et c'est le seul sous-corps du corps cyclotomique $\mathbb{Q}(\mathbb{U}_{p^{m+1}})$ qui soit de degré p^m.*
De plus, si $m \leq n$, on a :

$$K_{p,m} \subseteq K_{p,n}.$$

Démonstration. On commence par traiter l'unicité dans le cas $m = 1$. On se donne K et L deux corps de type p de degré p et on veut voir que $K = L$. On considère le corps KL, qui est encore de type p d'après 9.21. Si KL est de degré p, on a $K = L$. Sinon, il est de degré p^2 car le groupe de Galois de KL se plonge dans $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$, et donc le lemme 9.27 s'applique : l'extension $KL/\mathbb{Q}$ est cyclique et donc $L = K$ est le seul-sous-corps de degré p.
On prend $m \geq 0$ quelconque à présent, et on considère le corps cyclotomique $\mathbb{Q}(\mathbb{U}_{p^{m+1}})$ dont le groupe de Galois est isomorphe à $\left(\mathbb{Z}/p^{m+1}\mathbb{Z}\right)^\times$ qui est cyclique d'après le théorème 1.59 car p est impair. Ainsi ce corps a un unique sous-corps $K_{p,m}$ de degré p^m car $p^m \mid \varphi(p^{m+1})$. Or on sait que seul p est ramifié dans $\mathbb{Q}(\mathbb{U}_{p^m})$ d'après 8.10 donc $K_{p,m}$ est bien de type p, et c'est une extension cyclique de $\mathbb{Q}$ car tout quotient d'un groupe cyclique est un groupe cyclique.

Il est clair que si $m \leq n$, on a $\mathbb{Q}(\mathbb{U}_{p^{m+1}}) \subseteq \mathbb{Q}(\mathbb{U}_{p^{n+1}})$ et donc $K_{p,m} \subseteq K_{p,n}$ car les sous-corps d'un corps cyclique sont ordonnés par la divisibilité de leur degré.
On se donne alors K un corps de type p de degré p^m et on montre que $K = K_{p,m}$. On peut clairement supposer $m \geq 1$. Considérons σ un générateurde $\mathrm{Gal}(K_{p,m}/\mathbb{Q})$ et $\tau \in \mathrm{Gal}(KK_{p,m}/\mathbb{Q})$ un antécédent de σ par le morphisme surjectif de restriction :

$$\mathrm{Gal}(KK_{p,m}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K_{p,m}/\mathbb{Q}).$$

On pose alors :

$$F = (KK_{p,m})^{\tau}$$

le sous-corps de $KK_{p,m}$ fixé par τ. Notons que :

$$F \cap K_{p,m} = K_{p,m}^{\tau} = K_{p,m}^{\sigma} = \mathbb{Q}$$

car σ génère le groupe de Galois de $K_{p,m}/\mathbb{Q}$.
Supposons que $F \neq \mathbb{Q}$. Le degré de F est alors une puissance de p non triviale et la théorie de Sylow assure que $\mathrm{Gal}(F/\mathbb{Q})$ possède un sous-groupe d'indice p et donc, par la correspondance de Galois, F contient un sous-corps de degré p. Ce sous-corps est de type p et de degré p, donc par l'unicité dans le cas $m = 1$, c'est nécessairement le corps $K_{p,1}$:

$$K_{p,1} \subseteq F.$$

Or on a $K_{p,1} \subseteq K_{p,m}$ car $m \geq 1$, donc $K_{p,1} \subseteq F \cap K_{p,m} = \mathbb{Q}$, ce qui est absurde. Ainsi on a montré :

$$F = \mathbb{Q}$$

et donc que τ engendre le groupe de Galois de $KK_{p,m}$. L'extension $KK_{p,m}$ est donc cyclique et les sous-corps K et $K_{p,m}$, ayant le même degré, sont égaux (voir la remarque 9.15). □

Ce théorème implique le théorème de Kronecker-Weber pour les corps de type $p \geq 3$. Il reste à traiter le cas $p = 2$ pour conclure.

9.3.3 Cas des corps de type 2

Contrairement au cas p impair, il n'y a plus unicité des corps de type 2 de degré fixé. On peut quand même tous les lister pour $m = 1$.

Lemme 9.29. *Les corps de type 2 de degré 2 sont $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{-2})$.*
On a de plus :

$$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\mathbb{U}_8)$$

et :

$$\mathbb{Q}(i) \subseteq \mathbb{Q}(\mathbb{U}_4).$$

Démonstration. Il suffit d'utiliser la formule du discriminant d'un corps quadratique 6.9. Elle impose que $K = \mathbb{Q}(\sqrt{d})$ avec $|d|$ une puissance de 2 sans facteur carré différente de 0 et 1, donc $d \in \{-2, -1, 2\}$. Réciproquement, le discriminant de ces corps quadratiques est toujours une puissance de 2.

On a clairement $\mathbb{Q}(\mathbb{U}_4) = \mathbb{Q}(i)$ et en notant $\omega = \frac{\sqrt{2}}{2}(1+i) = e^{\frac{2i\pi}{8}}$ un générateur de $\mathbb{U}_8$, on a :

$$\sqrt{2} = \omega + \omega^7 \in \mathbb{Q}(\mathbb{U}_8)$$

et :

$$\sqrt{-2} = \pm\left(\omega - \omega^7\right) \in \mathbb{Q}(\mathbb{U}_8)$$

comme voulu. □

Lemme 9.30. *Soit K un corps de type 2 de degré au moins 4. Alors K contient le nombre $\sqrt{2}$.*

Démonstration. On pose $K' = K \cap \mathbb{R}$, qui est encore de type 2 et contenu dans $\mathbb{R}$. Puisque K' est le sous-corps de K fixé par l'automorphisme $z \mapsto \overline{z}$, on a :

$$[K : K'] \leq 2$$

et donc $K' \neq \mathbb{Q}$ car $[K : \mathbb{Q}] \geq 4$. Par la théorie de Sylow, $\mathrm{Gal}(K'/\mathbb{Q})$ possède donc un sous-groupe d'indice 2 et par la correspondance de Galois, K' possède ainsi un sous-corps quadratique. Ainsi K possède un sous-corps quadratique de type 2 contenu dans $\mathbb{R}$, et le lemme 9.29 assure que c'est $\mathbb{Q}(\sqrt{2})$. □

On peut alors montrer le théorème de Kronecker-Weber pour les corps de type 2.

Proposition 9.31. *Tout corps de type 2 est contenu dans un corps cyclotomique. Plus précisément, si K est de type 2 et de degré 2^m, alors :*

$$K \subseteq \mathbb{Q}(\mathbb{U}_{2^{m+2}}).$$

Démonstration. On peut clairement supposer $m \geq 2$ d'après le lemme 9.29. Ainsi par le lemme 9.30, on a :

$$\mathbb{Q}(\sqrt{2}) \subseteq K.$$

On considère maintenant le corps :

$$L = \mathbb{Q}(\mathbb{U}_{2^{m+2}}) \cap \mathbb{R}.$$

C'est un corps de nombres abéliens de groupe de Galois :

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\mathbb{U}_{2^{m+2}})/\mathbb{Q})/\langle z \mapsto \overline{z}\rangle \cong \left(\mathbb{Z}/2^{m+2}\mathbb{Z}\right)^\times/\langle -1\rangle.$$

Ce groupe est cyclique d'après le théorème 1.59, donc $L/\mathbb{Q}$ est une extension cyclique de degré $\varphi(2^{m+2})/2 = 2^m$. On se donne σ un générateur de $\mathrm{Gal}(L/\mathbb{Q})$ et τ un antécédent de σ par le morphisme surjectif de restriction :

$$\mathrm{Gal}(KL/\mathbb{Q}) \longrightarrow \mathrm{Gal}(L/\mathbb{Q}).$$

On considère alors $F = (KL)^\tau$ de sorte que :

$$F \cap L = L^\sigma = \mathbb{Q}.$$

On sait que seul 2 peut se ramifier dans $\mathbb{Q}(\mathbb{U}_{2^{m+2}})$ d'après le théorème 8.10 donc L est de type 2 et KL et F aussi d'après 9.21.
Par le lemme 9.30, on a que $\sqrt{2} \in L$ car L est de type 2 et de degré au moins 4, et donc $\sqrt{2} \notin F$ sans quoi on aurait $\sqrt{2} \in F \cap L = \mathbb{Q}$. Donc $[F : \mathbb{Q}] \leq 2$, toujours d'après le lemme 9.30.
Ainsi, d'après le lemme 9.29, on a :

$$F = \mathbb{Q}, \mathbb{Q}(i) \text{ ou } \mathbb{Q}(\sqrt{-2}).$$

On va à présent déterminer l'ordre ω de τ dans le groupe $\mathrm{Gal}(KL/\mathbb{Q})$. Naturellement, l'ordre de σ dans $\mathrm{Gal}(L/\mathbb{Q})$ divise ω car σ est l'image de τ par un morphisme de groupes :

$$2^m \mid \omega.$$

De plus, on a :

$$\exp(\mathrm{Gal}(KL/\mathbb{Q})) \mid \mathrm{ppcm}(\exp(\mathrm{Gal}(K/\mathbb{Q}), \exp(L/\mathbb{Q})))$$

d'après la proposition 9.17, et en particulier :

$$\omega \mid 2^m$$

donc :

$$\omega = 2^m.$$

Or on a $\mathrm{Gal}(KL/F) = \langle \tau \rangle$ donc $[KL : F] = 2^m$ et par complémentarité de K et L (voir la proposition 9.17) :

$$[KL : \mathbb{Q}] = \frac{[K : \mathbb{Q}][L : \mathbb{Q}]}{[K \cap L : \mathbb{Q}]} = \frac{2^{2m}}{[K \cap L : \mathbb{Q}]}.$$

Il y a alors deux cas à traiter pour conclure.
Si $F = \mathbb{Q}$, on a alors :

$$[K \cap L : \mathbb{Q}] = \frac{2^{2m}}{[KL : F]} = 2^m = [K : \mathbb{Q}] = [L : \mathbb{Q}]$$

donc $K = L$ et K est ainsi contenu dans le corps cyclotomique $\mathbb{Q}(\mathbb{U}_{2^{m+2}})$.
Si $F \neq \mathbb{Q}$, F est quadratique et donc :

$$[K \cap L : \mathbb{Q}] = \frac{2^{2m}}{[KL : \mathbb{Q}]} = \frac{2^{2m}}{[KL : F] \cdot [F : \mathbb{Q}]} = 2^{m-1}.$$

De plus, dans ce cas on a $F \not\subseteq \mathbb{R}$ donc $KL \not\subseteq \mathbb{R}$, or $L \subseteq \mathbb{R}$, donc K n'est pas contenu dans $\mathbb{R}$. Ainsi $[K \cap \mathbb{R} : \mathbb{Q}] = 2^{m-1}$ car la conjugaison complexe est un automorphisme d'ordre 2 sur K, et puisque $K \cap L \subseteq K \cap \mathbb{R}$ et que ces deux corps sont de degré 2^{m-1}, on a :

$$K \cap L = K \cap \mathbb{R}.$$

Ainsi par complémentarité :

$$[FL : \mathbb{Q}] = \frac{[F : \mathbb{Q}][L : \mathbb{Q}]}{[F \cap L : \mathbb{Q}]} = 2^{m+1}$$

et :

$$[KL : \mathbb{Q}] = \frac{2^{2m}}{[K \cap L : \mathbb{Q}]} = 2^{m+1}.$$

Or $FL \subseteq KL$ donc $FL = KL$ et :

$$K \subseteq KL \subseteq FL \subseteq \mathbb{Q}(\mathbb{U}_{2^{m+2}})$$

car $F \subseteq \mathbb{Q}(\mathbb{U}_8)$, ce qui achève la preuve. □

Le lemme 9.25, le théorème 9.28 et la proposition 9.31 démontrent le théorème de Kronecker-Weber 9.18.

Chapitre 10

Théorie du genre de Gauss pour les corps quadratiques

Déterminer le groupe des classes d'un corps de nombres est une tâche difficile et on ne dispose pas de beaucoup de résultats généraux dans cette direction. La théorie du genre de Gauss est un des rares résultats explicites sur le groupe des classes, ou plutôt sur la 2-torsion d'une version un peu modifiée du groupe des classes. Elle s'applique uniquement dans un cas très particulier : celui des corps quadratiques. La théorie du corps de classe apporte en fait quelques généralisations, d'une part pour certains corps multiquadratiques (voir l'article de Pagano et Koymans [6]) et d'autre part pour les extensions quadratiques de corps de nombres (voir l'article de Kluners et Wang [4]). Cela dit, dans le deuxième cas, ce n'est pas un résultat explicite mais une borne supérieure.
Avant de présenter la théorie du genre de Gauss, mentionnons le résultat suivant :

Théorème 10.1. *(Stark, Heegner) Les seuls corps quadratiques imaginaires dont l'anneau d'entier est principal sont les* $\mathbb{Q}(\sqrt{-d})$ *avec :*

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Là encore, il s'agit d'un des rares énoncés explicites sur la question du groupe des classes d'un corps de nombres. Pour les corps quadratiques réels, on ne sait même pas à ce jour s'il existe une infinité de corps quadratiques réels dont l'anneau des entiers est principal.
La théorie du genre de Gauss, énoncée et démontrée par Gauss dans le langage des formes quadratiques à coefficients entiers, se reformule aujourd'hui au travers du groupe des casses restreint d'un corps quadratique.
Dans la suite, on se permettra de noter $\mathcal{F}(K)$ et $\mathrm{Princ}(K)$ au lieu de $\mathcal{F}(\mathcal{O}_K)$ et $\mathrm{Princ}(\mathcal{O}_K)$.

10.1 Le groupe des classes restreint d'un corps de nombres

Définition 10.2. *Soit K un corps de nombres. Un élément x de $K^\times$ est dit totalement positif si pour tout $\sigma : K \longrightarrow \mathbb{R}$ un plongement réel, on a $\sigma(x) > 0$. On note K^+ le sous-groupe de $K^\times$ formé des éléments totalement positifs. En d'autres termes, on a une suite exacte :*

$$1 \longrightarrow K^+ \longrightarrow K^\times \longrightarrow \{\pm 1\}^r \longrightarrow 1$$

où r est le nombre de plongements réels de K et le morphisme $K^\times \longrightarrow \{\pm 1\}^r$ envoie x sur la famille des signes de $\sigma(x)$ où σ parcourt les plongements réels de K.
Notons que ce morphisme est surjectif car K est dense dans $K_\mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$ et donc il existe des éléments de K qui, vus dans $K_\mathbb{R}$, ont leurs r premières coordonnées de signes arbitraires.
Un idéal fractionnaire principal est dit totalement positif s'il est engendré par un élément de K^+. On note $\mathrm{Princ}^+(K)$ *le sous-groupe de* $\mathrm{Princ}(K)$ *formé des idéaux fractionnaires principaux totalement positifs. Enfin, on définit le groupe des classes restreint (narrow class group en anglais) comme le quotient suivant :*

$$\mathrm{Cl}^+(K) = \frac{\mathcal{F}(K)^\times}{\mathrm{Princ}^+(K)}.$$

Le groupe des classes restreint n'est pas très différent du groupe des classes puisqu'on a une suite exacte :

$$1 \longrightarrow \frac{\mathrm{Princ}(K)}{\mathrm{Princ}^+(K)} \longrightarrow \mathrm{Cl}^+(K) \longrightarrow \mathrm{Cl}(K) \longrightarrow 1$$

De plus les morphismes surjectifs $K^\times \longrightarrow \mathrm{Princ}(K)$ et $K^+ \longrightarrow \mathrm{Princ}^+(K)$ qui envoient x sur $x\mathcal{O}_K$ induisent des isomorphismes canoniques :

$$\mathrm{Princ}(K) \cong \frac{K^\times}{\mathcal{O}_K^\times}$$

et, en notant $\mathcal{O}_K^+ = \mathcal{O}_K^\times \cap K^+$:

$$\mathrm{Princ}^+(K) \cong \frac{K^+}{\mathcal{O}_K^+}$$

de sorte qu'on a un isomorphisme canonique :

$$\frac{\mathrm{Princ}(K)}{\mathrm{Princ}^+(K)} \cong \frac{K^\times}{K^+\mathcal{O}_K^\times}.$$

On a donc une suite exacte :

$$1 \longrightarrow \frac{K^\times}{K^+\mathcal{O}_K^\times} \longrightarrow \mathrm{Cl}^+(K) \longrightarrow \mathrm{Cl}(K) \longrightarrow 1 \quad (*)$$

dont on déduit le résultat suivant, qui quantifie la différence entre le groupe des classes et le groupe des classes restreint.

Proposition 10.3. *Soit K un corps de nombres avec r plongements réels, on a :*

$$\frac{|\mathrm{Cl}(K)^+|}{|\mathrm{Cl}(K)|} \mid 2^r.$$

Ensuite, pour tout nombre premier impair p, en notant $G[p]$ la p-torsion d'un groupe G, on a :

$$\mathrm{Cl}(K)^+[p] = \mathrm{Cl}(K)[p]$$

et pour $p = 2$, en notant $r_2(K)$ la dimension du $\mathbb{F}_2$-espace vectoriel $\mathrm{Cl}(K)[2]$ et $r_2^+(K)$ la dimension de $\mathrm{Cl}^+(K)[2]$, on a :

$$0 \leq r_2^+(K) - r_2(K) \leq r.$$

Démonstration. Le premier résultat vient de la suite exacte $(*)$ en notant que $K^\times/(K^+\mathcal{O}_K^\times)$ est un quotient de $K^\times/K^+$ donc est un $\mathbb{F}_2$-espace vectoriel de dimension au plus r. Toujours de la suite exacte $(*)$ on obtient en prenant la p-torsion qui est exacte à gauche (voir le lemme suivant 10.4) :

$$1 \to \frac{K^\times}{K^+\mathcal{O}_K^\times}[p] \to \mathrm{Cl}^+(K)[p] \to \mathrm{Cl}(K)[p] \to \frac{K^\times}{K^+\mathcal{O}_K^\times} \otimes_{\mathbb{Z}} \mathbb{F}_p$$

or $K^\times/(K^+\mathcal{O}_K^\times)$ est un espace vectoriel sur $\mathbb{F}_2$ donc pour $p \geq 3$ on obtient que les termes extrêmes sont nuls et donc :

$$\mathrm{Cl}^+(K)[p] = \mathrm{Cl}(K)[p].$$

Pour $p = 2$, on obtient la suite exacte suivante :

$$1 \to \frac{K^\times}{K^+\mathcal{O}_K^\times} \to \mathrm{Cl}^+(K)[2] \to \mathrm{Cl}(K)[2]$$

qui donne en regardant la dimension de ces $\mathbb{F}_2$-espaces vectoriels :

$$\dim_{\mathbb{F}_2}\left(\frac{K^\times}{K^+\mathcal{O}_K^\times}\right) - r_2^+(K) + r_2(K) \geq 0$$

donc :

$$r_2^+(K) - r_2(K) \leq \dim_{\mathbb{F}_2} \leq r.$$

Enfin, en tensorisant $(*)$ par $\mathbb{F}_2$ au dessus de $\mathbb{Z}$ on a une surjection :

$$\mathrm{Cl}^+(K) \otimes \mathbb{F}_2 \longrightarrow \mathrm{Cl}(K) \otimes \mathbb{F}_2 \longrightarrow 1$$

qui donne $r_2^+(K) \geq r_2(K)$ car pour un groupe abélien fini G, on voit facilement en décomposant G en produit de groupes cycliques que les $\mathbb{F}_2$-espaces vectoriels $G[2]$ et $G \otimes \mathbb{F}_2$ ont la même dimension. □

Dans la preuve précédente on a utilisé le lemme suivant, qui admet de multiples généralisations. Dans le langage de l'algèbre homologique, il vient du fait que le foncteur de p-torsion a pour (premier) foncteur dérivé à droite le foncteur de tensorisation par $\mathbb{F}_p$.

Lemme 10.4. *Soit p un nombre premier et $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ une suite exacte courte de groupes abéliens. On a alors une suite exacte longue :*

$$0 \to A[p] \to B[p] \to C[p] \xrightarrow{\nabla} A \otimes \mathbb{F}_p \to B \otimes \mathbb{F}_p \to C \otimes \mathbb{F}_p \to 0.$$

Démonstration. La seule difficulté est de construire la flèche du milieu $C[p] \xrightarrow{\nabla} A \otimes \mathbb{F}_p$. On explique ici sa construction mais on ne donne pas les détails de l'exactitude :
Soit $c \in C[p]$. Par surjectivité de $B \longrightarrow C$, on trouve $b \in B$ un antécédent de c. Ainsi pb est envoyé sur 0 dans C (car il est envoyé sur $pc = 0$) et donc pb est dans l'image de $A \longrightarrow B$: on trouve $a \in A$ qui s'envoie sur pb. On pose alors :

$$\nabla(c) = a \otimes 1 \in A \otimes \mathbb{F}_p$$

et on vérifie facilement que ∇ est bien définie et rend la suite de l'énoncé exacte. □

10.2 Le théorème de Gauss

Dans ce qui suit, $K = \mathbb{Q}(\sqrt{d})$ est un corps de nombres quadratiques avec $d \neq 0, 1$ sans facteur carré. On note σ l'unique générateur du groupe de Galois de $K/\mathbb{Q}$, c'est le morphisme qui envoie $\sqrt{d}$ sur $-\sqrt{d}$. On s'intéresse à la 2-torsion du groupe de classes restreint, ce que l'on note toujours $\mathrm{Cl}^+(K)[2]$, et dont on note toujours $r_2^+(K)$ la dimension sur $\mathbb{F}_2$.
Pour calculer $r_2^+(K)$, on se base sur la méthode de [5]. On définit le groupe :

$$K_2^+ = \left\{ x \in K^+ \mid \forall \mathfrak{p}\ v_\mathfrak{p}(x) \equiv 0\ [2] \right\}$$

des éléments totalement positifs dont toutes les valuations $\mathfrak{p}$-adiques sont paires. Le lemme suivant permet de le relier au groupe $\mathrm{Cl}^+(K)[2]$.

Lemme 10.5. *Le morphisme $\sqrt{\bullet} : K_2^+ \longrightarrow \mathrm{Cl}^+(K)[2]$ qui envoie x sur la classe de l'idéal $\prod_\mathfrak{p} \mathfrak{p}^{\frac{1}{2}v_\mathfrak{p}(x)}$ est bien défini et donne lieu à la suite exacte suivante :*

$$1 \longrightarrow \mathcal{O}_K^+(K^+)^2 \longrightarrow K_2^+ \xrightarrow{\sqrt{\bullet}} \mathrm{Cl}^+(K)[2] \longrightarrow 1.$$

Démonstration. Le morphisme est bien défini car les valuations $\mathfrak{p}$-adiques d'un $x \in K_2^+$ sont paires et on a :

$$\left(\prod_\mathfrak{p} \mathfrak{p}^{\frac{1}{2}v_\mathfrak{p}(x)} \right)^2 = (x)$$

qui est trivial dans le groupe de classes restreint car x est totalement positif donc $\sqrt{x}$ est bien un élément de $\mathrm{Cl}^+(K)[2]$.
Il est surjectif : soit $\omega \in \mathrm{Cl}^+(K)[2]$ la classe d'un idéal fractionnaire J. On a $J^2 = (x)$ avec x un élément totalement positif. Ainsi les valuations de x sont paires, donc $x \in K_2^+$ et on a :

$$J = \prod_\mathfrak{p} \mathfrak{p}^{\frac{1}{2}v_\mathfrak{p}(x)}.$$

Le noyau est formé des $x \in K_2^+$ tels que l'idéal $\prod_\mathfrak{p} \mathfrak{p}^{\frac{1}{2}v_\mathfrak{p}(x)}$ soit de la forme (y) avec $y \in K^+$, de sorte que $x/y^2 \in \mathcal{O}_K^+$. Le noyau est donc exactement $\mathcal{O}_K^+(K^+)^2$. □

La suite exacte du lemme 10.5 passe au quotient pour donner la suite exacte suivante :

$$1 \longrightarrow \frac{\mathcal{O}_K^+}{\left(\mathcal{O}_K^+\right)^2} \longrightarrow \frac{K_2^+}{(K^+)^2} \longrightarrow \mathrm{Cl}^+(K)[2] \longrightarrow 1 \qquad (*)$$

car $\mathcal{O}_K^+ \cap (K^+)^2 = (\mathcal{O}_K^+)^2$ (si $x^2 \in \mathcal{O}_K$, alors $x \in \mathcal{O}_K$ car $\mathcal{O}_K$ est intégralement clos).

Lemme 10.6. *On a une suite exacte :*

$$1 \longrightarrow (\mathbb{Q}_+^*)^2 \longrightarrow \mathbb{Q}_+^* \cap K_2^+ \longrightarrow \frac{K_2^+}{(K^+)^2} \longrightarrow 1.$$

Démonstration. Déterminons maintenant le noyau de la flèche canonique $\mathbb{Q}_+^* \cap K_2^+ \longrightarrow \frac{K_2^+}{(K^+)^2}$. Si x est dans ce noyau, on peut écrire $x = (a + b\sqrt{d})^2$ avec $a, b \in \mathbb{Q}$ et $a + b\sqrt{d} \in K^+$. On a donc :

$$x = a^2 + db^2 + 2ab\sqrt{d}$$

de sorte que $ab = 0$. Supposons par l'absurde que $a = 0$. Ainsi $x = db^2$ et $b \neq 0$. Puisque $x > 0$, on a nécessairement $d > 0$ et puisque $a + b\sqrt{d} = b\sqrt{d} \in K^+$, on a $b\sqrt{d} > 0$ et $-b\sqrt{d} > 0$, ce qui est absurde. Donc $a \neq 0$ et $b = 0$. On obtient :

$$x = a^2$$

donc $x \in (\mathbb{Q}^*)^2$. Réciproquement un tel élément est clairement dans le noyau (en effet $(\mathbb{Q}^*)^2 = (\mathbb{Q}_+^*)^2$).
Il reste à voir la surjectivité. Soit $x \in K_2^+$. On écrit :

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$$

de sorte que :

$$N_{K/\mathbb{Q}}(x)\mathbb{Z} = \|(x)\|_{K/\mathbb{Q}} = \prod_p \prod_{\mathfrak{p} \ni p} p^{f(\mathfrak{p}|p) v_{\mathfrak{p}}(x)}$$

et donc les valuations p-adiques de $N_{K/\mathbb{Q}}(x)$ sont paires. Ainsi il existe $a \in \mathbb{Q}_+^*$ tel que :

$$N_{K/\mathbb{Q}}(x) = a^2$$

puisque, x étant totalement positif, sa norme est positive. On a donc :

$$N_{K/\mathbb{Q}}\left(\frac{x}{a}\right) = 1.$$

Par le théorème 90 de Hilbert pour l'extension cyclique $K/\mathbb{Q}$, il existe donc $b \in K^\times$ tel que :

$$\frac{\sigma b}{b} = \frac{x}{a}.$$

Or $\frac{x}{a}$ est totalement positif donc, si $d > 0$, b et σb sont de même signe et quitte à remplacer b par $-b$ on peut supposer b totalement positif (et si $d < 0$ c'est bien sûr le cas).
On a ainsi :

$$x = \frac{a \cdot \sigma b}{b} = \frac{a(\sigma b)^2}{N_{K/\mathbb{Q}}(b)} \equiv \frac{a}{N_{K/\mathbb{Q}}(b)} \; [(K^+)^2]$$

avec $a/N_{K/\mathbb{Q}}(b) \in \mathbb{Q}_+^*$ qui est aussi dans K_2^+ car $x \in K_2^+$ et $(\sigma b)^2 \in K_2^+$. La flèche $\mathbb{Q}_+^* \cap K_2^+ \longrightarrow \frac{K_2^+}{(K^+)^2}$ est donc surjective. □

Lemme 10.7. *Le groupe* $\frac{\mathcal{O}_K^+}{(\mathcal{O}_K^+)^2}$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z}$.

Démonstration. Si $d < 0$, c'est simplement $\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^2} = \mathbb{U}_\infty(K) \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ d'après le théorème des unités 6.29. Or $\mathbb{U}_\infty(K)$ contient -1 donc est un groupe cyclique d'ordre pair et ainsi la tensorisation par $\mathbb{Z}/2\mathbb{Z}$ donne $\mathbb{Z}/2\mathbb{Z}$.
Si $d > 0$, d'après le théorème 6.29, il existe $u \in \mathcal{O}_K^\times$ une unité fondamentale, au sens où on a la somme directe interne (notée multiplicativement) :

$$\mathcal{O}_K^\times = \mathbb{U}_\infty(K) \odot u^{\mathbb{Z}}.$$

Puisque $K \subseteq \mathbb{R}$, on a $\mathbb{U}_\infty(K) = \{-1, 1\}$ et donc :

$$\mathcal{O}_K^+ = u^{\mathbb{Z}} \cap K^+.$$

Notons que $u^2 \in K^+$ donc $u^{\mathbb{Z}} \cap K^+$ est un sous-groupe non trivial de $u^{\mathbb{Z}}$, donc c'est isomorphe à $\mathbb{Z}$, engendré par u ou u^2 selon les cas. Ainsi :

$$\mathcal{O}_K^+ \cong \mathbb{Z}$$

et

$$\mathcal{O}_K^+/(\mathcal{O}_K^+)^2 \cong \mathbb{Z}/2\mathbb{Z}.$$

□

On dispose de tous les ingrédients pour démontrer le théorème de Gauss.

Théorème 10.8. *(Théorie du genre de Gauss) Soit K un corps de nombres quadratique. On note t le nombre de nombre premiers qui se ramifient dans K. On a alors l'égalité suivante :*

$$r_2^+(K) = t - 1.$$

De plus $\mathrm{Cl}^+(K)[2]$ est engendré par les t premiers de K qui sont au dessus de nombres premiers ramifiés.
En conséquence, si K est imaginaire on a $r_2(K) = t - 1$ et si K est réel on a un encadrement de $r_2(K)$:

$$t - 3 \leq r_2(K) \leq t - 1.$$

Démonstration. Dans la suite exacte $(*)$, tous les groupes sont des $\mathbb{F}_2$-espaces vectoriels donc on a :

$$r_2^+(K) = \dim_{\mathbb{F}_2} \frac{K_2^+}{(K^+)^2} - \dim_{\mathbb{F}_2} \frac{\mathcal{O}_K^+}{(\mathcal{O}_K^+)^2}.$$

Par le lemme 10.6, on a un isomorphisme :

$$\frac{K_2^+}{(K^+)^2} \cong \frac{\mathbb{Q}_+^* \cap K_2^+}{(\mathbb{Q}_+^*)^2}.$$

La décomposition en facteurs premiers permet d'écrire :

$$\mathbb{Q}_+^* = \bigodot_p p^{\mathbb{Z}}$$

et un élément $x \in \mathbb{Q}_+^*$ est dans K_2^+ si et seulement si pour tout $\mathfrak{p}$ premier de K le nombre $v_\mathfrak{p}(x)$ est pair. Or si p est le nombre premier en dessous de $\mathfrak{p}$, on a :

$$v_\mathfrak{p}(x) = e(\mathfrak{p} \mid p) v_p(x).$$

Puisque $K/\mathbb{Q}$ est quadratique, $e(\mathfrak{p} \mid p)$ vaut 2 si p est ramifié et 1 sinon. Ainsi, en utilisant le corollaire du théorème de Dedekind 5.42 on a la décomposition suivante :

$$\mathbb{Q}_+^* \cap K_2^+ = \bigodot_{p \mid \mathrm{Disc}(K)} p^{\mathbb{Z}} \odot \bigodot_{p \nmid \mathrm{Disc}(K)} p^{2\mathbb{Z}}.$$

D'autre part :

$$(\mathbb{Q}_+^*)^2 = \bigodot_{p} p^{2\mathbb{Z}}$$

donc le quotient est isomorphe à :

$$\frac{K_2^+}{(K^+)^2} \cong \bigodot_{p \mid \mathrm{Disc}(K)} p^{\mathbb{Z}/2\mathbb{Z}} \cong \mathbb{F}_2^t.$$

De plus le lemme 10.7 assure que $\dim_{\mathbb{F}_2} \frac{\mathcal{O}_K^+}{(\mathcal{O}_K^+)^2} = 1$ donc :

$$r_2^+(K) = t - 1.$$

En reprenant la suite exacte $(*)$ et celle de 10.6 on voit que des générateurs de $\mathrm{Cl}^+(K)[2]$ sont donnés par les $\sqrt{p}$ pour p premier ramifié dans K (en utilisant la notation $\sqrt{\bullet}$ du lemme 10.5). En écrivant $p = \mathfrak{p}^2$, on a $\sqrt{p} = \mathfrak{p}$ et donc $\mathrm{Cl}^+(K)[2]$ est engendré par les t premiers de K au dessus des premiers ramifiés.
La dernière inégalité vient de la proposition 10.3. □

Remarque 10.9. On peut tirer quelques conséquences qualitatives du théorème 10.8. D'abord, pour tous les $d \geq 2$ sans facteur carré avec au moins 4 diviseurs premiers distincts (ou 3 si $d \equiv 3$ [4]), le discriminant de $\mathbb{Q}(\sqrt{d})$ a au moins 4 diviseurs premiers distincts donc $t \geq 4$ et le groupe de classes est non trivial. On a donc trouvé une famille infinie de corps quadratiques réels dont l'anneau d'entier n'est pas principal. Ensuite, pour chaque nombre premier p congru à 1 modulo 4, le discriminant de $\mathbb{Q}(\sqrt{p})$ vaut p et donc $t = 1$ et le groupe de classes de $\mathbb{Q}(\sqrt{p})$ n'a pas de 2-torsion. Il y a d'ailleurs une infinité de tels nombres premiers.

Troisième partie

Théorie analytique des corps de nombres

Chapitre 11

Nombre d'idéaux de norme bornée

On fixe K un corps de nombres. La proposition 6.21 affirme que pour tout $t > 0$, il n'y a qu'un nombre fini d'idéaux de $\mathcal{O}_K$ de norme inférieure ou égale à t. Dans ce chapitre, on vise à préciser ce résultat. L'objectif est de démontrer le théorème suivant, tiré de [9], qui servira ensuite à obtenir la convergence de certaines fonctions L de Dirichlet. Le lecteur peut admettre le résultat suivant s'il le désire, bien que la preuve soit une jolie considération géométrique sur le réseau $\mathcal{O}_K$.

Théorème 11.1. *Soit $C \in \mathrm{Cl}(\mathcal{O}_K)$ une classe d'idéaux de $\mathcal{O}_K$. On note $\nu_C(t)$ le nombre d'idéaux (contenus dans $\mathcal{O}_K$) de la classe C de norme inférieure ou égale à t. Il existe alors une constante $\kappa > 0$ indépendante de C telle que :*

$$\nu_C(t) = \kappa t + O\left(t^{1-1/d}\right)$$

lorsque t tend vers l'infini.

11.1 Mise en place géométrique

Par le théorème des unités de Dirichlet 6.29, le groupe $\mathcal{O}_K^\times$ possède un sous-groupe abélien libre F de rang $r + s - 1$ tel que :

$$\mathcal{O}_K^\times = \mathbb{U}_\infty(K) \odot F.$$

On rappelle que $\odot$ désigne une somme directe interne en notation multiplicative. On fixe dans toute la suite un tel sous-groupe F. On considère également C une classe d'idéaux de $\mathcal{O}_K$ et on se donne un idéal $J \subseteq \mathcal{O}_K$ de la classe *inverse* C^{-1}. On note C_+ l'ensemble des éléments de C qui sont *contenus* dans $\mathcal{O}_K$, ce sont ces éléments que l'on veut compter. La proposition suivante permet de traduire le problème du comptage des idéaux de la classe C de norme bornée par t en un problème géométrique.

Proposition 11.2. *Soit D un système de représentants du quotient $(K_\mathbb{R} \setminus \{0\})/F$. Pour tout $r \geq 0$ on notera $D_r = \{\alpha \in D \mid |N(\alpha)| \leq r\}$. On a alors l'égalité suivante :*

$$\nu_C(t) = \frac{\left|J \setminus \{0\} \cap D_{t\|J\|}\right|}{|\mathbb{U}_\infty(K)|}$$

Démonstration. À tout élément α de $J\setminus\{0\}$ on peut associer $\alpha J^{-1}\in C_+$. Cela définit une application surjective :

$$J\setminus\{0\}\longrightarrow C_+$$

par définition de C_+ et de J. Cette application se factorise en une bijection :

$$\frac{J\setminus\{0\}}{\mathcal{O}_K^\times}\cong C_+$$

qui fait correspondre les idéaux de C_+ de norme inférieure ou égale à t avec les éléments de $(J\setminus\{0\})/\mathcal{O}_K^\times$ de norme inférieure ou égale à $t\|J\|$ en valeur absolue (puisque les éléments de $\mathcal{O}_K^\times$ sont de norme 1 en valeur absolue, on peut parler sans ambigüité de valeur absolue de la norme d'un élément du quotient $(J\setminus\{0\})/\mathcal{O}_K^\times$). Or on a :

$$\frac{J\setminus\{0\}}{\mathcal{O}_K^\times}\cong\frac{J\setminus\{0\}}{F}/\mathbb{U}_\infty(K)$$

et l'action de $\mathbb{U}_\infty(K)$ sur $(J\setminus\{0\})/F$ est *libre* car $\mathbb{U}_\infty(K)\cap F=\{1\}$. On a donc :

$$\nu_C(t)=\left|\{\bar\alpha\in(J\setminus\{0\})/\mathcal{O}_K^\times\mid|N(\alpha)|\leq t\|J\|\}\right|=\frac{1}{|\mathbb{U}_\infty(K)|}\left|\{\bar\alpha\in(J\setminus\{0\})/F\mid|N(\alpha)|\leq t\|J\|\}\right|$$

Cette dernière quantité est égale à $\frac{|J\setminus\{0\}\cap D_{t\|J\|}|}{|\mathbb{U}_\infty(K)|}$ car D est un système de représentants du quotient par F.

□

La stratégie à suivre est donc de choisir un bon système de représentants D pour $K_\mathbb{R}\setminus\{0\}/F$ puis d'estimer le cardinal de $|J\setminus\{0\}\cap D_r|$ pour tout $r>0$ à l'aide du paragraphe 4.2.4.

Remarque 11.3. On peut se demander pourquoi on choisit de quotienter par F plutôt que de directement quotienter par $\mathcal{O}_K^\times$. L'avantage de F est qu'il s'agit d'un groupe libre qui va former un réseau d'un certain espace dans la suite.

11.2 Choix du système de représentants D

On rappelle qu'on dispose d'un isomorphisme de groupes de Lie :

$$\ell:\begin{cases}K_\mathbb{R}^\times\longrightarrow\{\pm1\}^r\times\mathbb{U}^s\times\mathbb{R}^{r+s}\\(x_1,\dots,x_r,y_1,\dots,y_s)\mapsto\left(\frac{x_1}{|x_1|},\dots,\frac{x_r}{|x_r|},\frac{y_1}{|y_1|},\dots,\frac{y_s}{|y_s|},\log|x_1|,\dots,\log|x_r|,2\log\left|y_1\right|,\dots,2\log\left|y_s\right|\right)\end{cases}$$

entre $K_\mathbb{R}^\times$ et $\{\pm1\}^r\times\mathbb{U}^s\times\mathbb{R}^{r+s}$ qui envoie S_K sur $\{\pm1\}^r\times\mathbb{U}^s\times H$ (voir 6.33 pour les notations). On note encore $\pi:\{\pm1\}^r\times\mathbb{U}^s\times\mathbb{R}^{r+s}\longrightarrow\mathbb{R}^{r+s}$ la projection sur les dernières coordonnées, et $\hat\ell=\pi\circ\ell$. On note aussi $\Lambda=\hat\ell(F)=\hat\ell(\mathcal{O}_K^\times)$ le réseau des unités. On peut à présent choisir notre système de représentants D pour $K_\mathbb{R}\setminus\{0\}/F$ de la façon suivante : on se

donne $(v_1, \dots, v_{r+s-1})$ une $\mathbb{Z}$-*base* du réseau Λ et on considère Δ le domaine fondamental mesurable de Λ bordé par la base (v_i). On considère ensuite la droite :

$$L = \mathbb{R} \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 2 \\ \vdots \\ 2 \end{pmatrix}$$

avec r fois le nombre 1 et s fois le nombre 2. On a ainsi $\mathbb{R}^{r+s} = H \oplus L$. On pose alors $D' = \Delta + L$, qui est un système de représentants du quotient $\mathbb{R}^{r+s}/\Lambda$. On définit enfin D comme l'image réciproque de D' par $\hat{\ell}$:

$$D = \hat{\ell}^{-1}(D') \subseteq K_{\mathbb{R}}^{\times}.$$

Lemme 11.4. *L'ensemble mesurable D est un système de représentants du quotient :*

$$(K_{\mathbb{R}} \setminus \{0\})/F.$$

Démonstration. Soit $\alpha \in K_{\mathbb{R}} \setminus \{0\}$. Comme D' est un système de représentants du quotient $\mathbb{R}^{r+s}/\hat{\ell}(F)$, il existe $d' \in D'$ et $f \in F$ tel que :

$$\hat{\ell}(\alpha) = d' + \hat{\ell}(f)$$

Puisque $\hat{\ell}$ est surjective, on peut alors écrire :

$$\alpha = dfk$$

avec $d \in D$ et $k \in \ker \hat{\ell}$. Mais $dk \in D$ donc α est bien représenté par un élément de D modulo F. Il y a unicité de cet élément, car si $d_1 f_1 = d_2 f_2$ avec $d_1, d_2 \in D$ et $f_1, f_2 \in F$, alors en appliquant $\hat{\ell}$ et en utilisant le fait que D' est un système de représentants on obtient :

$$\hat{\ell}(d1) = \hat{\ell}(d_2)$$

Or on a aussi $\hat{\ell}(d_1) + \hat{\ell}(f_1) = \hat{\ell}(d_2) + \hat{\ell}(f_2)$ donc $\hat{\ell}(f_1) = \hat{\ell}(f_2)$ et on conclut en utilisant l'injectivité de $\hat{\ell}$ sur F. □

Proposition 11.5. *L'ensemble D est un cône, c'est à dire qu'il est stable par multiplication par tout réel non nul, et on a, pour tout $t > 0$:*

$$D_t = t^{1/d} D_1$$

où la notation D_t signifie toujours $\{\alpha \in D \mid |N(\alpha)| \leq t\}$.

Démonstration. L'ensemble D est un cône car $\hat{\ell}(\mathbb{R}^* \cdot 1_{K_{\mathbb{R}}}) \subseteq L$, et donc pour tout $r \in \mathbb{R}^*$ on a $\hat{\ell}(rD) = \hat{\ell}(r) + D' = D'$. La deuxième égalité vient du fait que pour tout $r > 0$ et tout $\alpha \in K_{\mathbb{R}}$, on a :

$$N(r\alpha) = r^d N(\alpha).$$

□

11.3 Calcul de la mesure de D_1

On fixe la mesure de Lebesgue μ sur $K_{\mathbb{R}}$ obtenue en identifiant $K_{\mathbb{R}}$ à $\mathbb{R}^d$ et en prenant la mesure de Lebesgue canonique sur $\mathbb{R}^d$. Il s'agit de la même mesure que celle définie dans la preuve de 6.16. La proposition 11.5 montre qu'il suffit de calculer la mesure de D_1 pour obtenir celle de D_t. Le cône D a de nombreuses symétries provenant du noyau de $\hat{\ell}$, donc on considère un ensemble plus élémentaire :

$$D_1^+ = \{(x_1,\dots,x_r,y_1,\dots,y_s) \in D_1 \mid \forall i\ x_i \geq 0\}.$$

On a donc naturellement :

$$\mu(D_1) = 2^r \mu(D_1^+)$$

puisqu'il y a 2^r choix de signes $\varepsilon_1,\dots,\varepsilon_r \in \{\pm 1\}$.

Lemme 11.6. *L'ensemble D_1 est borné et intersecte bien les réseaux au sens du paragraphe 4.2.4.*

Démonstration. Il suffit de montrer que D_1^+ est borné et qu'il intersecte bien les réseaux : en effet une réunion disjointe finie de parties qui intersectent bien les réseaux est une partie qui intersecte bien les réseaux et D_1 est réunion disjointes de copies symétriques de D_1^+. On définit :

$$K_{\mathbb{R}}^+ =]0,+\infty[^r \times (\mathbb{C}^\times)^s \subseteq K_{\mathbb{R}}$$

de sorte que $D_1^+ = D_1 \cap K_{\mathbb{R}}^+$. On a un isomorphisme de groupes de Lie :

$$\Phi : \begin{cases} \mathbb{R}^{r+s} \times \mathbb{U}^s \longrightarrow K_{\mathbb{R}}^+ \\ (x_1,\dots,x_r,y_1,\dots,y_s,\omega_1,\dots,\omega_s) \mapsto \left(\exp(x_1),\dots,\exp(x_r),\omega_1 \exp\left(\frac{y_1}{2}\right),\dots,\omega_s \exp\left(\frac{y_s}{2}\right)\right) \end{cases}.$$

C'est en particulier un difféomorphisme et il fournit un paramétrage lisse de D_1^+ de la façon suivante. On définit L_- la demi-droite $]-\infty,0] \cdot (1,\dots,1,2,\dots,2) \subseteq L$ et $X = (\Delta + L_-) \times \mathbb{U}^s$ de sorte que :

$$\Phi(X) = D_1^+.$$

En effet, la condition $|N(\alpha)| \leq 1$ se traduit pour $\hat{\ell}(\alpha)$ par le fait d'être du côté "négatif" de l'hyperplan H, c'est à dire celui ou $\sum x_i + \sum y_i \leq 0$.
Soit $p = (x_1,\dots,x_r,y_1,\dots,y_s,\omega_1,\dots,\omega_s) \in X$. Par définition de X on peut écrire :

$$(x_1,\dots,x_r,y_1,\dots,y_s) = \sum_j t_j v_j - uh$$

avec $h = (1,\dots,1,2,\dots,2)$, $t_j \in [0,1[$, $u \geq 0$. Ainsi $x_i = \sum_j t_j e_i^*(v_j) - u$ et $y_i = \sum_j t_j e_{i+r}^*(v_j) - 2u$ avec $\underline{e^*}$ la base duale de la base canonique $\underline{e}$ de $\mathbb{R}^{r+s}$. On en déduit que :

$$|e^{x_i}| \leq \exp\left(\sum_j \left|e_i^*(v_j)\right|\right)$$

et de même pour $\exp(y_i/2)$. Cela montre que D_1^+ est borné.
On montre maintenant que $\Phi_{|X}$ est lipschitzienne en munissant $\mathbb{R}^{r+s} \times \mathbb{U}^s$ d'une distance issue d'une norme quelconque sur $\mathbb{R}^{r+s} \times \mathbb{C}^s$. Pour cela on estime la norme d'opérateur de la différentielle $d_p\Phi$ pour $p \in X$:

$$d_p\Phi = \left(e^{x_1}dx_1, \dots, e^{x_r}dx_r, \frac{\omega_1}{2}e^{y_1/2}dy_1 + e^{y_1/2}d\omega_1, \dots, \frac{\omega_s}{2}e^{y_s/2}dy_s + e^{y_s/2}d\omega_s\right)$$

en identifiant l'espace tangent $T_{\omega_j}\mathbb{U}$ de $\mathbb{U}$ en ω_j à $i\omega_j\mathbb{R}$, la 1-forme complexe $d\omega_j$ étant simplement l'inclusion

$$T_{\omega_j} \subseteq \mathbb{C}.$$

En munissant les espaces tangents de départ et d'arrivée de la norme infinie associée aux valeurs absolues sur $\mathbb{R}$ et $\mathbb{C}$ on a, pour $p \in X$:

$$\left|\left|\left|d_p\Phi\right|\right|\right| \leq \max\left(e^{x_1}, \dots, e^{x_r}, \frac{3}{2}e^{y_1/2}, \dots, \frac{3}{2}e^{y_s/2}\right)$$

et on a vu ci-dessus que ces exponentielles sont bornées. Ainsi $\Phi_{|X}$ est lipschitzienne.
On va utiliser ceci pour montrer que D_1^+ vérifie les hypothèhses de 4.48.
Puisque Φ est un homéomorphisme, le bord de D_1^+ dans l'espace topologique $K_{\mathbb{R}}^+$ est exactement $\Phi(\partial X)$. Ainsi le bord de D_1^+ dans $K_{\mathbb{R}}$ vérifie :

$$\partial D_1^+ \subseteq \Phi(\partial X) \cup (\partial D_1^+ \cap \partial K_{\mathbb{R}}^+)$$

Pour voir que ∂D_1^+ vérifie les hypothèhses de 4.48, on montre que $\Phi(\partial X)$ et $\partial D_1^+ \cap \partial K_{\mathbb{R}}^+$ peuvent être recouverts par un nombre fini d'images de fonctions lipschitziennes définies sur $[0,1]^{d-1}$ avec toujours $d = [K : \mathbb{Q}] = r + 2s$. D'abord on a $\partial X = ((\partial_H\Delta + L_-) \cup \Delta) \times \mathbb{U}^s$ en notant $\partial_H\Delta$ le bord de Δ calculé dans l'hyperplan H (c'est le bord du domaine fondamental Δ). On peut facilement recouvrir chaque face de ∂X par une image d'application lipschitzienne de source $[0,1]^{d-1}$, et puisque Φ est lipschitzienne, on obtient un recouvrement de $\Phi(\partial X)$ par de tels ensembles. Pour recouvrir $\partial D_1^+ \cap \partial K_{\mathbb{R}}^+$, on utilise le fait que D_1^+ est borné et que $\partial K_{\mathbb{R}}^+$ est contenu dans une réunion finie d'hyperplans (dans cet ensemble, au moins une coordonnée est nulle).
Ainsi par le théorème 4.48, D_1^+ intersecte bien les réseaux. □

Proposition 11.7. *On munit toujours $K_{\mathbb{R}}$ de la mesure de Lebesgue canonique sur $\mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^d$. Le volume de D_1^+ est alors donné par la formule suivante :*

$$\mu(D_1^+) = \pi^s \operatorname{Reg}(K)$$

où le régulateur de K, $\operatorname{Reg}(K)$, est défini en 6.33.

Démonstration. On utilise encore le paramétrage Φ et l'ensemble X définis dans la preuve du lemme 11.6. Pour $p = (x_1, \dots, x_r, y_1, \dots, y_s, \omega_1, \dots, \omega_s) \in X$, on a :

$$d_p\Phi = \left(e^{x_1}dx_1, \dots, e^{x_r}dx_r, \frac{\omega_1}{2}e^{y_1/2}dy_1 + e^{y_1/2}d\omega_1, \dots, \frac{\omega_s}{2}e^{y_s/2}dy_s + e^{y_s/2}d\omega_s\right)$$

On utilise ici le formalisme de la géométrie différentielle. Il est bien sûr possible d'effectuer ce calcul à la main avec un calcul de jacobien (voir par exemple le chapitre 6 du livre de Marcus [9]). On a :

$$\mu(D_1^+) = \int_{D_1^+} dx_1 \dots dx_r d^2z_1 \dots d^2z_s = \pm \int_{X^\circ} \Phi^*(dx_1 \wedge \cdots \wedge dx_r \wedge d^2z_1 \wedge \cdots \wedge d^2z_s).$$

Ici la notation d^2z_j désigne la 2-forme $d\operatorname{Re} z_j \wedge d\operatorname{Im} z_j$.
Au point p, on a :

$$\begin{aligned}
&\Phi^*(dx_1 \wedge \cdots \wedge dx_r \wedge d^2z_1 \wedge \cdots \wedge d^2z_s) \\
&= \bigwedge_{j=1}^{r} e^{x_j} dx_j \wedge \bigwedge_{j=1}^{s} \left(\operatorname{Re}\left(\frac{\omega_j}{2} e^{y_j/2} dy_j + e^{y_j/2} d\omega_j \right) \wedge \operatorname{Im}\left(\frac{\omega_j}{2} e^{y_j/2} dy_j + e^{y_j/2} d\omega_j \right) \right) \\
&= \exp\left(\sum_i x_i + \sum_i y_i \right) \bigwedge_{j=1}^{r} dx_j \wedge \bigwedge_{j=1}^{s} \left(\operatorname{Re}\left(\frac{\omega_j}{2} dy_j + d\omega_j \right) \wedge \operatorname{Im}\left(\frac{\omega_j}{2} dy_j + d\omega_j \right) \right)
\end{aligned}$$

On observe que sur $T_\omega \mathbb{U}$, on a :

$$\operatorname{Re} d\omega \wedge \operatorname{Im} d\omega = 0$$

car c'est une 2-forme réelle sur un espace vectoriel réel de dimension 1. On peut aussi le voir directement : si $u, v \in T_\omega \mathbb{U} = i\omega\mathbb{R}$, un calcul montre que $\operatorname{Re}(u)\operatorname{Im}(v) - \operatorname{Re}(v)\operatorname{Im}(u) = 0$. On en déduit que :

$$\begin{aligned}
\operatorname{Re}\left(\frac{\omega}{2} dy + d\omega \right) \wedge \operatorname{Im}\left(\frac{\omega}{2} dy + d\omega \right) &= \frac{1}{2} \operatorname{Re}(\omega) dy \wedge \operatorname{Im}(d\omega) - \frac{1}{2} \operatorname{Im}(\omega) dy \wedge \operatorname{Re}(d\omega) \\
&= \frac{dy}{2} \left(\operatorname{Re}(\omega) \operatorname{Im}(d\omega) - \operatorname{Im}(\omega) \operatorname{Re}(d\omega) \right) \\
&= \frac{dy}{2} \operatorname{Im}\left(\overline{\omega} d\omega \right) = \frac{dy}{2} \operatorname{Im}\left(\frac{d\omega}{\omega} \right).
\end{aligned}$$

Notons que la 1-forme réelle $\operatorname{Im}\left(\frac{d\omega}{\omega}\right)$ est exactement la 1-forme équivariante sur le cercle $d\theta$ telle que :

$$\int_{\mathbb{U}} d\theta = 2\pi.$$

En effet $\int_{\mathbb{U}} \frac{d\omega}{\omega} = 2i\pi$ par le théorème des résidus ou par un calcul direct. On note alors $d\theta_j = \operatorname{Im}\left(d\omega_j / \omega_j \right)$. Ainsi on a :

$$\begin{aligned}
&\Phi^*(dx_1 \wedge \cdots \wedge dx_r \wedge d^2z_1 \wedge \cdots \wedge d^2z_s) \\
&= \exp\left(\sum_i x_i + \sum_i y_i \right) \bigwedge_{j=1}^{r} dx_j \wedge \bigwedge_{j=1}^{s} \left(\frac{dy_j}{2} \wedge d\theta_j \right) \\
&= \pm \frac{\exp\left(\sum_i x_i + \sum_i y_i \right)}{2^s} dx_1 \wedge \cdots \wedge dx_r \wedge dy_1 \wedge \cdots \wedge dy_s \wedge d\theta_1 \wedge \cdots \wedge d\theta_s
\end{aligned}$$

On a donc par Fubini :

$$\mu(D_1^+) = \frac{(2\pi)^s}{2^s} \int_{\Delta+L'} \exp\left(\sum_i x_i + \sum_i y_i\right) d^r\underline{x} d^s\underline{y}.$$

Paramétrer selon la base $(v_1,\dots,v_{r+s-1},v_{r+s})$ avec $v_{r+s} = -(1,\dots,1,2,\dots,2)$ fait apparaître le déterminant de la base $\underline{v}$ dans la base canonique de $\mathbb{R}^{r+s}$, noté $\left|\det(\underline{v})\right|$:

$$\begin{aligned}
\mu(D_1^+) &= \pi^s \left|\det(\underline{v})\right| \int_0^1 \dots \int_0^1 \int_0^\infty \exp\left(\sum_{i=1}^{r}\left(\sum_{j=1}^{r+s-1} t_j e_i^*(v_j) - u\right) + \sum_{i=1}^{s}\left(\sum_{j=1}^{r+s-1} t_j e_{i+r}^*(v_j) - 2u\right)\right) dt_1 \dots dt_{r+s-1} du \\
&= \pi^s \left|\det(\underline{v})\right| \int_0^1 \dots \int_0^1 \int_0^\infty \exp\left(\sum_{j=1}^{r+s-1} t_j \sum_{i=1}^{r+s} e_i^*(v_j) - ud\right) dt_1 \dots dt_{r+s-1} du \\
&= \pi^s \left|\det(\underline{v})\right| \int_0^1 \dots \int_0^1 \int_0^\infty \exp(-ud)\, dt_1 \dots dt_{r+s-1} du \\
&= \frac{\pi^s \left|\det(\underline{v})\right|}{d}
\end{aligned}$$

car $v_j \in H$ pour $1 \le j \le r+s-1$. Il reste à déterminer $\left|\det(\underline{v})\right|$. La formule du volume du prisme ($d-1$-volume de la base multiplié par la hauteur du prisme qui est la distance entre H et v_{r+s}) donne :

$$\left|\det(\underline{v})\right| = \operatorname{covol}(\Lambda) \cdot d(H, v_{r+s}) = \sqrt{r+s} \cdot \operatorname{Reg}(K) \cdot d(H, v_{r+s})$$

La distance $d(H, v_{r+s})$ est la norme du projeté orthogonal de v_{r+s} sur $H^\perp = \mathbb{R}\cdot(1,\dots,1)$:

$$d(H, v_{r+s}) = \left|\left\langle v_{r+s}, \frac{(1,\dots,1)}{\sqrt{r+s}}\right\rangle\right| = \frac{r+2s}{\sqrt{r+s}} = \frac{d}{\sqrt{r+s}}.$$

Au total on a bien :

$$\mu(D_1^+) = \pi^s \operatorname{Reg}(K).$$

□

11.4 Conclusion

En remettant les morceaux ensemble, on a donc démontré le théorème 11.1. On a même une détermination de la constante κ qui sera utile pour obtenir la formule analytique du nombre de classes. On résume cela ainsi :

Théorème 11.8. *Pour C une classe d'idéaux de $\mathcal{O}_K$, on a :*

$$\nu_C(t) = \kappa t + O(t^{1-1/d})$$

avec :

$$\kappa = \frac{2^{r+s}\pi^s \operatorname{Reg}(K)}{|\mathbb{U}_\infty(K)|\sqrt{|\operatorname{Disc} K|}}$$

Par conséquent, en notant h le cardinal du groupe des classes $\mathrm{Cl}(\mathcal{O}_K)$, on a aussi :

$$\nu(t) = \kappa h t + O(t^{1-1/d})$$

avec $\nu(t)$ le nombre d'idéaux non nuls de $\mathcal{O}_K$ de norme inférieure ou égale à t.

Démonstration. On utilise d'abord la proposition 11.2 :

$$\nu_C(t) = \frac{\left|J \setminus \{0\} \cap D_{t\|J\|}\right|}{|\mathbb{U}_\infty(K)|}$$

Ensuite, puisque $D_{t\|J\|} = (t\,\|J\|)^{1/d} D_1$ (proposition 11.5) et D_1 intersecte bien les réseaux, on a ensuite :

$$\left|J \setminus \{0\} \cap D_{t\|J\|}\right| = \frac{\mu(D_1)}{\mathrm{covol}(J)} t\,\|J\| + O(t^{1-1/d})$$

On a donc :

$$\begin{aligned}\kappa &= \frac{\mu(D_1)\,\|J\|}{\mathrm{covol}(J)\,|\mathbb{U}_\infty(K)|} = \frac{2^r \mu(D_1^+)}{\mathrm{covol}(\mathcal{O}_K)\,|\mathbb{U}_\infty(K)|} \\ &= \frac{2^r \pi^s \,\mathrm{Reg}(K)}{\mathrm{covol}(\mathcal{O}_K)\,|\mathbb{U}_\infty(K)|}\end{aligned}$$

et on conclut avec :

$$\mathrm{covol}(\mathcal{O}_K) = \frac{1}{2^s}\sqrt{|\mathrm{Disc}\, K|}$$

qui est démontré dans la preuve du théorème 6.16.

□

11.5 Cas des corps quadratiques

On présente ici la valeur de κ dans le cas particulier d'un corps *quadratique imaginaire* $K = \mathbb{Q}(\sqrt{d})$ avec $d < 0$ sans facteur carré. Dans ce cas, l'étude géométrique menée précedemment pour obtenir la valeur de κ est beaucoup plus directe car $\mathcal{O}_K$ est *déjà un réseau* de $\mathbb{C}$. Le lecteur interessé par ce cas particulier pourra se référer au livre de Marcus, [9], au chapitre 6.

Théorème 11.9. *Pour $K = \mathbb{Q}(\sqrt{d})$ avec $d < 0$ sans facteur carré, on a :*

$$\kappa = \frac{2\pi}{\left|\mathcal{O}_K^\times\right| \sqrt{|\mathrm{Disc}\, K|}} = \begin{cases} \frac{2\pi}{|\mathcal{O}_K^\times|\sqrt{-d}} & \text{si } d \equiv 1\ [4] \\ \frac{\pi}{|\mathcal{O}_K^\times|\sqrt{-d}} & \text{sinon} \end{cases}$$

Démonstration. Cela découle directement du théorème 11.8 en observant que pour un corps quadratique, $\mathcal{O}_K^\times$ est un groupe fini (car de rang $r + s - 1 = 0$). □

Chapitre 12

Fonctions ζ de Dedekind

> On trouve, en effet, entre ces limites un nombre environ égal à celui-ci, de racines réelles, et il est très probable que toutes les racines sont réelles. Il serait à désirer, sans doute, que l'on eût une démonstration rigoureuse de cette proposition ; néanmoins j'ai laissé cette recherche de côté pour le moment après quelques rapides essais infructueux, car elle paraît superflue pour le but immédiat de mon étude.
>
> Bernhard Riemann, Sur le nombre de nombres premiers inférieurs à une taille donnée

Dans ce chapitre, on suit la trame du livre de Marcus [9] (chapitre 7). Le but est de généraliser la fonction ζ de Riemann à des corps de nombres quelconques, et d'étudier le lien entre les propriétés analytiques de cette fonction et les propriétés statistiques des idéaux premiers du corps de nombres. Plus précisément, si K est un corps de nombres, on va définir une fonction :

$$\zeta_K(s) = \sum_I \frac{1}{||I||^s}$$

avec la somme qui porte sur les idéaux non-nuls de $\mathcal{O}_K$. Cette fonction ζ admettra une factorisation en produit Eulérien :

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - ||\mathfrak{p}||^{-s}}$$

avec le produit qui porte sur les premiers de K. On pourra alors relier le résidu en $s = 1$ au nombre de classes du corps de nombres K.

Notation 12.1. *Soit A un anneau intègre. Dans tout ce qui suit, $\mathbb{P}_A$ désigne l'ensemble des premiers de A, c'est à dire l'ensemble des idéaux premiers de A non nuls. Pour $A = \mathbb{Z}$, on note simplement $\mathbb{P}$ et on l'identifie avec l'ensemble des nombres premiers. De plus, $\mathcal{I}_A$ désigne l'ensemble des idéaux non nuls de A, et pour $A = \mathbb{Z}$, on identifiera $\mathcal{I}_A$ à $\mathbb{N}^*$.*

12.1 Produits infinis

Définition 12.2. *Soit I un ensemble et $(a_i)_{i\in I}$ une famille de réels positifs. On définit le produit des $1+a_i$, noté $\prod_{i\in I}(1+a_i)$ comme la borne supérieure des produits finis $\prod_{j\in J}(1+a_j)$, avec J qui parcourt les parties finies de I. On dit que la famille $(1+a_i)$ a un produit fini si $\prod_{i\in I}(1+a_i)$ est un réel.*
Soit maintenant $(a_i)_{i\in I}$ une famille de complexes. On dit que le produit des $(1+a_i)$ converge absolument si la famille $(1+|a_i|)_{i\in I}$ a un produit fini.

Remarque 12.3. On peut généraliser cette notion à des familles d'éléments d'une algèbre de Banach quelconque.

Proposition 12.4. *Soit $(a_i)_{i\in I}$ une famille de réels positifs. Alors le produit des $(1+a_i)$ est fini si et seulement si la famille (a_i) est sommable, au sens où $\sum_{i\in I} a_i < \infty$.*
En particulier, si la famille $(1+a_i)$ a un produit fini, alors l'ensemble des i pour lesquels $a_i > 0$ est au plus dénombrable.

Démonstration. Soit J une partie finie de I. On a :

$$\sum_{j\in J} a_j \leq \prod_{j\in J}(1+a_j) \leq \exp\left(\sum_{j\in J} a_j\right)$$

d'où le résultat. Ici la première inégalité s'obtient en développant le produit et la seconde en utilisant l'inégalité $1+a_j \leq \exp(a_j)$. □

Théorème 12.5. *Soit (a_i) une famille non vide de complexes telle que le produit des $1+a_i$ converge absolument (i.e. une famille sommable d'après 12.4). Il existe alors un unique nombre complexe ℓ tel que, pour tout $\varepsilon > 0$, il existe une partie finie J_0 de I telle que pour toute partie finie J contenant J_0, on a :*

$$\left|\prod_{j\in J}(1+a_j) - \ell\right| < \varepsilon$$

Démonstration. L'unicité est claire. D'après la proposition 12.4, on peut supposer I dénombrable quitte à ne garder que les i pour lesquels $a_i > 0$. On peut même prendre $I = \mathbb{N}$ sans perte de généralité. On note alors :

$$P_N = \prod_{n=0}^{N}(1+a_n)$$

La suite (P_N) est bornée car $|P_N| \leq \exp(\sum |a_n|)$. On prend alors $M > 0$ un réel tel que $|P_N| \leq M$ pour tout N. On a, pour $p \leq q$:

$$\left|P_q - P_p\right| = \left|P_p\right| \left| 1 - \prod_{n=p+1}^{q} (1 + a_n) \right| \leq M \left(\prod_{n=p+1}^{q} (1 + |a_n|) - 1 \right)$$

où la dernière inégalité s'obtient en développant le produit puis en appliquant l'inégalité triangulaire avant de refactoriser le produit. On a donc :

$$\left|P_q - P_p\right| \leq M \left(\exp\left(\sum_{n=p+1}^{q} |a_n| \right) - 1 \right)$$

Or la suite $\left(\sum_{n=0}^{N} |a_n|\right)$ est de Cauchy donc la suite $\left(\exp\left(\sum_{n=0}^{N} |a_n|\right) - 1\right)$ aussi, et ainsi (P_N) est de Cauchy dans $\mathbb{C}$ (ou dans une algèbre de Banach) donc *converge* vers un complexe ℓ.
Il reste à vérifier que ℓ satisfait l'énoncé du théorème. Soit $\varepsilon > 0$, il existe N tel que pour tout $n \geq N$ on a :

$$|P_N - \ell| < \varepsilon$$

et ainsi, en posant $J_0 = \{0, 1, \ldots, N\}$, pour toute partie finie J de $\mathbb{N}$ contenant J_0 on a bien :

$$\left| \prod_{j \in J} (1 + a_j) - \ell \right| < \varepsilon$$

□

Définition 12.6. *Le complexe ℓ de la proposition 12.5 est appelé produit de la famille $\prod_{i \in I}(1 + a_i)$ (pour une famille dont le produit converge absolument) et on le note :*

$$\prod_{i \in I} a_i$$

Dans le cas où les a_i sont positifs, on retrouve la notion de produit définie comme la borne supérieure des produits finis. Par convention, si $I = \emptyset$, on pose $\prod_{i \in I}(1 + a_i) = 1$.

Remarque 12.7. L'intérêt de cette construction est qu'elle ne nécessite pas d'ordonner I. Ainsi pour toute permutation σ de I, les produits $\prod_{i \in I}(1 + a_i)$ et $\prod_{i \in I}(1 + a_{\sigma(i)})$ ont la même nature en terme de convergence absolue et le même produit si le produit existe.

Proposition 12.8. *Soit (a_i) une famille de complexes telle que le produit des $1 + a_i$ converge absolument. Alors le produit des $\frac{1}{1+a_i}$ converge absolument et on a :*

$$\prod_{i \in I} (1 + a_i) \times \prod_{i \in I} \frac{1}{1 + a_i} = 1$$

En particulier :

$$\prod_{i \in I} (1 + a_i) \in \mathbb{C} \setminus \{0\}.$$

Démonstration. D'après 12.4, il s'agit de vérifier que la famille des $\frac{1}{1+a_i} - 1$ est sommable. On peut suppoer $I = \mathbb{N}$ sans perte de généralité et on a alors $\sum |a_n| < \infty$ donc $a_n \longrightarrow 0$ et ainsi :

$$\left| \frac{1}{1+a_n} - 1 \right| = O(|a_n|)$$

quand n tend vers l'infini et $\sum_n |a_n| < \infty$. Le produit égal à 1 est clair sur les produits partiels donc est vrai en passant à la limite. □

Proposition 12.9. *Soit $(a_i)_{i\in I}$ une famille de complexes telle que le produit des $(1+a_i)$ converge absolument. Si $(A_n)_{n\in\mathbb{N}}$ est une suite croissante de parties finies de I telles que :*

$$I = \bigcup_{n\in\mathbb{N}} A_n$$

alors on a :

$$\prod_{i\in I}(1+a_i) = \lim_n \prod_{i\in A_n}(1+a_i).$$

Démonstration. Soit $\varepsilon > 0$. Par le théorème 12.5 il existe J_0 une partie finie de I telle que pour toute partie finie J de I contenant J_0 on a :

$$\left| \prod_{j\in J}(1+a_j) - \ell \right| < \varepsilon$$

Or il existe $N \in \mathbb{N}$ tel que $J_0 \subseteq A_N$ car J_0 est fini et I est recouvert par les A_n. Ainsi, pour tout $n \geq N$, on a $A_n \supseteq A_N \supseteq J_0$ et donc :

$$\left| \prod_{i\in A_n}(1+a_i) - \ell \right| < \varepsilon$$

comme voulu. □

Le théorème suivant permet de manipuler les produits infinis plus facilement : on peut regrouper les facteurs comme on le souhaite.

Théorème 12.10. *(Produit par paquets) Soit I un ensemble et $(J_\lambda)_{\lambda\in\Lambda}$ une partition de I. Soit $(a_i)_{i\in I}$ une famille de réels positifs et (b_i) une famille de complexes telle que le produit des $1+b_i$ converge absolument. On a :*

$$\prod_{i\in I}(1+a_i) = \prod_{\lambda\in\Lambda}\prod_{j\in J_\lambda}(1+a_j)$$

Il s'agit d'une égalité entre deux éléments de $[1,+\infty]$. Par convention, $+\infty \times a = +\infty$ pour tout réel strictement positif a. De plus, pour tout $\lambda \in \Lambda$, le produit des $1+b_j$ avec $j \in J_\lambda$ converge absolument, et le produit des $\prod_{j\in J_\lambda}(1+b_j)$ avec $\lambda \in \Lambda$ converge absolument, et on a :

$$\prod_{i\in I}(1+b_i) = \prod_{\lambda\in\Lambda}\prod_{j\in J_\lambda}(1+b_j)$$

Démonstration. Soit K une partie finie de I. On a :

$$\prod_{k\in K}(1+a_k)=\prod_{\lambda\in\Lambda}\prod_{k\in J_\lambda\cap K}(1+a_k)\leq\prod_{\lambda\in\Lambda}\prod_{j\in J_\lambda}(1+a_j)$$

car il y a un nombre fini de $\lambda\in\Lambda$ pour lesquels $J_\lambda\cap K$ est non vide. En passant à la borne supérieure sur les parties finies K de I on obtient :

$$\prod_{i\in I}(1+a_i)\leq\prod_{\lambda\in\Lambda}\prod_{j\in J_\lambda}(1+a_j)$$

Ensuite, soit L une partie finie de Λ. Soit $(K_\ell)_{\ell\in L}$ une famille de parties finies de chaque J_ℓ. On a naturellement :

$$\prod_{\ell\in L}\prod_{k\in K_\ell}(1+a_j)=\prod_{i\in\bigsqcup_{\ell\in L}K_\ell}(1+a_i)\leq\prod_{i\in I}(1+a_i)$$

On passe alors successivement à la borne supérieure sur les parties finies K_ℓ de chaque J_ℓ (cela fait un nombre fini d'opérations à effectuer) et on obtient :

$$\prod_{\ell\in L}\prod_{k\in J_\ell}(1+a_j)\leq\prod_{i\in I}(1+a_i)$$

On passe enfin à la borne supérieure sur les parties finies L de Λ pour obtenir la deuxième inégalité :

$$\prod_{i\in I}(1+a_i)\geq\prod_{\lambda\in\Lambda}\prod_{j\in J_\lambda}(1+a_j)$$

Passons au cas des b_i complexes. Puisque le produit des $1+b_i$ converge absolument, on a :

$$\prod_{\lambda\in\Lambda}\prod_{j\in J_\lambda}(1+\left|b_j\right|)<\infty$$

en utilisant ce qui précède avec $a_i=\left|b_j\right|$. Chacun des facteurs du produit portant sur λ est un réel supérieur ou égal à 1 et donc chaque facteur est fini. Ainsi, pour tout $\lambda\in\Lambda$, le produit des $1+b_j$ avec $j\in J_\lambda$ converge absolument, et le produit des $\prod_{j\in J_\lambda}(1+b_j)$ avec $\lambda\in\Lambda$ converge absolument. On pose :

$$P=\prod_{i\in I}(1+b_i)$$

On commence par traiter le cas où Λ possède *deux éléments* : on a $I=J_1\sqcup J_2$ et on veut voir que :

$$P=\prod_{i\in J_1}(1+b_i)\times\prod_{i\in J_2}(1+b_i).$$

On peut supposer I dénombrable, et il existe alors (A_n) une suite croissante de parties finies de J_1 qui recouvre J_1 et il existe (B_n) une suite croissante de parties finies de J_2 qui recouvre J_2. Par continuité de la multiplication on obtient :

$$\prod_{i\in J_1}(1+b_i)\times\prod_{i\in J_2}(1+b_i)=\lim_n\prod_{i\in A_n}(1+b_i)\times\prod_{i\in B_n}(1+b_i)=\lim_n\prod_{i\in A_n\sqcup B_n}(1+b_i)=P$$

car la suite $(A_n \sqcup B_n)$ est une suite croissante de parties finies de I qui recouvre I. Par récurrence on obtient aussi le théorème lorsque Λ est une partie *finie*. Enfin, on traite le cas général.
Soit $\varepsilon > 0$, il existe K_0 une partie finie de I telle que pour toute partie finie K de I contenant K_0, on a :

$$\left| \prod_{k \in K} (1 + b_k) - P \right| < \varepsilon$$

On pose alors :

$$L_0 = \{\lambda \in \Lambda \mid J_\lambda \cap K_0 \neq \emptyset\}$$

qui est une partie finie de Λ. Soit L une partie finie de Λ contenant L_0. D'après le cas où Λ est fini, on a :

$$\prod_{\ell \in L} \prod_{j \in J_\ell} (1 + b_j) = \prod_{j \in \bigsqcup_{\ell \in L} J_\ell} (1 + b_j)$$

Ainsi :

$$\left| \prod_{\ell \in L} \prod_{j \in J_\ell} (1 + b_j) - P \right| = \left| \prod_{j \in \bigsqcup_{\ell \in L} J_\ell} (1 + b_j) - P \right| \leq \varepsilon$$

car $\prod_{j \in \bigsqcup_{\ell \in L} J_\ell} (1 + b_j)$ est dans l'adhérence des $\prod_{k \in K} (1 + b_k)$ puisque $K_0 \subseteq \bigsqcup_{\ell \in L} J_\ell$. □

Remarque 12.11. Le théorème précédent devient le théorème de *Fubini* pour les produits lorsque la partition provient d'un produit cartésien $I = J_1 \times J_2$. On laisse au lecteur le soin d'énoncer ce théorème.

12.2 Séries de Dirichlet

Définition 12.12. *Soit $f : \mathbb{N}^* \longrightarrow \mathbb{C}$ une application. On définit la série de Dirichlet associée par :*

$$L_f(s) = \sum_{n \geq 1} \frac{f(n)}{n^s}$$

pour $s \in \mathbb{C}$ tel que la série converge.

Proposition 12.13. *Soit $f : \mathbb{N}^* \longrightarrow \mathbb{C}$ une application et $s_0 \in \mathbb{C}$ tel que la série définissant $L_f(s_0)$ converge absolument. Alors la série définissant L_f converge normalement sur le demi-plan fermé $\{\mathrm{Re}(s) \geq \mathrm{Re}(s_0)\}$. En particulier, L_f est holomorphe sur l'intérieur de ce demi-plan fermé.*
Dans le cas où il existe un tel s_0, si L_f est nulle en tout s tel que $\mathrm{Re}(s) > \mathrm{Re}(s_0)$, alors f est nulle. On ne perd donc pas d'information sur f en considérant L_f.

Démonstration. On note $u = \mathrm{Re}(s_0)$. Soit s vérifiant $\mathrm{Re}(s) \geq u$. On a :

$$\left| \frac{f(n)}{n^s} \right| = |f(n)| \exp(-\mathrm{Re}(s) \log(n)) \leq |f(n)| \exp(-u \log(n)) \leq |f(n)|/n^u$$

Or $\sum |f(n)|/n^u = \sum \left|\frac{f(n)}{n^{s_0}}\right| < \infty$ par hypothèse.
Ensuite, supposons $f \neq 0$. Il existe alors $m \geq 1$ minimal tel que $f(m) \neq 0$. Pour $x > u$, on a :

$$0 = L_f(x) = f(m)/m^x + \sum_{n>m} f(n)/n^x$$

De plus :

$$\left|\sum_{n>m} f(n)/n^x\right| \leq \sum_{n>m} \frac{|f(n)|}{n^u} n^{u-x} \leq \sum_{n>m} \frac{|f(n)|}{n^u} (m+1)^{u-x} \leq C \times (m+1)^{u-x}$$

en posant $C = \sum_{n\geq 1} |f(n)| n^u < \infty$. On a donc :

$$|f(m)| \leq C m^x (m+1)^{u-x} \longrightarrow 0$$

quand x tend vers $+\infty$. C'est absurde. □

L'exemple fondamental de série de Dirichlet est la fonction Zeta de Riemann définie comme L_1 :

$$\zeta(s) = L_1(s) = \sum_{n\geq 1} \frac{1}{n^s}.$$

D'après la proposition précédente, cette formule définit une fonction holomorphe sur le demi-plan $\mathrm{Re}(s) > 1$. On admet dans la suite que la fonction ζ de Riemann se prolonge en une fonction méromorphe sur $\mathbb{C}$, toujours notée ζ, dont le seul pôle est un pôle simple de résidu 1 en $s = 1$. On pourra trouver une preuve de ce résultat célèbre dans [2], paragraphe 2.4.

Proposition 12.14. *Soit $f : \mathbb{N}^* \longrightarrow \mathbb{C}$ une application telle que :*

$$\sum_{n=1}^{N} f(n) = O(N^r)$$

quand N tend vers $+\infty$, avec r un réel positif. Alors la série définissant L_f converge uniformément sur tout compact du demi-plan ouvert $\mathrm{Re}(s) > r$. En particulier, L_f est holomorphe sur ce demi-plan ouvert.

Remarque 12.15. Il n'y a pas nécessairement convergence absolue en tout point dans cette situation.

Démonstration. On pose :

$$F(n) = \sum_{k=1}^{n} f(k)$$

et $F(0) = 0$ de sorte que $F(n) = O(n^r)$ par hypothèse. Pour tout complexe s et tout $N \geq 1$, on a :

$$\sum_{n=1}^{N} \frac{f(n)}{n^s} = \sum_{n=1}^{N} \frac{F(n) - F(n-1)}{n^s} = \sum_{n=1}^{N-1} F(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + \frac{F(N)}{N^s}.$$

On se place sur un compact de la forme :

$$[a,b]\times[-c,c]\subseteq\{\mathrm{Re}(s)>r\}$$

avec $r<a<b$ et $c>0$. Pour $s=x+iy$ dans ce compact on a :

$$\begin{aligned}\left|\frac{1}{n^s}-\frac{1}{(n+1)^s}\right| &\leq \frac{1}{(n+1)^x}\left|\left(1+\frac{1}{n}\right)^s-1\right| \leq \frac{1}{(n+1)^x}\left|\left(1+\frac{1}{n}\right)^x-1\right|+\frac{1}{(n+1)^x}\left|\left(1+\frac{1}{n}\right)^x-\left(1+\frac{1}{n}\right)^s\right| \\ &\leq \frac{1}{(n+1)^a}\left(\left(1+\frac{1}{n}\right)^x-1\right)+\frac{1}{n^x}\left|1-\exp\left(iy\log\left(1+\frac{1}{n}\right)\right)\right| \\ &\leq \frac{1}{(n+1)^a}\left(\left(1+\frac{1}{n}\right)^b-1\right)+\frac{2}{n^x}\left|\sin\left(\frac{y}{2}\log\left(1+\frac{1}{n}\right)\right)\right| \\ &\leq \frac{1}{n^a}\left(\left(1+\frac{1}{n}\right)^b-1\right)+\frac{|y|}{n^a}\left|\log\left(1+\frac{1}{n}\right)\right| \\ &\leq \frac{1}{n^a}\left(\left(1+\frac{1}{n}\right)^b-1\right)+\frac{c}{n^a}\left|\log\left(1+\frac{1}{n}\right)\right|\end{aligned}$$

en utilisant $|\sin t|\leq|t|$ et $\left|1-e^{it}\right|=\left|e^{-it/2}-e^{it/2}\right|=2|\sin(t/2)|$ pour tout réel t. On peut alors borner $F(n)\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)$ de façon indépendante de $s\in[a,b]\times[-c,c]$ par :

$$\frac{F(n)}{n^a}\left(\left(1+\frac{1}{n}\right)^b-1+c\log\left(1+\frac{1}{n}\right)\right)=O(n^{r-a-1}).$$

Or on a $r-a-1<-1$ donc la suite des sommes partielles :

$$\sum_{n=1}^{N-1}F(n)\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)$$

converge uniformémént sur $[a,b]\times[-c,c]$. Enfin il est clair que $F(N)/N^s$ tend vers 0 uniformément sur tout compact du demi-plan $\mathrm{Re}(s)>r$. □

Proposition 12.16. *Soit $f:\mathbb{N}^*\longrightarrow\mathbb{C}$ une application telle que :*

$$\sum_{n=1}^{N}f(n)=\rho N+O(N^r)$$

quand N tend vers $+\infty$, avec $r\in[0,1[$ et $\rho\neq0$. Alors L_f définit une fonction holomorphe sur le demi-plan ouvert $\mathrm{Re}(s)>1$ qui se prolonge en une fonction méromorphe, toujours notée L_f, sur le demi-plan $\mathrm{Re}(s)>r$. Cette fonction a un seul pôle, en $s=1$, et c'est un pôle simple de résidu ρ.

Démonstration. D'abord on a :

$$\sum_{n=1}^{N}f(n)=O(N)$$

donc par ce qui précède L_f définit une fonction holomorphe sur le demi-plan ouvert $\mathrm{Re}(s) > 1$. Ensuite on écrit :

$$f(n) = g(n) + \rho$$

de sorte que g vérifie l'hypothèse de la proposition 12.14 et ainsi L_f est la somme de L_g, qui est holomorphe sur le demi-plan $\mathrm{Re}(s) > r$ et de $\rho\zeta$ qui est méromorphe sur $\mathbb{C}$ avec pour seul pôle un pôle simple de résidu ρ en $s = 1$ d'après les propriétés admises de la fonction ζ de Riemann. □

12.3 Produits eulériens

On fixe A un anneau de Dedekind.

Définition 12.17. *Soit $f : \mathcal{I}_A \longrightarrow \mathbb{C}$ une application. On dit que f est multiplicative (resp. complétement multiplicative) si $f(1) = 1$, et pour tous $a, b \in I_A$ premiers entre eux (resp. pour tous $a, b \in I_A$) on a :*

$$f(ab) = f(a)f(b)$$

Ainsi une application multiplicative est entièrement déterminée par ses valeurs sur les puissances des premiers et une application complétement multiplicative est entièrement déterminée par ses valeurs sur les premiers de A.

Théorème 12.18. *Soit $f : \mathcal{I}_A^* \longrightarrow \mathbb{R}_+^*$ une application multiplicative réelle positive et soit $g : \mathcal{I}_A \longrightarrow \mathbb{C}$ une application. Si f est positive, on a :*

$$\sum_{I \in \mathcal{I}_A} f(I) = \prod_{p \in \mathbb{P}_A} \left(\sum_{k \geq 0} f(p^k) \right)$$

Si g est sommable, au sens où $\sum_{I \in \mathcal{I}_A} |g(I)| < \infty$, alors :

$$\sum_{I \in \mathcal{I}_A} g(I) = \prod_{p \in \mathbb{P}_A} \left(\sum_{k \geq 0} g(p^k) \right)$$

avec un produit qui converge absolument. Enfin, si g est sommable et complétement multiplicative on a :

$$\sum_{I \in \mathcal{I}_A} g(I) = \prod_{p \in \mathbb{P}_A} \frac{1}{1 - g(p)}$$

avec un produit qui converge absolument.

Démonstration. Soit F une partie finie de $\mathbb{P}_A$. On a :

$$\begin{aligned} \prod_{p \in F} \left(\sum_{k \geq 0} f(p^k) \right) &= \sum_{(k_p) \in \mathbb{N}^F} \prod_{p \in F} f\left(p^{k_p}\right) \\ &= \sum_{(k_p) \in \mathbb{N}^F} f\left(\prod_{p \in F} p^{k_p} \right) \end{aligned}$$

par positivité de f puis par multiplicativité de f. Puisque A est un anneau de Dedekind, la factorisation unique en produit de premiers donne :

$$\prod_{p\in F}\left(\sum_{k\geq 0} f(p^k)\right) = \sum_{I\in S_F} f(I)$$

avec S_F l'ensemble des idéaux I de A dont les diviseurs premiers sont dans F. On passe à la borne supérieure sur toutes les parties finies F de $\mathbb{P}_A$:

$$\prod_{p\in \mathbb{P}_A}\left(\sum_{k\geq 0} f(p^k)\right) = \sum_{I\in \mathcal{I}_A} f(I)$$

car $\sum_{k\geq 0} f(p^k) \geq 1$.

Traitons maintenant le cas de g. En appliquant ce qui précède à $f = |g|$, on obtient que les sommes $\sum_{k\geq 0} g(p^k)$ convergent absolument et le produit infini converge absolument. Soit $\varepsilon > 0$. Il existe une partie finie F_0 de $\mathbb{P}_A$ telle que pour toute partie finie F de $\mathbb{P}_A$ contenant F_0, on a :

$$\left|\prod_{p\in F}\left(\sum_{k\geq 0} g(p^k)\right) - \prod_{p\in \mathbb{P}_A}\left(\sum_{k\geq 0} g(p^k)\right)\right| < \varepsilon$$

et ainsi :

$$\left|\sum_{I\in S_F} g(I) - \prod_{p\in \mathbb{P}_A}\left(\sum_{k\geq 0} g(p^k)\right)\right| < \varepsilon$$

pour toute partie finie F de $\mathbb{P}_A$ contenant F_0. On conclut alors par définition de la somme d'une famille sommable :

$$\sum_{I\in \mathcal{I}_A} g(I) = \prod_{p\in \mathbb{P}_A}\left(\sum_{k\geq 0} g(p^k)\right)$$

comme voulu. □

12.4 Fonction ζ d'un corps de nombres

On considère K un corps de nombres de degré d. On note $\mathbb{P}_K$ l'ensemble des premiers de l'anneau de Dedekind $\mathcal{O}_K$, autrement dit l'ensemble de ses idéaux premiers non nuls.

Définition 12.19. *On définit la fonction ζ_K de Dedekind associée à K de la façon suivante :*

$$\zeta_K(s) = \sum_I \frac{1}{\|I\|^s}$$

où la somme porte sur tous les idéaux non nuls de $\mathcal{O}_K$.

Théorème 12.20. *(Formule analytique du nombre de classes) La somme définissant ζ_K converge normalement sur tout compact de $\{\mathrm{Re}(s) > 1\}$. De plus, ζ_K se prolonge méromorphiquement sur $\{\mathrm{Re}(s) > 1 - 1/d\}$ avec pour unique pôle un pôle simple en $s = 1$. On dispose enfin de la formule suivante :*

$$\mathrm{Res}(\zeta_K, 1) = \kappa h = \frac{2^{r+s}\pi^s \,\mathrm{Reg}(K) h}{|\mathbb{U}_\infty(K)| \sqrt{|\mathrm{Disc}\, K|}}$$

avec h le nombre de classes de K c'est à dire l'ordre du groupe des classes $\mathrm{Cl}(K)$. Le régulateur de K, $\mathrm{Reg}(K)$ est défini en 6.33.

Démonstration. Soit $x > 1$ un réel. Montrons que la somme de termes positifs $\sum_I \frac{1}{\|I\|^x}$ est finie. Puisque tout est positif, on a :

$$\sum_I \frac{1}{\|I\|^x} = \sum_{n \geq 1} \frac{\nu(n) - \nu(n-1)}{n^x}$$

avec les notations de 11.8. Ici $\nu(n) - \nu(n-1)$ est le nombre d'idéaux non nuls de $\mathcal{O}_K$ de norme n. Posons $f(n) = \nu(n) - \nu(n-1)$ de sorte que :

$$\sum_{k=1}^{n} f(k) = \nu(n) = \kappa h n + O\left(n^{1-1/d}\right)$$

Ainsi la série définissant L_f converge normalement sur tout compact du demi-plan $\mathrm{Re}(s) > 1$ et d'après la proposition 12.16 elle définit une fonction méromorphe sur le demi-plan $\mathrm{Re}(s) > 1 - 1/d$ dont le seul pôle est un pôle simple en $s = 1$ de résidu κh. En particulier pour $x > 1$:

$$\sum_I \frac{1}{\|I\|^x} < \infty$$

donc la somme définissant ζ_K converge normalement sur tout compact du demi-plan $\mathrm{Re}(s) > 1$ et coïncide sur $]1, +\infty[$ avec L_f donc coïncide partout avec L_f. Ainsi $\zeta_K = L_f$ et on a :

$$\mathrm{Res}(\zeta_K, 1) = \kappa h.$$

□

Remarque 12.21. Soit $\mathcal{C} \subseteq \mathrm{Cl}(K)$. Pour C une classe d'idéaux on note C^+ l'ensemble des éléments de C contenus dans $\mathcal{O}_K$. On peut alors définir une fonction ζ associée à $\mathcal{C}$ par :

$$\sum_{I \in \bigsqcup_{C \in \mathcal{C}} C^+} \frac{1}{\|I\|^s}$$

et on a, avec la même preuve, un résidu en $s = 1$ relié au cardinal de $\mathcal{C}$. Par exemple en considérant $\mathcal{C} = \mathrm{Cl}(K)[2]$, la 2-torsion du groupe des classes, on obtient une formule analytique pour $h_2(K)$, la taille de la 2-torsion du groupe des classes.
La taille de $h_2(K)$ en fonction du discriminant de K est d'ailleurs un sujet de recherche active en théorie des nombres : un article de 2017 de Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, Zhao, [1], donne une borne asymptotique pour ce nombre, qui reste loin de la borne conjecturée.

Le théorème 12.18 permet d'écrire la fonction ζ_K comme un produit infini.

Proposition 12.22. *Pour* $\mathrm{Re}(s) > 1$, *le produit suivant converge absolument et on a l'égalité :*

$$\prod_{\mathfrak{p}} \frac{1}{1 - \|\mathfrak{p}\|^{-s}} = \zeta_K(s)$$

où le produit porte sur tous les premiers de K.

Démonstration. Fixons s de partie réelle $x > 1$. On applique le théorème 12.18 à la fonction complétement multiplicative :

$$I \mapsto \|I\|^{-s}.$$

Pour cela on vérifie qu'elle est sommable, c'est à dire que :

$$\sum_I \left| \frac{1}{\|I\|^s} \right| < \infty.$$

En effet, on a :

$$\sum_I \left| \frac{1}{\|I\|^s} \right| = \sum_I \frac{1}{\|I\|^x} < \infty$$

car $x > 1$. □

12.5 Caractères et fonctions L

Dans certains cas, le théorème 12.20 qui donne la formule analytique du nombre de classes permet de calculer explicitement le nombre de classes d'un corps de nombres. On fera ce calcul dans le cas des corps quadratiques, en se référant à [9], chapitre 7. Pour cela on a besoin de la notion de caractères de Dirichlet et des fonctions L qui leur sont associées.
Soit $m \geq 1$ un entier. On rappelle qu'étant donné un groupe abélien fini G, on peut considérer son groupe dual $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times) = \mathrm{Hom}(G, \mathbb{U})$, et que ce groupe est alors un groupe abélien (non canoniquement) isomorphe à G. Les éléments de ce groupe sont appelés les *caractères* de G.

Remarque 12.23. On rappelle que les caractères d'un groupe abélien forment une base orthonormale de l'espace hermitien des fonctions de G vers $\mathbb{C}$ muni du produit scalaire :

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} \overline{f(x)} g(x).$$

En particulier, pour χ un caractère non trivial, la relation d'orthogonalité $\langle \chi_1, \chi \rangle = 0$ avec χ_1 le caractère trivial (qui vaut toujours 1) donne :

$$\sum_{x \in G} \chi(x) = 0.$$

Donnons-en une démonstration très rapide :

$$\sum_{x\in G}\chi(x)=\sum_{y\in\mathrm{Im}(\chi)}y\left|\chi^{-1}(y)\right|=\sum_{y\in\mathrm{Im}(\chi)}y\,|\mathrm{Ker}\,\chi|=0$$

car $\mathrm{Im}\,\chi$ est un sous-groupe fini de $\mathbb{C}^\times$, c'est donc un certain $\mathbb{U}_n$ avec $n\geq 2$ car χ est non trivial, et la somme des racines n-èmes de l'unité pour $n\geq 2$ est une somme géométrique qui vaut 0.

Ainsi le groupe $(\mathbb{Z}/m\mathbb{Z})^\times$ possède $\varphi(m)$ caractères, appelés caractères modulo m. Étant donné χ un caractère de $(\mathbb{Z}/m\mathbb{Z})^\times$, on l'étend à $\mathbb{Z}/m\mathbb{Z}$ en posant $\chi(x)=0$ pour x non inversible modulo m. On peut ainsi voir χ comme une fonction définie sur $\mathbb{Z}$ en composant avec la projection canonique $\mathbb{Z}\longrightarrow\mathbb{Z}/m\mathbb{Z}$.

Définition 12.24. *Soit χ un caractère modulo m. On lui associe la fonction L suivante :*

$$L(s,\chi)=\sum_{n\geq 1}\frac{\chi(n)}{n^s}$$

c'est à dire la série de Dirichlet associée à la fonction χ.

Puisque $|\chi(n)|\leq 1$ pour tout $n\geq 1$, d'après la proposition 12.13, $L(\bullet,\chi)$ est une fonction holomorphe sur $\{\mathrm{Re}(s)>1\}$. De plus $n\mapsto\chi(n)/n^s$ est une fonction complétement multiplicative donc pour $\mathrm{Re}(s)>1$ on a le produit absolument convergent suivant, d'après 12.18 :

$$L(s,\chi)=\prod_p\frac{1}{1-\chi(p)p^{-s}}.$$

Le caractère trivial χ_1 modulo m est l'élément neutre de $(\mathbb{Z}/m\mathbb{Z})^\times$. Vu comme une fonction sur $\mathbb{Z}$, on a donc :

$$\chi_1(n)=\begin{cases}1 & \text{si } \mathrm{pgcd}(n,m)=1\\ 0 & \text{sinon}\end{cases}.$$

Proposition 12.25. *La fonction L associée au caractère trivial est donnée par :*

$$L(s,\chi_1)=\zeta(s)\prod_{p|m}(1-p^{-s}).$$

En particulier son prolongement méromorphe a un pôle simple en $s=1$ de résidu :

$$\mathrm{Res}(L(\bullet,\chi),1)=\prod_{p|m}\left(1-\frac{1}{p}\right).$$

Démonstration. Il suffit d'utiliser la formule du produit eulérien :

$$L(s,\chi)=\prod_p\frac{1}{1-\chi(p)p^{-s}}=\prod_{p\nmid m}\frac{1}{1-p^{-s}}=\prod_p\frac{1}{1-p^{-s}}\prod_{p|m}(1-p^{-s})=\zeta(s)\prod_{p|m}(1-p^{-s}).$$

Le reste découle du fait que la fonction ζ de Riemann a un pôle simple de résidu 1 en $s=1$. □

Pour un caractère χ non trivial, la fonction $L(\bullet, \chi)$ admet un prolongement holomorphe sur $\{\mathrm{Re}(s) > 0\}$ et on sait évaluer sa valeur en $s = 1$.

Proposition 12.26. *Soit χ un caractère modulo m non trivial. La fonction $L(\bullet, \chi)$ se prolonge en une fonction holomorphe sur le demi-plan ouvert $\{\mathrm{Re}(s) > 0\}$, et on a :*

$$L(1, \chi) = -\frac{1}{m} \sum_{\omega \in \mathbb{U}_m \setminus \{1\}} G_{\chi,\omega} \log(1 - \omega)$$

avec $G_{\chi,\omega}$ la somme de Gauss définie par :

$$G_{\chi,\omega} = \sum_{a \in \mathbb{Z}/m\mathbb{Z}} \frac{\chi(a)}{\omega^a}.$$

Démonstration. On calcule pour $\mathrm{Re}(s) > 1$ (la somme converge absolument donc on peut sommer par paquets) :

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) \sum_{n \equiv a\ [m], n \geq 1} \frac{1}{n^s} = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) \sum_{n \geq 1} \frac{\delta_a(n)}{n^s}$$

avec $\delta_a(n)$ qui vaut 1 si $n \equiv a\ [m]$ et 0 sinon. On calcule alors la transformée de Fourier discrète de la fonction δ_a, autrement dit on a pour tout $n \in \mathbb{Z}$:

$$\delta_a(n) = \frac{1}{m} \sum_{\omega \in \mathbb{U}_m} \omega^{n-a}$$

comme on peut le vérifier avec un calcul de somme géométrique. On en déduit :

$$L(s, \chi) = \frac{1}{m} \sum_{\omega \in \mathbb{U}_m} \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) \sum_{n \geq 1} \frac{\omega^{n-a}}{n^s} = \frac{1}{m} \sum_{\omega \in \mathbb{U}_m} \left(\sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \frac{\chi(a)}{\omega^a} \right) \sum_{n \geq 1} \frac{\omega^n}{n^s}.$$

Or pour $\omega = 1$, le facteur $\sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \frac{\chi(a)}{\omega^a}$ est nul car χ n'est pas le caractère trivial, par l'orthogonalité des caractères 12.23. On peut donc sommer seulement pour $\omega \neq 1$, et pour un tel ω, on a :

$$\sum_{n=1}^{N} \omega^n = \omega \frac{1 - \omega^N}{1 - \omega} = O(1)$$

donc par la proposition 12.14, la somme $\sum_{n \geq 1} \frac{\omega^n}{n^s}$ converge uniformément sur tout compact du demi-plan $\{\mathrm{Re}(s) > 0\}$ et y définit une fonction holomorphe, dont la valeur en $s = 1$ est :

$$\sum_{n \geq 1} \frac{\omega^n}{n} = -\log(1 - \omega)$$

avec la détermination principale du logarithme. Ainsi $L(\bullet, \chi)$ admet un prolongement holomorphe sur $\{\mathrm{Re}(s) > 0\}$ et sa valeur en $s = 1$ est bien celle donnée par l'énoncé. □

On souhaite calculer explicitement $|L(1,\chi)|$ pour χ non trivial. C'est difficile en général et on va faire une hypothèse sur χ pour pouvoir mener ce calcul : on va supposer que χ est **primitif**, au sens suivant.

Définition 12.27. *Soit $m \geq 1$ un entier. Pour tout $d \mid m$, on a un morphisme surjectif de restriction :*

$$(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\pi} (\mathbb{Z}/d\mathbb{Z})^\times$$

d'après 8.16. Par dualité, on a donc un morphisme injectif :

$$i : \widehat{(\mathbb{Z}/d\mathbb{Z})^\times} \hookrightarrow \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$$

au niveau des groupes duaux (qui à ψ associe $\psi \circ \pi$). L'image de ce morphisme est l'ensemble des caractères χ modulo m qui se factorisent par $(\mathbb{Z}/d\mathbb{Z})^\times$:

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^\times & \xrightarrow{\chi} & \mathbb{C}^\times \\ {\scriptstyle\pi}\big\downarrow & \nearrow & \\ (\mathbb{Z}/d\mathbb{Z})^\times & & \end{array}$$

autrement dit ce sont les caractères dont la restriction à $\operatorname{Ker}\pi$ est triviale.
Un caractère primitif modulo m est alors un caractère qui n'appartient à aucun sous-groupe $i\left(\widehat{(\mathbb{Z}/d\mathbb{Z})^\times}\right)$ avec $d < m$. De façon équivalente, un caractère est primitif si pour tout $d \mid m$, avec $d < m$, il existe $b \in (\mathbb{Z}/m\mathbb{Z})^\times$ tel que $b \equiv 1\ [d]$ et $\chi(b) \neq 1$.

Proposition 12.28. *Soit χ un caractère primitif modulo m. On fixe θ un générateur de $\mathbb{U}_m$, i.e. une racine primitive m-ème de l'unité. On a alors :*

$$\left|G_{\chi,\theta}\right| = \sqrt{m}.$$

De plus, si $\omega \in \mathbb{U}_m$ n'est pas une racine primitive, on a :

$$G_{\chi,\omega} = 0.$$

Enfin, pour toute racine primitive $\omega = \theta^k$ avec $k \in (\mathbb{Z}/m\mathbb{Z})^\times$, on a :

$$G_{\chi,\theta^k} = \overline{\chi(k)} G_{\chi,\theta}.$$

Démonstration. On commence par le troisième point (qui est valable même si χ n'est pas primitif). Si $k \in (\mathbb{Z}/m\mathbb{Z})^\times$, on a :

$$G_{\chi,\theta^k} = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \theta^{-ak}\chi(a) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \theta^{-a}\chi\left(\frac{a}{k}\right) = \frac{G_{\chi,\theta}}{\chi(k)} = \overline{\chi(k)} G_{\chi,\theta}$$

car la multiplication par k est une bijection de $(\mathbb{Z}/m\mathbb{Z})^\times$.
On montre maintenant le second point. Si ω n'est pas primitive, on peut trouver $d \mid m$

tel que $\omega \in \mathbb{U}_d$ et $d < m$. Puisque χ est primitif, il existe $b \in (\mathbb{Z}/m\mathbb{Z})^\times$ tel que $b \equiv 1\ [d]$ et $\chi(b) \neq 1$. Ainsi :

$$G_{\chi,\omega} = \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \omega^{-a}\chi(a) = \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \omega^{-ab}\chi(ab).$$

Or $\omega \in \mathbb{U}_d$ donc $\omega^b = \omega^1 = \omega$ et ainsi :

$$G_{\chi,\omega} = \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \omega^{-a}\chi(a)\chi(b) = \chi(b)G_{\chi,\omega}$$

donc $G_{\chi,\omega} = 0$ puisque $\chi(b) \neq 1$.
On montre enfin le premier point. On calcule :

$$\begin{aligned}
\left|G_{\chi,\theta}\right|^2 = G_{\chi,\theta}\cdot\overline{G_{\chi,\theta}} &= G_{\chi,\theta}\sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times}\overline{\chi(a)}\theta^a \\
&= \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times}\overline{\chi(a)}G_{\chi,\theta}\theta^a = \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} G_{\chi,\theta^a}\theta^a \qquad \text{par le premier point} \\
&= \sum_{a\in\mathbb{Z}/m\mathbb{Z}} G_{\chi,\theta^a}\theta^a \qquad \text{par le second point} \\
&= \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times}\chi(b)\sum_{a\in\mathbb{Z}/m\mathbb{Z}}\theta^a\theta^{-ab}.
\end{aligned}$$

Or $\sum_{a\in\mathbb{Z}/m\mathbb{Z}}\theta^a\theta^{-ab}$ est une somme géométrique qui vaut 0 si $b \not\equiv 1\ [m]$ (car θ est d'ordre m) et m sinon. On a donc :

$$\left|G_{\chi,\theta}\right|^2 = \chi(1)m = m$$

comme souhaité. □

On a tout ce qu'il faut pour calculer le module de $L(1,\chi)$.

Théorème 12.29. *Soit $m \geq 1$ et χ un caractère primitif non trivial modulo m. On a alors, en prenant la convention que $0\times\infty = 0$ (en réalité la somme ne porte que sur les k premiers avec m) :*

$$|L(1,\chi)| = \frac{1}{\sqrt{m}}\left|\sum_{k=1}^{m}\chi(k)\left(\log\sin\left(\frac{k\pi}{m}\right) - \frac{i\pi k}{m}\right)\right|.$$

On peut simplifier un peu plus en faisant une disjonction de cas selon si χ est pair ou impair, c'est à dire selon si $\chi(-1)$ vaut 1 ou -1 (on sait que $\chi(-1)$ est d'ordre au plus 2 dans $\mathbb{C}^\times$) :
Si χ est pair, on a :

$$|L(1,\chi)| = \frac{1}{\sqrt{m}}\left|\sum_{k=1}^{m}\chi(k)\log\sin\left(\frac{k\pi}{m}\right)\right|.$$

Si χ est impair, on a :

$$|L(1,\chi)| = \frac{\pi}{m\sqrt{m}}\left|\sum_{k=1}^{m}\chi(k)k\right|.$$

Démonstration. On pose $\theta = \exp\left(\frac{2i\pi}{m}\right)$ une racine primitive m-ème de l'unité. Pour tout k entre 1 et $m-1$ on a :

$$\log(1-\theta^k) = \log\left|1-\theta^k\right| + i\arg(1-\theta^k)$$

en choisissant l'argument entre $-\pi$ et π. Or on a :

$$1-\theta^k = e^{i\pi\frac{k}{m}}\left(e^{-i\pi\frac{k}{m}} - e^{i\pi\frac{k}{m}}\right) = -2i\sin\left(\frac{k\pi}{m}\right)e^{i\pi\frac{k}{m}}.$$

Or $\sin\left(\frac{k\pi}{m}\right) > 0$ donc :

$$\log(1-\theta^k) = \log 2 + \log\sin\left(\frac{k\pi}{m}\right) + i\frac{\pi k}{m} - i\frac{\pi}{2}.$$

Par la proposition 12.28, les sommes de Gauss $G_{\chi,\omega}$ sont nulles si ω n'est pas une racine primitive (car χ est primitif) et donc on a :

$$L(1,\chi) = \frac{-1}{m}\sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times} G_{\chi,\theta^k}\log(1-\theta^k) = \frac{-G_{\chi,\theta}}{m}\sum_{k=1}^{m}\overline{\chi(k)}\left(\log\left|\sin\left(\frac{k\pi}{m}\right)\right| + i\frac{\pi k}{m}\right)$$

en utilisant le troisième point de la proposition 12.28 et le fait que $\sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times}\overline{\chi(k)} = 0$. On a mis des valeurs absolues sur le sinus pour qu'il ne dépende pas du choix du représentant de k. Si on force ce représentant à être entre 1 et m, les valeurs absolues sont inutiles.
En conjugant et en utilisant le premier point de 12.28, on obtient la première formule annoncée.
Ensuite, si χ est pair, on a :

$$\sum_{k=1}^{m}\chi(k)k = \sum_{k=1}^{m}\chi(-k)(m-k) = 0 - \sum_{k=1}^{m}\chi(k)k$$

donc cette somme est nulle, d'où la formule annoncée. C'est exactement le même raisonnement lorsque χ est impair pour retirer le terme en sinus. □

En exploitant certaines symétries, on peut rendre la formule encore plus simple d'un point de vue calculatoire.

Lemme 12.30. *Si χ est pair, on a :*

$$\sum_{k=1}^{m}\chi(k)\log\sin\left(\frac{k\pi}{m}\right) = 2\sum_{1\le k<\frac{m}{2}}\chi(k)\log\sin\left(\frac{k\pi}{m}\right).$$

Si χ est impair et primitif, on a :

$$\sum_{k=1}^{m}\chi(k)k = \frac{m}{\overline{\chi}(2)-2}\sum_{1\le k<\frac{m}{2}}\chi(k).$$

Démonstration. Si χ est pair, la symétrie $k \mapsto m-k$ permet d'écrire :

$$\sum_{k=1}^{m} \chi(k) \log \left| \sin\left(\frac{k\pi}{m}\right) \right| = \sum_{1 \leq k < \frac{m}{2}} \chi(k) \log \sin\left(\frac{k\pi}{m}\right) + \sum_{\frac{m}{2} < k \leq m} \chi(k) \log \sin\left(\frac{k\pi}{m}\right).$$

En effet l'éventuel terme $k = m/2$ si m est pair ne contribue pas à la somme car $\log \sin(\pi/2) = 0$. Il suffit alors de remarquer que ces deux sommes sont les mêmes grâce à la symétrie $k \mapsto m-k$ car χ est pair.
Si χ est impair et primitif, on va distinguer le cas m pair et le cas m impair. On définit les quantités suivantes :

$$A = \sum_{k=1}^{m} k\chi(k)$$

ainsi que :

$$B = \sum_{k<m/2} k\chi(k)$$

et :

$$C = \sum_{k<m/2} \chi(k).$$

Le but est donc de calculer A.
Traitons d'abord le cas m impair. On a alors, d'une part :

$$A = \sum_{k<m/2} k\chi(k) + \sum_{m/2<k\leq m} k\chi(k) = B + \sum_{k<m/2} (m-k)\chi(-k) = 2B - mC.$$

D'autre part, en sommant sur les termes pairs et impairs séparément :

$$A = \sum_{1\leq k\leq m, 2|k} k\chi(k) + \sum_{1\leq k\leq m, 2\nmid k} k\chi(k) = \sum_{1\leq k\leq m, 2|k} k\chi(k) + \sum_{1\leq k\leq m, 2|k} (m-k)\chi(-k)$$

car m est impair, en faisant le changement de variable $k \mapsto m-k$. On a donc :

$$A = 2 \sum_{1\leq k\leq m, 2|k} k\chi(k) - m \sum_{1\leq k\leq m, 2|k} \chi(k) = 4\chi(2) \sum_{i<m/2} i\chi(i) - m\chi(2) \sum_{i<m/2} \chi(i) = 4\chi(2)B - m\chi(2)C.$$

En éliminant B, on obtient, puisque $\chi(2) \neq \frac{1}{2}$ (c'est un nombre de module 1) :

$$A = 2B - mC = \frac{mC(1-\chi(2))}{1-2\chi(2)} - \frac{mC(1-2\chi(2))}{1-2\chi(2)} = \frac{mC\chi(2)}{1-2\chi(2)} = \frac{mC}{\overline{\chi(2)}-2}$$

comme voulu.
On suppose maintenant que m est pair et on note $n = m/2$. Puisque χ est primitif, sa restriction à $\{x \in (\mathbb{Z}/m\mathbb{Z})^\times \mid x \equiv 1 \ [n]\}$ n'est pas triviale. Or cet ensemble est contenu dans $\{1, n+1\}$ et $\chi(1) = 1$, donc nécessairement $n+1 \in (\mathbb{Z}/m\mathbb{Z})^\times$ et $\chi(n+1) \neq 1$.
Ceci impose que m soit un multiple de 4 car $\frac{m}{2}+1$ et m sont premiers entre eux. En particulier n est pair et $(n+1)^2 \equiv n^2 + m + 1 \equiv 1 \ [m]$ car $n^2/m = \frac{n}{2} \in \mathbb{Z}$. Ainsi :

$$\chi(n+1)^2 = 1$$

or $\chi(n+1) \neq 1$ donc $\chi(n+1) = -1$. De plus, pour tout k impair :

$$nk \equiv n\ [m]$$

car $nk - n = n(k-1)$ et $2 \mid k-1$. Ainsi :

$$\chi(n+k) = \chi(nk+k) = \chi(k)\chi(n+1) = -\chi(k).$$

Cette formule est également vraie pour k pair puisque les deux membres valent 0. On obtient alors l'égalité suivante :

$$A = \sum_{k=1}^{n} k\chi(k) + \sum_{k=1}^{n} (k+n)\chi(k+n) = \sum_{k=1}^{n} k\chi(k) - \sum_{k=1}^{n} (k+n)\chi(k) = -nC$$

car $\chi(n) = 0$. Enfin :

$$A = -\frac{m}{2}C = \frac{mC}{\overline{\chi(2)} - 2}.$$

□

Au total, on obtient la formule plus facile à calculer suivante.

Théorème 12.31. *Soit $m \geq 1$ et χ un caractère primitif non trivial modulo m.*
Si χ est pair, on a :

$$|L(1,\chi)| = \frac{2}{\sqrt{m}} \left| \sum_{1 \leq k < \frac{m}{2}} \chi(k) \log \sin\left(\frac{k\pi}{m}\right) \right|.$$

Si χ est impair, on a :

$$|L(1,\chi)| = \frac{\pi}{\sqrt{m}|\chi(2) - 2|} \left| \sum_{1 \leq k < \frac{m}{2}} \chi(k) \right|.$$

12.6 Fonction ζ d'un corps de nombres abélien

Soit K un corps de nombres abélien de groupe de Galois G. Par le théorème de Kronecker-Weber, on peut plonger K dans un corps cyclotomique $\mathbb{Q}(\mathbb{U}_m)$, dont on identifie le groupe de Galois à $(\mathbb{Z}/m\mathbb{Z})^\times$ (voir 8.4). Ainsi on a un morphisme surjectif de restriction :

$$(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\pi} G$$

qui induit une injection par dualité :

$$\widehat{G} \hookrightarrow \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}.$$

On peut ainsi associer à tout caractère χ de G un caractère modulo m, noté $\chi^{(m)}$ ou simplement χ s'il n'y a pas d'ambiguïté sur le choix de m.
Puisque K est galoisien, pour tout nombre premier p on note simplement $e(p)$ et $f(p)$ les indices de ramification et d'inertie des premiers au dessus de p dans K et $r(p)$ le nombre de premiers au dessus de p dans K, de sorte que $e(p)f(p)r(p) = [K : \mathbb{Q}]$.

Lemme 12.32. *Soit p un nombre premier qui ne divise pas m. L'ordre de $\pi(p)$ dans G est égal à l'indice d'inertie $f(p)$. On a de plus :*

$$\prod_{\chi\in\widehat{G}}(1-\chi(p)p^{-s}) = (1-p^{-sf(p)})^{r(p)} = \prod_{\mathfrak{p}\ni p}(1-\|\mathfrak{p}\|^{-s})$$

pour tout complexe s.

Démonstration. Puisque p ne divise pas m, p n'est pas ramifié dans $\mathbb{Q}(\mathbb{U}_m)$ et donc n'est pas ramifié dans K (voir 8.20 par exemple). Puisque K est abélien, le Frobenius modulo p définit un élément φ_p de G pour K et donne l'élément p de $(\mathbb{Z}/m\mathbb{Z})^\times$ pour $\mathbb{Q}(\mathbb{U}_m)$. Or le diagramme suivant est clairement commutatif :

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^\times & \twoheadrightarrow & G \\ \uparrow & & \uparrow \\ \overline{G}(\mathfrak{q}\mid p) & \twoheadrightarrow & \overline{G}(\mathfrak{p}\mid p) \end{array}$$

en choisissant $\mathfrak{q}\supseteq\mathfrak{p}\ni p$ des premiers de $\mathbb{Q}(\mathbb{U}_m)$ et de K. Ainsi on a $\pi(p)=\varphi_p$ et l'ordre de $\pi(p)$ dans G est donc égal à l'ordre de $x\mapsto x^p$ dans $\overline{G}(\mathfrak{p}\mid p)$, qui est exactement $f(\mathfrak{p}\mid p)=f(p)$.
Ensuite, remarquons que l'application $\eta:\widehat{G}\longrightarrow\mathbb{C}^\times$ qui à χ associe $\chi(\pi(p))$ est un morphisme de groupes, et comme $\pi(p)$ est d'ordre $f(p)$, ce morphisme est à valeurs dans $\mathbb{U}_{f(p)}$, et il est surjectif : il existe un caractère sur $\langle\pi(p)\rangle$ dont l'image est $\mathbb{U}_{f(p)}$ et tout caractère d'un sous-groupe se prolonge en un caractère de G.
Ainsi le noyau de ce morphisme η est de cardinal $\left|\widehat{G}\right|/f(p)=|G|/f(p)=e(p)r(p)=r(p)$ car p n'est pas ramifié et G est isomorphe à son dual (non canoniquement).
On en déduit :

$$\prod_{\chi\in\widehat{G}}(1-\chi(p)p^{-s}) = \prod_{\omega\in\mathbb{U}_{f(p)}}\prod_{\chi\in\eta^{-1}(\omega)}(1-\omega p^{-s}) = \prod_{\omega\in\mathbb{U}_{f(p)}}(1-\omega p^{-s})^{r(p)} = (1-p^{-sf(p)})^{r(p)}.$$

De plus on a :

$$\prod_{\mathfrak{p}\ni p}(1-\|\mathfrak{p}\|^{-s}) = \prod_{\mathfrak{p}\ni p}\left(1-p^{-sf(p)}\right) = (1-p^{-sf(p)})^{r(p)}.$$

□

De ce calcul on déduit une factorisation de la fonction ζ_K.

Théorème 12.33. *Soit K un corps de nombres abélien. La fonction ζ_K admet un prolongement méromorphe à $\{\mathrm{Re}(s)>0\}$ avec un seul pôle, en $s=1$, qui est un pôle simple. Si K est plongé dans $\mathbb{Q}(\mathbb{U}_m)$, on a :*

$$\zeta_K(s) = \zeta(s)\prod_{\chi\in\widehat{G}\setminus\{\chi_1\}}L(s,\chi^{(m)})\prod_{p\mid m}(1-p^{-s})\left(1-p^{-sf(p)}\right)^{-r(p)}$$

et :

$$\mathrm{Res}(\zeta_K,1) = \prod_{\chi\in\widehat{G}\setminus\{\chi_1\}}L(1,\chi)\prod_{p\mid m}\left(1-\frac{1}{p}\right)\left(1-p^{-f(p)}\right)^{-r(p)}.$$

Démonstration. On plonge K dans un $\mathbb{Q}(\mathbb{U}_m)$ par Kronecker-Weber. Par le théorème des zéros isolés, il suffit de montrer cette égalité pour $\mathrm{Re}(s) > 1$, là où on a de la convergence absolue des produits infinis :

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \|\mathfrak{p}\|^{-s}} = \prod_{p} \prod_{\mathfrak{p} \ni p} \frac{1}{1 - \|\mathfrak{p}\|^{-s}} = \prod_{p} \prod_{\chi \in \widehat{G}} \frac{1}{1 - \chi(p) p^{-s}} \prod_{p \mid m} \left(1 - p^{-sf(p)}\right)^{-r(p)}$$

car, pour $p \mid m$, on a $\chi(p) = 0$ et la formule du lemme 12.32 n'est a priori valable que pour $p \mid m$. On peut réécrire cela en introduisant les fonctions $L(\bullet, \chi^{(m)})$:

$$\begin{aligned} \zeta_K(s) &= \prod_{\chi \in \widehat{G}} L(s, \chi^{(m)}) \prod_{p \mid m} \left(1 - p^{-sf(p)}\right)^{-r(p)} \\ &= \zeta(s) \prod_{\chi \in \widehat{G} \setminus \{\chi_1\}} L(s, \chi^{(m)}) \prod_{p \mid m} (1 - p^{-s}) \left(1 - p^{-sf(p)}\right)^{-r(p)}. \end{aligned}$$

par un simple calcul de $L(s, \chi_1)$.
On utilise ensuite le fait que ζ a un pôle simple en $s = 1$ de résidu 1 et que les caractères $\chi^{(m)}$ pour $\chi \neq \chi_1$ ne sont pas triviaux pour conclure à l'aide de 12.26 (noter qu'on sait que ζ_K a un pôle simple en $s = 1$ car le résidu calculé dans la formule analytique du nombre de classes 12.20 est non nul, et cela montre que les $L(1, \chi^{(m)})$ sont non nuls). □

12.7 Symboles de Legendre et de Jacobi

Les caractères qui apparaissent dans le cas des corps quadratiques s'expriment en fonction du symbole de Legendre.

Définition 12.34. *(Symboles de Legendre et de Jacobi) Soit p un nombre premier impair et n un entier relatif. On définit le symbole de Legendre de la façon suivante :*

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ est premier avec } p \text{ et est un carré modulo } p \\ -1 & \text{si } n \text{ est premier avec } p \text{ et n'est pas un carré modulo } p \\ 0 & \text{sinon} \end{cases}.$$

Puisque les carrés de $\mathbb{F}_p^\times$ forment un sous-groupe d'indice 2, $\left(\frac{\bullet}{p}\right)$ est un caractère modulo p. Ensuite, si m est un entier naturel impair, on définit le symbole de Jacobi en étendant le symbole de Legendre multiplicativement :

$$\left(\frac{n}{m}\right) = \prod_{p \geq 3} \left(\frac{n}{p}\right)^{v_p(m)}$$

de sorte que le symbole de Jacobi est défini pour $n \in \mathbb{Z}$ et $m \geq 1$ impair.

Puisque les symboles de Legendre sont complétement multiplicatifs en n, le symbole de Jacobi aussi, et par construction il est complétement multiplicatif en m, autrement dit pour tous $n, n' \in \mathbb{Z}$ et tous m, m' entiers naturels impairs :

$$\left(\frac{nn'}{m}\right) = \left(\frac{n}{m}\right)\left(\frac{n'}{m}\right)$$

et :

$$\left(\frac{n}{mm'}\right) = \left(\frac{n}{m}\right)\left(\frac{n}{m'}\right).$$

On fera attention à ce que si m n'est pas premier, le symbole de Jacobi $\left(\frac{n}{m}\right)$ n'indique pas en général si n est un carré modulo m.

Proposition 12.35. *Soit $m \geq 1$ un entier impair. Le symbole de Jacobi $\left(\frac{\bullet}{m}\right)$ est m-périodique et définit un caractère modulo m.*

Démonstration. Soit $n \in \mathbb{Z}$, on a :

$$\left(\frac{n+m}{m}\right) = \prod_{p|m}\left(\frac{n+m}{p}\right)^{v_p(m)} = \prod_{p|m}\left(\frac{n}{p}\right)^{v_p(m)} = \left(\frac{n}{m}\right)$$

car le symbole de Legendre modulo p est p-périodique.
Ensuite, si n et m sont premiers entre eux, n est premier à tous les diviseurs premiers de m donc :

$$\left(\frac{n}{m}\right) \neq 0.$$

Au contraire, si n et m ne sont pas premiers entre eux, un des symboles de Legendre modulo p pour un $p \mid m$ s'annule en n et le symbole de Jacobi aussi.
Puisque le symbole de Jacobi est multiplicatif en n, ceci suffit à dire qu'il définit un caractère modulo m. □

Un caractère modulo m est dit *quadratique* si il prend ses valeurs dans l'ensemble $\{-1, 1\}$. La proposition suivante servira dans la suite à démontrer la loi de réciprocité quadratique 12.40.

Proposition 12.36. *Pour p un nombre premier, le symbole de Legendre $\left(\frac{\bullet}{p}\right)$ est le seul caractère quadratique non trivial modulo p.*

Démonstration. Soit φ un caractère quadratique non trivial modulo p. Vu comme morphisme $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$, son noyau est un sous-groupe d'indice 2 du groupe $\mathbb{F}_p^\times$, or ce groupe est cyclique donc il possède un seul sous-groupe d'indice 2 (à savoir le sous-groupe des carrés non nuls).
De plus φ est entièrement déterminée par son noyau, donc φ est le symbole de Legendre modulo p. □

Les nombres -1 et 2 ont un traitement particulier : on a des formules simples pour calculer $\left(\frac{-1}{m}\right)$ et $\left(\frac{2}{m}\right)$. Ces formules s'appellent les *lois complémentaires*, car elles viennent compléter la loi de réciprocité quadratique que l'on démontrera dans la suite.

Théorème 12.37. *(Lois complémentaires) Soit $m \geq 1$ un entier impair. On a :*

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

et :

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}.$$

Démonstration. On traite d'abord le cas où $m = p$ est un nombre premier.
Pour ce qui est de -1, notons qu'on a une suite exacte :

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{F}_p^\times \overset{x\mapsto x^2}{\longrightarrow} \mathbb{F}_p^\times \overset{x\mapsto x^{\frac{p-1}{2}}}{\longrightarrow} \{\pm 1\} \longrightarrow 1.$$

En effet, si $f(x) = x^2$ et $g(x) = x^{\frac{p-1}{2}}$, on a $g \circ f = 1$, puis $g(x)^2 = x^{p-1} = 1$ par le petit théorème de Fermat, donc $g(x) \in \{\pm 1\}$. Le noyau de g est d'ordre au plus $\frac{p-1}{2}$ pour des raisons de degré, or l'image de f est d'ordre exactement $\frac{p-1}{2}$ donc $\mathrm{Ker}(g) = \mathrm{Im}(f)$.
Ainsi -1 est un carré modulo p si et seulement si il est dans l'image de f, autrement dit s'il est dans le noyau de g, i.e. si :

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

On en déduit directement l'une des lois complémentaires :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Pour savoir quand 2 est un carré modulo p, on s'inspire de l'égalité :

$$\sqrt{2} = \exp(i\pi/4) + \exp(-i\pi/4).$$

On considère $\omega \in \overline{\mathbb{F}_p}$ une racine 8-ème primitive de l'unité dans une clôture algébrique de $\mathbb{F}_p$. On rappelle que comme p est impair, il y a 8 racines 8-èmes de l'unité dans $\overline{\mathbb{F}_p}$ (voir 8.13). On a alors :

$$\left(\omega + \frac{1}{\omega}\right)^2 = \omega^2 + \omega^{-2} + 2 = \omega^2 + \omega^6 + 2 = \omega^2(1 + \omega^4) + 2 = 2$$

car ω^4 est une racine primitive 2-ème de l'unité, i.e. $\omega^4 = -1$.
On en déduit que 2 est un carré modulo p si et seulement si $\omega + \omega^{-1} \in \mathbb{F}_p$, ce qui équivaut à ce que cet élément soit fixé par le groupe de Galois $\mathrm{Gal}(\mathbb{F}_p[\omega]/\mathbb{F}_p)$ qui est engendré par le Frobenius $x \mapsto x^p$. Ainsi 2 est un carré modulo p si et seulement si :

$$\omega + \omega^{-1} = \omega^p + \omega^{-p}.$$

On peut alors faire la disjonction de cas suivante :
Si $p \equiv 1\ [8]$, 2 est un carré modulo p.
Si $p \equiv 3\ [8]$, on a $\omega^3 + \omega^{-3} = -(\omega + \omega^{-1})$ car $\omega^4 = -1$ donc 2 n'est pas un carré modulo p.
Si $p \equiv 5\ [8]$, on est dans le même cas qu'avant car $\omega^{-5} = \omega^3$.

Si $p \equiv 7\ [8]$ enfin, on est dans le même cas que pour 1 modulo 8, donc 2 est un carré modulo p.
Autrement dit 2 est un carré modulo p si et seulement si $p \equiv \pm 1\ [8]$, ce qui se traduit par :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Pour $m \geq 1$ impair quelconque, par multiplicativité on a $\left(\frac{-1}{m}\right) = 1$ si et seulement si le nombre de diviseurs premiers de m congrus à 3 modulo 4 comptés avec multiplicités est pair, ce qui équivaut à ce que m soit congru à 1 modulo 4, ou encore à ce que $(-1)^{\frac{m-1}{2}} = 1$.
De même on a $\left(\frac{-1}{m}\right) = 1$ si et seulement si le nombre de diviseurs premiers de m congrus à ± 3 modulo 8 comptés avec multiplicité est pair (on peut s'en convaincre en regardant les puissances successives de 3 modulo 8), ce qui équivaut à ce que m soit congru à ± 1 modulo 8 ou encore à ce que $(-1)^{\frac{m^2-1}{8}} = 1$. □

12.8 Formule du nombre de classes d'un corps quadratique et loi de réciprocité quadratique

Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique avec $d \neq 0, 1$ sans facteur carré. On note Δ la valeur absolue de son discriminant, qui vaut $|d|$ si $d \equiv 1\ [4]$ et $4|d|$ sinon.
D'après 6.7, l'anneau des entiers de K est engendré par un élément ω dont le polynôme minimal P est unitaire de degré 2 et de discriminant Δ (voir la proposition 5.32). Par le théorème 9.19, K est contenu dans le corps cyclotomique $\mathbb{Q}(\mathbb{U}_\Delta)$. Le groupe de Galois G de K étant d'ordre 2, il possède un unique caractère non trivial χ.
Pour déterminer le caractère $\chi^{(\Delta)}$, il suffit de le calculer sa valeur sur les nombres premiers.

Lemme 12.38. *Soit p un nombre premier impair qui ne divise pas Δ. On a :*

$$\chi^{(\Delta)}(p) = \left(\frac{d}{p}\right)$$

et si 2 ne divise pas Δ (ce qui impose $d \equiv 1\ [4]$ et $\Delta = |d|$) :

$$\chi^{(\Delta)}(2) = \begin{cases} 1 & \text{si } d \equiv 1\ [8] \\ -1 & \text{si } d \equiv 5\ [8] \end{cases}.$$

De plus, pour $p \mid \Delta$ premier, on a bien entendu $\chi^{(\Delta)}(p) = 0$.

Démonstration. Puisque G est d'ordre 2, χ prend les valeurs 1 et -1 sur G. Si $p \nmid \Delta$, on a $\chi^{(\Delta)}(p) = -1$ si et seulement si l'ordre de $\pi(p)$ dans G vaut 2, autrement dit, d'après le lemme 12.32 si et seulement si $f(p) = 2$. Cette condition équivaut à ce que le polynôme P (polynôme minimal de ω un générateur de $\mathcal{O}_K$) soit irréductible modulo p d'après 5.48.

Si $p \geq 3$, cela équivaut à ce que le discriminant de ce polynôme, $\mathrm{Disc}(K)$, ne soit pas un carré modulo p (par la formule du trinôme qui fonctionne en caractéristique impaire), et donc :

$$\chi^{(\Delta)}(p) = \left(\frac{\mathrm{Disc(K)}}{p}\right) = \left(\frac{d}{p}\right)$$

car $\left(\frac{4}{p}\right) = 1$.
Si 2 ne divise pas Δ, on a $d \equiv 1\ [4]$ et $\Delta = |d|$, et P est donné par :

$$P = X^2 - X - \frac{d-1}{4}.$$

Le seul polynôme de degré 2 irréductible dans $\mathbb{F}_2$ est X^2+X+1, donc P est irréductible modulo 2 si et seulement si $\frac{d-1}{4}$ est impair, autrement dit si $d \equiv 5\ [8]$. On a donc :

$$\chi^{(\Delta)}(2) = \begin{cases} 1 & \text{si } d \equiv 1\ [8] \\ -1 & \text{si } d \equiv 5\ [8] \end{cases}$$

et ce sont les seuls cas car $d \equiv 1\ [4]$. □

Remarque 12.39. On aurait pu aussi définir un caractère comme ça et remarquer que la fonction ζ_K se factorise par $L(\bullet, \chi)$, mais il aurait été plus délicat de montrer que χ est bien un caractère (notamment que c'est une fonction Δ-périodique).

Pour pouvoir utiliser le théorème 12.31 et calculer $|L(1,\chi)|$, il reste à montrer que $\chi^{(\Delta)}$ est un caractère primitif. Pour cela on va d'abord démontrer la *loi de réciprocité quadratique*, qui permet de manipuler les symboles de Jacobi.

Théorème 12.40. *(Loi de réciprocité quadratique) Soient $m, n \geq 1$ impairs. On a :*

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)(-1)^{\frac{(m-1)(n-1)}{4}}.$$

Démonstration. On considère d'abord le cas où $m = p$ est un nombre premier impair. On pose :

$$p^* = (-1)^{\frac{p-1}{2}} p$$

c'est à dire que si $p \equiv 1\ [4]$ on a $p^* = p$ et sinon $p^* = -p$. De cette façon p^* est toujours congru à 1 modulo 4 et le corps quadratique $\mathbb{Q}(\sqrt{p^*})$ a pour discriminant p^*. On applique ce qui précède à ce corps : c'est un sous-corps de $\mathbb{Q}(\mathbb{U}_p)$, dont le groupe de Galois a pour unique caractère non trivial un caractère que l'on note φ, dont les valeurs sont spécifiées par le lemme 12.38. Ainsi $\varphi^{(p)}$ est un caractère quadratique non trivial modulo p, et c'est donc le symbole de Legendre modulo p d'après la proposition 12.36.
On en déduit que pour tout nombre premier impair q différent de p :

$$\left(\frac{p^*}{q}\right) = \varphi^{(p)}(q) = \left(\frac{q}{p}\right).$$

On utilise alors la multiplicativité et la loi complémentaire 12.37 :

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{-1}{q}\right)^{\frac{p-1}{2}} = \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}}.$$

Notons que cette formule est aussi valable si $p = q$ puisque dans ce cas les deux caractères sont nuls.
Soient alors $m, n \geq 1$ des entiers impairs. On utilise l'astuce de remplacer $(-1)^{\frac{n-1}{2}}$ par $\left(\frac{-1}{n}\right)$ à plusieurs reprises. Par multiplicativité, on a :

$$\begin{aligned}
\left(\frac{n}{m}\right) &= \prod_{p\geq 3}\prod_{q\geq 3}\left(\frac{q}{p}\right)^{v_q(n)v_p(m)} \\
&= \prod_{p\geq 3}\prod_{q\geq 3}\left(\frac{p}{q}\right)^{v_q(n)v_p(m)}\left(\frac{-1}{q}\right)^{\frac{p-1}{2}v_q(n)v_p(m)} \\
&= \left(\frac{m}{n}\right)\prod_{p\geq 3}\left(\frac{-1}{n}\right)^{\frac{p-1}{2}v_p(m)} \\
&= \left(\frac{m}{n}\right)\prod_{p\geq 3}\left(\frac{-1}{p}\right)^{\frac{n-1}{2}v_p(m)} \\
&= \left(\frac{m}{n}\right)\left(\frac{-1}{m}\right)^{\frac{n-1}{2}} \\
&= \left(\frac{m}{n}\right)(-1)^{\frac{(m-1)(n-1)}{4}}.
\end{aligned}$$

□

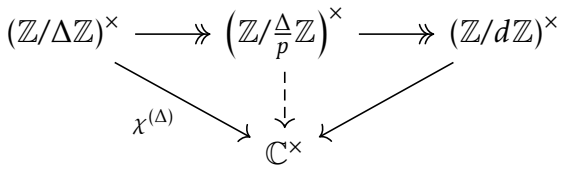
On peut reformuler cette égalité en disant que $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ sauf dans le cas où $m \equiv n \equiv 3\ [4]$, où ils sont opposés.
La loi de réciprocité quadratique 12.40 ainsi que ses deux lois complémentaires 12.37 et la périodicité du symbole de Jacobi en la première variable modulo la seconde permet de calculer efficacement n'importe quel symbole de Jacobi. Par exemple :

$$\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{-2}{7}\right) = -\left(\frac{-1}{7}\right)\left(\frac{2}{7}\right) = -(-1)^{\frac{7-1}{2}}(-1)^{\frac{7^2-1}{8}} = 1$$

donc 7 est un carré modulo 19 mais 19 n'est pas un carré modulo 7 (car 7 et 19 sont premiers).

Proposition 12.41. *Le caractère $\chi^{(\Delta)}$ est un caractère primitif modulo Δ.*

Démonstration. Supposons qu'il ne soit pas primitif : il existe alors d un diviseur strict de Δ tel que $\chi^{(\Delta)}$ se factorise par $(\mathbb{Z}/d\mathbb{Z})^\times$. Puisque $d \neq \Delta$, il existe p un nombre premier divisant Δ tel que $d \mid \frac{\Delta}{p}$, et ainsi $\chi^{(\Delta)}$ se factorise aussi par $\left(\mathbb{Z}/\frac{\Delta}{p}\mathbb{Z}\right)^\times$:



et donc pour tout $x \in (\mathbb{Z}/\Delta\mathbb{Z})^\times$ tel que $x \equiv 1\ [\Delta/p]$, on a $\chi(x) = 1$.
Ainsi, pour montrer que $\chi^{(\Delta)}$ est primitif, il suffit de montrer que pour tout premier $p \mid \Delta$ il existe $x \in (\mathbb{Z}/\Delta\mathbb{Z})^\times$ tel que $x \equiv 1\ [\Delta/p]$ et $\chi(x) = -1$.
On écrit $\Delta = 2^k s$ avec s impair et $d = (-1)^t |d|$.
Si $p \mid \Delta$ est impair, il existe $x_0 \in \mathbb{F}_p$ qui n'est pas un carré modulo p et donc, par le théorème des restes chinois, il existe $n \geq 1$ tel que :

$$n \equiv x_0\ [p],\ n \equiv 1\ [8], n \equiv 1\ [q]$$

pour tout premier impair $q \neq p$ divisant Δ. Par construction, n est impair et :

$$\left(\frac{n}{p}\right) = -1$$

et n est premier à Δ. On a donc, par imparité de n et par le lemme 12.38 :

$$\chi(n) = \prod_{q \geq 3} \left(\frac{d}{q}\right)^{v_q(n)} = \left(\frac{d}{n}\right) = \left(\frac{-1}{n}\right)^t \left(\frac{2^k}{n}\right)\left(\frac{s}{n}\right) = (-1)^{\frac{n-1}{2}t}(-1)^{\frac{n^2-1}{8}k}(-1)^{\frac{(n-1)(s-1)}{4}}\left(\frac{n}{s}\right) = \left(\frac{n}{s}\right)$$

en utilisant la loi de réciprocité quadratique et ses lois complémentaires et la congruence $n \equiv 1\ [8]$. On a alors, puisque s est sans facteur carré (car $s \mid d$) :

$$\chi(n) = \left(\frac{n}{s}\right) = \left(\frac{n}{p}\right) \prod_{q \mid s, q \neq p} \left(\frac{n}{q}\right) = -1$$

par construction de n. De plus, $n \equiv 1\ [\Delta/p]$ par le théorème chinois et par construction (encore une fois car s est sans facteur carré et que la valuation 2-adique de Δ vaut au plus 3).
Il reste à traiter le cas de $p = 2$. Dans ce cas Δ est pair, et donc $d \not\equiv 1\ [4]$, sinon on aurait $\Delta = |d|$.
Si $d \equiv 2\ [4]$, on a $\Delta = 4|d|$, donc $s = \frac{\Delta}{8}$, et $k = 3$. On trouve alors par le théorème des restes chinois un $n \geq 1$ tel que :

$$n \equiv 1\ [s],\ n \equiv 5\ [8]$$

de sorte que n est impair, premier à Δ et :

$$\chi(n) = \left(\frac{d}{n}\right) = (-1)^{\frac{n-1}{2}t}(-1)^{\frac{n^2-1}{8}k}(-1)^{\frac{(n-1)(s-1)}{4}}\left(\frac{n}{s}\right)$$

or $(-1)^{\frac{n-1}{2}t} = 1$, $(-1)^{\frac{n^2-1}{8}k} = (-1)^k = -1$ et $(-1)^{\frac{(n-1)(s-1)}{4}} = (-1)^{s-1} = 1$ donc :

$$\chi(n) = -\left(\frac{n}{s}\right) = -1$$

en factorisant s en produit de nombres premiers sans répétition, tous impairs, modulo lesquels n est congru à 1. On a de plus $n \equiv 1\ [\Delta/2]$ comme souhaité : en effet $n \equiv 1\ [4s]$, i.e. $n \equiv 1\ [\Delta/2]$.

Enfin, si $d \equiv 3\ [4]$, on a cette fois-ci $s = \frac{\Delta}{4} = |d|$ et $k = 2$. On choisit alors $n \geq 1$ tel que $n \equiv 1\ [s]$ et $n \equiv 3\ [4]$ de sorte que $n \equiv 1\ [2s]$ donc $n \equiv 1\ [\Delta/2]$. On a alors toujours, par imparité de n :

$$\chi(n) = (-1)^{\frac{n-1}{2}t}(-1)^{\frac{n^2-1}{8}k}(-1)^{\frac{(n-1)(s-1)}{4}}\left(\frac{n}{s}\right)$$

et puisque $k = 2$, $(-1)^{\frac{n^2-1}{8}k} = 1$ et en écrivant $n = 4a + 3$:

$$\frac{(n-1)(s-1)}{4} = (2a+1)\frac{s-1}{2} \equiv \frac{s-1}{2}\ [2]$$

qui vaut -1 dans le cas $d > 0$ et 1 dans le cas $d < 0$. Comme précedemment $\left(\frac{n}{s}\right) = 1$ et $(-1)^{\frac{n-1}{2}t} = (-1)^t$ vaut 1 dans le cas $d > 0$ et -1 dans le cas $d < 0$. Au total :

$$\chi(n) = -1$$

ce qui conclut. □

On a alors tous les ingrédients pour donner une formule pour le nombre de classes d'un corps quadratique.

Théorème 12.42. *Soit $d \neq 0, 1$ sans facteur carré, $K = \mathbb{Q}(\sqrt{d})$ et Δ la valeur absolue du discriminant de K. Si $d > 0$, on a, en notant α une unité fondamentale :*

$$|\mathrm{Cl}(K)| = \frac{1}{|\log \alpha|}\left|\sum_{1 \leq k < \Delta/2} \chi(k) \log \sin\left(\frac{k\pi}{\Delta}\right)\right|$$

et si $d < 0$, avec $d \neq -1$ et $d \neq -3$:

$$|\mathrm{Cl}(K)| = \frac{1}{2 - \chi(2)}\left|\sum_{1 \leq k < \Delta/2} \chi(k)\right|.$$

Enfin, pour $d = -1$ ou -3 le nombre de classes est 1.

Démonstration. Il s'agit simplement de remettre les morceaux ensemble. D'après 12.33, on a :

$$\mathrm{Res}(\zeta_K, 1) = L(1, \chi)\prod_{p|\Delta}(1 - p^{-s})(1 - p^{-s})^{-1} = L(1, \chi)$$

car les premiers divisant Δ sont ramifiés par le théorème de Dedekind 5.42 et donc vérifient $f(p) = r(p) = 1$. De plus ce résidu est un réel strictement positif donc on peut remplacer $L(1, \chi)$ par sa valeur absolue, que l'on sait calculer car χ est primitif.
Le nombre $-1 \in (\mathbb{Z}/\Delta\mathbb{Z})^\times$ correspond à la conjugaison complexe sur $\mathbb{Q}(\mathbb{U}_m)$ et donc $\pi(-1)$ est la conjugaison complexe sur K, qui est triviale si et seulement si $d > 0$. Ainsi, si $d > 0$ on a $\chi^{(\Delta)}(-1) = 1$ donc χ est pair et sinon χ est impair.
Il reste à utiliser la formule 12.31 en utilisant le fait que χ est primitif, ainsi que la formule analytique du nombre de classes pour conclure. On notera que si $d < 0$ et $d \neq -1, -3$, les seules racines de l'unité présentes dans K sont -1 et 1 car si $\mathbb{Q}(\mathbb{U}_n) \subseteq K$, alors $\varphi(n) \leq 2$ ce qui impose $n = 1, 2, 3, 4$ ou $n = 6$, et si $n = 4$ cela impose $d = -1$ tandis que si $n = 6$ ou $n = 3$ on a $d = -3$ (on utilise le fait que les $\mathbb{Q}(\sqrt{d})$ sont tous distincts, pour d sans facteur carré différent de 0 et de 1, voir proposition 6.5).
On laisse au lecteur le soin d'appliquer les mêmes formules pour traiter les cas $d = -1$ et $d = -3$. □

12.9 Densité de Dirichlet

Le but de cette partie est de définir une mesure de la taille d'un ensemble de premiers $X \subseteq \mathbb{P}_K$ d'un corps de nombres K. Dans certains cas, on pourra l'interpréter comme l'ordre fractionnaire d'une certaine fonction ζ associée à X en $s = 1$. On commence par définir la notion d'ordre fractionnaire d'une fonction holomorphe en un point de l'adhérence de son domaine de définition.

12.9.1 Ordre fractionnaire d'une fonction holomorphe

On rappelle que si f est une fonction méromorphe sur un ouvert de $\mathbb{C}$ et si a est un point de cet ouvert au voisinage duquel f n'est pas nulle, on peut écrire $f(z) \sim c(z-a)^n$ quand $z \longrightarrow a$ avec $c \in \mathbb{C}^\times$ et $n \in \mathbb{Z}$ un certain entier relatif, appelé l'ordre (d'annulation) de f en a. Le but de ce paragraphe est de généraliser cette notion à des fonctions qui ne sont pas méromorphes au voisinage de a comme la fonction $(z-a)^{1/2}$ par exemple. On parlera d'*ordre usuel* pour évoquer la notion d'ordre que l'on vient de rappeler.

Définition 12.43. *Soit U un ouvert de $\mathbb{C}$ et $a \in \overline{U}$ un point adhérent à U. Soit f une fonction méromorphe sur U.*
Si f est nulle au voisinage de a, on dit que f est d'ordre ∞ en a. Sinon, on dit que f admet un ordre fractionnaire en a si la limite suivante existe dans $\mathbb{R}$:

$$\lim_{z \longrightarrow a, z \in U} \frac{\log|f(z)|}{\log|z-a|}.$$

Dans ce cas on définit l'ordre fractionnaire de f en a comme la valeur de cette limite, et on le note $\mathrm{ord}_a(f)$.

L'ordre fractionnaire se comporte bien avec les produits et quotients de fonctions méromorphes : on laisse la preuve de la proposition suivante en exercice.

Proposition 12.44. *On se place dans le même contexte que la définition 12.43. L'ensemble des fonctions méromorphes sur U nulles sur aucun ouvert non trivial et qui admettent un ordre fractionnaire en a est un groupe pour la multiplication et* ord_a *définit un morphisme de ce groupe vers le groupe additif $\mathbb{R}$.*
De plus, si f est une fonction méromorphe sur U nulle sur aucun ouvert non trivial et s'il existe $n \in \mathbb{Z} \setminus \{0\}$ tel que f^n admet un ordre fractionnaire en a, alors f admet un ordre fractionnaire en a et :

$$\mathrm{ord}_a(f) = \frac{1}{n}\mathrm{ord}_a(f^n).$$

Voyons à présent un exemple fondamental d'ordre fractionnaire : on considère la fonction holomorphe $f(z) = (z-a)^\alpha = \exp(\alpha \log(z-a))$ avec $\alpha \in \mathbb{C}$. On peut définir cette fonction sur l'ouvert $U = \mathbb{C} \setminus (a + \mathbb{R}_-)$ en choisissant la détermination usuelle du logarithme complexe.

Lemme 12.45. *La fonction holomorphe $f(z) = (z-a)^\alpha$ admet un ordre fractionnaire en a et on a :*

$$\mathrm{ord}_a(f) = \mathrm{Re}(\alpha).$$

Démonstration. On note $\alpha = x + iy$ avec $x, y \in \mathbb{R}$ et pour $z \in U$:

$$\log(z-a) = \log|z-a| + i\theta(z-a)$$

avec $\theta(z-a) \in]-\pi, \pi[$. On a donc :

$$\log|f(z)| = \log\left|\exp(x\log|z-a| + i(\dots) - y\theta(z-a))\right| = \log\exp(x\log|z-a| - y\theta(z-a)) = x\log(z-a) + O(1)$$

quand $z \longrightarrow a$. Ainsi :

$$\frac{\log|f(z)|}{\log|z-a|} = x + o(1)$$

comme souhaité. □

Dans le cas où le point a est "entouré" par l'ouvert U, l'ordre fractionnaire, s'il existe, est toujours entier et f est alors méromorphe sur $U \cup \{a\}$.

Théorème 12.46. *Soit U un ouvert de $\mathbb{C}$, $a \in \overline{U}$ tel que $U \cup \{a\}$ est un ouvert et soit f une fonction méromorphe sur U non nulle au voisinage de a et qui admet un ordre fractionnaire α en a. Alors $\alpha \in \mathbb{Z}$, f est méromorphe sur $U \cup \{a\}$ et son ordre (au sens usuel) en a est exactement α.*
Réciproquement, si g est une fonction méromorphe sur $U \cup \{a\}$ non nulle au voisinage de a, alors elle admet un ordre fractionnaire entier en a et cet ordre fractionnaire est l'ordre au sens usuel de g en a.

Démonstration. Puisque l'ordre fractionnaire et l'ordre usuel se comportent bien vis à vis du produit, quitte à multiplier par $(z-a)^n$ pour un certain $n \in \mathbb{Z}$, on peut remplacer α par $\alpha + n$ et ainsi supposer que :

$$0 \leq \alpha < 1.$$

On va alors montrer que f se prolonge en une fonction holomorphe sur l'ouvert $U \cup \{a\}$. Fixons $\varepsilon > 0$ assez petit. Pour z assez proche de a dans U on a, par hypothèse d'existence d'un ordre fractionnaire :

$$\left|\alpha - \frac{\log|f(z)|}{\log|z-a|}\right| \leq \varepsilon.$$

On a donc :

$$|\log|f(z)|| \leq (\alpha+\varepsilon)\log\frac{1}{|z-a|}$$

car pour z assez proche de a, $|\log|z-a|| = \log\frac{1}{|z-a|}$. En particulier $\log|f(z)| \leq (\alpha+\varepsilon)\log\frac{1}{|z-a|}$ et donc :

$$|f(z)| \leq |z-a|^{-\alpha-\varepsilon}$$

et ainsi :

$$|(z-a)f(z)| \leq |z-a|^{1-\alpha-\varepsilon} = o(1)$$

en choisissant ε assez petit pour que $1-\alpha-\varepsilon > 0$, ce qui est possible car $\alpha < 1$. Par le théorème de prolongement de Riemann, a est donc une singularité effaçable de f et f se prolonge en une fonction holomorphe sur l'ouvert $U \cup \{a\}$. Ceci entraîne que $\alpha = 0$

d'après la réciproque que l'on va montrer à présent.
Soit g méromorphe sur $U \cup \{a\}$ non nulle au voisinage de a, on note $k \in \mathbb{Z}$ son ordre usuel en a. On peut écrire sur un voisinage de a :

$$g(z) = (z-a)^k h(z)$$

avec h une fonction holomorphe sur un voisinage de a telle que $h(a) \neq 0$. D'après le lemme 12.45, la fonction $(z-a)^k$ est d'ordre fractionnaire k et par multiplicativité il suffit donc de montrer que h est d'ordre fractionnaire 0. Or on a :

$$\frac{\log|h(z)|}{\log|z-a|} \sim \frac{\log|h(a)|}{\log|z-a|} \longrightarrow 0.$$

□

Le théorème 12.46 permet par exemple de montrer qu'une fonction ne peut pas se prolonger sur un ouvert qui "entoure" la singularité dans le cas où la fonction admet un ordre fractionnaire non entier.

Remarque 12.47. Sans l'hypothèse que $U \cup \{a\}$ est ouvert et même si l'ordre fractionnaire est entier, f ne se prolonge pas nécessairement en une fonction méromorphe sur un voisinage de a. Par exemple, on laisse en exercice le fait que la fonction $\log z$ définie sur l'ouvert $\mathbb{C} \setminus \mathbb{R}_-$ a un ordre fractionnaire nul en 0 (alors qu'elle ne se prolonge pas en une fonction méromorphe d'ordre 0 en 0, i.e. une fonction holomorphe qui ne s'annule pas en 0).

12.9.2 Fonction ζ associée à un ensemble de premiers

Soit K un corps de nombres et X une partie de $\mathbb{P}_K$. On note $\langle X \rangle$ l'ensemble des idéaux non nuls de $\mathcal{O}_K$ dont les divieurs premiers sont dans l'ensemble X. On considère alors la fonction ζ associée à X définie par :

$$\zeta_{K,X}(s) = \sum_{I \in \langle X \rangle} \frac{1}{\|I\|^s}.$$

Puisqu'il y a moins de termes que dans la définition de ζ_K, cette somme converge normalement sur tout compact du demi-plan $\mathrm{Re}(s) > 1$ et y définit une fonction holomorphe, et on a, avec le théorème 12.18 pour $\mathrm{Re}(s) > 1$:

$$\zeta_{K,X}(s) = \prod_{\mathfrak{p} \in X} \frac{1}{1 - \|p\|^{-s}}.$$

Pour les mêmes raisons que précedemment on peut aussi définir la fonction holomorphe suivante sur le demi-plan $\mathrm{Re}(s) > 1$:

$$S_{K,X}(s) = \sum_{p \in X} \frac{1}{\|p\|^s}.$$

On note $S_K = S_{K,\mathbb{P}_K}$.

Proposition 12.48. *Pour $s > 1$ réel, $\zeta_{K,X}(s) > 0$ et on peut donc en prendre le logarithme, et on a :*

$$\log \zeta_{K,X}(s) = S_{K,X}(s) + O(1)$$

lorsque $s \longrightarrow 1$. En particulier on dispose des équivalents suivants lorsque $s > 1$ tend vers 1 :

$$S_K(s) \sim \log \zeta_K(s) \sim \log\left(\frac{1}{s-1}\right).$$

Démonstration. Soit s un réel strictement plus grand que 1. On a :

$$\zeta_{K,X}(s) \geq \zeta_{K,\emptyset}(s) = 1 > 0.$$

La formule d'Euler donne, puisque le produit converge absolument :

$$\log \zeta_{K,X}(s) = -\sum_{\mathfrak{p}\in X} \log\left(1 - \|\mathfrak{p}\|^{-s}\right) = \sum_{\mathfrak{p}\in X}\sum_{n\geq 1} \frac{\|\mathfrak{p}\|^{-sn}}{n} = S_{K,X}(s) + \sum_{n\geq 2}\frac{1}{n}\sum_{\mathfrak{p}\in X}\|\mathfrak{p}\|^{-sn}$$

car la norme d'un premier $\mathfrak{p}$ vaut toujours au moins 2 et que tous les termes présents sont positifs. On montre à présent que ce deuxième terme est borné pour $s \geq 1$:

$$\frac{1}{n}\sum_{\mathfrak{p}\in X}\|\mathfrak{p}\|^{-sn} \leq \frac{1}{2^n n}\sum_{\mathfrak{p}\in X}\left(\frac{\|\mathfrak{p}\|}{2}\right)^{-n} \leq \frac{1}{2^n n}\sum_{\mathfrak{p}\in X}\left(\frac{\|\mathfrak{p}\|}{2}\right)^{-2} \leq \frac{4}{2^n n}\zeta_K(2)$$

donc $\sum_{n\geq 2}\frac{1}{n}\sum_{\mathfrak{p}\in X}\|\mathfrak{p}\|^{-sn} \leq 4\zeta_K(2)\sum_{n\geq 2}\frac{1}{2^n n}$, qui est une constante finie. On a donc :

$$S_{K,X}(s) = \log \zeta_{K,X}(s) + O(1)$$

quand $s > 1$ tend vers 1. Dans le cas particulier où $X = \mathbb{P}_K$ on a de plus le théorème 12.20 qui assure que pour $s > 1$ qui tend vers 1 :

$$\log \zeta_K(s) = \log\left(\frac{\mathrm{Res}(\zeta_K, 1)}{s-1} + O(1)\right) \sim \log\left(\frac{1}{s-1}\right)$$

car le résidu est non nul, et le $O(1)$ est négligeable devant $\log\left(\frac{1}{s-1}\right)$, donc on a les équivalents suivants :

$$S_K(s) \sim \log \zeta_K(s) \sim \log\left(\frac{1}{s-1}\right).$$

□

12.9.3 Densité de Dirichlet d'un ensemble de premiers

Soit K un corps de nombres et $X \subseteq \mathbb{P}_K$ un ensemble de premiers.

Définition 12.49. *On dit que X admet une densité de Dirichlet si la limite suivante existe :*

$$\lim_{s\longrightarrow 1, s>1} \frac{S_{K,X}(s)}{S_K(s)}$$

et on note $\delta(X)$ cette limite dans ce cas : c'est la densité de Dirichlet de X. Au vu de la proposition 12.48, on peut aussi la définir comme :

$$\lim_{s\longrightarrow 1, s>1} \frac{S_{K,X}(s)}{\log\left(\frac{1}{s-1}\right)}.$$

Proposition 12.50. *Soit $X \subseteq \mathbb{P}_K$ admettant une densité de Dirichlet. On a :*

$$\delta(X) \in [0,1].$$

Soient $A, B, C \subseteq \mathbb{P}_K$ telles que $C = A \sqcup B$. Si deux des trois parties A, B et C ont une densité de Dirichlet, alors la troisième aussi et on a :

$$\delta(C) = \delta(A) + \delta(B).$$

On a $\delta(\emptyset) = 0$, $\delta(\mathbb{P}_K) = 1$ et si X a une densité de Dirichlet, $\mathbb{P}_K \setminus X$ aussi et $\delta(\mathbb{P}_K \setminus X) = 1 - \delta(X)$.
Enfin, si $A \subseteq B \subseteq \mathbb{P}_K$ et $\delta(B) = 0$, alors $\delta(A) = 0$.

Démonstration. Soit $s > 1$. On a :

$$0 \leq S_{K,X}(s) \leq S_K(s)$$

d'où la première affirmation. Ensuite on a :

$$S_C(s) = S_A(s) + S_B(s)$$

d'où la seconde affirmation.
Si $A \subseteq B \subseteq \mathbb{P}_K$ et $\delta(B) = 0$, alors on a :

$$0 \leq S_A(s) \leq S_B(s)$$

pour $s > 1$ et en divisant par $\log(1/(s-1))$ et en passant à la limite on obtient $\delta(A) = 0$.
Le reste est clair. □

Le théorème suivant relie la densité de Dirichlet à l'éventuel ordre fractionnaire de $\zeta_{K,X}$ en $s = 1$.

Théorème 12.51. *Soit $X \subseteq \mathbb{P}_K$. Si la fonction $\zeta_{K,X}$, définie sur l'ouvert $\{\mathrm{Re}(s) > 1\}$ admet un ordre fractionnaire en $s = 1$, alors X admet une densité de Dirichlet et on a :*

$$\delta(X) = -\mathrm{ord}_1(\zeta_{K,X}).$$

Démonstration. Notons α l'ordre fractionnaire de $\zeta_{K,X}$ en $s = 1$, de sorte que :

$$\frac{\log\left|\zeta_{K,X}(s)\right|}{\log|s-1|} \longrightarrow \alpha$$

lorsque $s \longrightarrow 1$ avec $\mathrm{Re}(s) > 1$. En particulier, puisque $\zeta_{K,X}(s) > 0$ pour $s > 1$, on a :

$$\frac{\log \zeta_{K,X}(s)}{\log(s-1)} \longrightarrow \alpha$$

quand $s \longrightarrow 1$ avec $s > 1$ réel. Or, d'après la proposition 12.48, on a :

$$\frac{S_{K,X}(s)}{\log\left(\frac{1}{s-1}\right)} = -\frac{\log \zeta_{K,X}(s) + O(1)}{\log(s-1)} \longrightarrow -\alpha$$

quand $s \longrightarrow 1$, donc X a pour densité de Dirichlet $-\alpha$. □

Remarque 12.52. Le théorème 12.51 implique en particulier que si $\zeta_{K,X}$ se prolonge en une fonction holomorphe en $s = 1$, alors son ordre fractionnaire est nul (il est positif mais on sait que $\zeta_{K,X}(s) \geq 1$ pour $s > 1$ donc par continuité $\zeta_{K,X}(1) \neq 0$) et donc X est de densité de Dirichlet nulle.
En particulier tout ensemble fini est de densité de Dirichlet nulle.

On obtient aussi le critère suivant.

Proposition 12.53. *Soit X un ensemble de premiers de K dont les indices d'inertie $f(\mathfrak{p} \mid p)$ sont tous au moins égaux à 2. Alors X est de densité de Dirichlet nulle.*

Démonstration. D'après la remarque 12.52 ci-dessus, il suffit de montrer que $\zeta_{K,X}$ se prolonge en une fonction holomorphe en $s = 1$. Or, pour $s > \frac{1}{2}$ réel, on a :

$$\prod_{\mathfrak{p}\in X} \frac{1}{1-\|\mathfrak{p}\|^{-s}} = \prod_{p\in\mathbb{P}_{\mathbb{Q}}} \prod_{\mathfrak{p}\in X, p\in\mathfrak{p}} \frac{1}{1-p^{-sf(\mathfrak{p}|p)}} \leq \prod_{p\in\mathbb{P}_{\mathbb{Q}}} \prod_{\mathfrak{p}\in X, p\in\mathfrak{p}} \frac{1}{1-p^{-2s}} \leq \prod_{p\in\mathbb{P}_{\mathbb{Q}}} \left(\frac{1}{1-p^{-2s}}\right)^{[K:\mathbb{Q}]} \leq \zeta(2s)^{[K:\mathbb{Q}]}$$

en utilisant le théorème du produit par paquets 12.10, puisqu'ici $\frac{1}{1-\|\mathfrak{p}\|^{-s}} \geq 1$. On a aussi utilisé le fait que, par hypothèse, on ait $f(\mathfrak{p} \mid p) \geq 2$ et qu'il y a au plus $[K : \mathbb{Q}]$ premiers au dessus d'un nombre premier p.
Ainsi, d'après le théorème 12.18 dans le cas positif :

$$\sum_{I\in\langle X\rangle} \frac{1}{\|I\|^s} \leq \zeta(2s)^{[K:\mathbb{Q}]}$$

pour tout $s > \frac{1}{2}$ réel. Or $\zeta(2s) < \infty$ donc cette somme converge absolument pour $s > \frac{1}{2}$ et par la proposition 12.13, la fonction $\zeta_{K,X}$ se prolonge holomorphiquement sur le demi-plan ouvert $\mathrm{Re}(s) > \frac{1}{2}$. □

Comme en théorie de la mesure, si deux ensembles X et Y de premiers diffèrent (au sens de la différence symétrique $X \cup Y \setminus X \cap Y$) d'un ensemble de densité nulle, et si X a une densité, alors Y aussi et $\delta(X) = \delta(Y)$ (cela découle facilement de 12.50). Ainsi lors du calcul de la densité d'un ensemble on peut toujours supprimer un nombre fini de premiers ou supprimer des premiers dont les indices d'inertie sont au moins 2.
Avec ceci, on peut démontrer le théorème suivant qui donne la densité de Dirichlet de l'ensemble des premiers totalement décomposés. On rappelle que dans une extension de Dedekind B/A, un premier $\mathfrak{p}$ de A est dit *totalement décomposé* si tous les indices $e(\mathfrak{q} \mid \mathfrak{p})$ et $f(\mathfrak{q} \mid \mathfrak{p})$ valent 1, autrement dit s'il y a exactement $[L : K]$ premiers au dessus de $\mathfrak{p}$.

Théorème 12.54. *Soit L/K une extension de corps de nombres et soit M la clôture normale de L/K, de sorte que M/K est galoisienne, $M \supseteq L$ et M est minimale pour ces propriétés. On considère X l'ensemble des premiers de K totalement décomposés dans L. On a alors l'égalité suivante :*

$$\delta(X) = \frac{1}{[M : K]}.$$

Démonstration. On commence par le cas où L/K est galoisienne, c'est à dire que $M = L$. On note $Y \subseteq \mathbb{P}_L$ l'ensemble des premiers de L au dessus des éléments de X. On calcule, pour $s > 1$ réel, via le théorème de produit par paquets 12.10 :

$$\zeta_{L,Y}(s) = \prod_{\mathfrak{p}\in X}\prod_{\mathfrak{q}\supseteq\mathfrak{p}} \frac{1}{1-\|\mathfrak{q}\|^{-s}} = \prod_{\mathfrak{p}\in X}\prod_{\mathfrak{q}\supseteq\mathfrak{p}} \frac{1}{1-\|\mathfrak{p}\|^{-s}} = \prod_{\mathfrak{p}\in X}\left(\frac{1}{1-\|\mathfrak{p}\|^{-s}}\right)^{[L:K]} = \zeta_{K,X}(s)^{[L:K]}$$

car pour $\mathfrak{q} \in Y$ au dessus de $\mathfrak{p} \in X$, on a $f(\mathfrak{q} \mid \mathfrak{p}) = 1$. On peut ensuite écrire :

$$\zeta_L(s) = \zeta_{L,Y}(s)\zeta_{L,\mathbb{P}_L\setminus Y}(s).$$

Or si $\mathfrak{q} \in \mathbb{P}_L \setminus Y$, en notant $\mathfrak{p} = \mathfrak{q} \cap K$ et p le nombre premier en dessous de $\mathfrak{p}$, on a nécessairement $e(\mathfrak{q} \mid \mathfrak{p}) \geq 2$ ou $f(\mathfrak{q} \mid \mathfrak{p}) \geq 2$ car L/K est galoisienne et donc ces indices ne dépendent que de $\mathfrak{p}$. On peut donc écrire :

$$\mathbb{P}_L \setminus Y = F \sqcup Z$$

avec F un ensemble fini de premiers (ceux pour lesquels $e \geq 2$ et donc qui divisent l'idéal différent $\mathrm{Diff}_{\mathcal{O}_L/\mathcal{O}_K}$) et Z un ensemble de premiers dont l'indice d'inertie au dessus de K et donc au dessus de $\mathbb{Q}$ est au moins égal à 2. On peut donc écrire :

$$\zeta_L(s) = \zeta_{L,Y}(s)\zeta_{L,F}(s)\zeta_{L,Z}(s)$$

et $\zeta_{L,F}$ ainsi que $\zeta_{L,Z}$ sont holomorphes en $s = 1$ d'après la remarque 12.52 et La preuve de la proposition 12.53. Leur valeur en $s = 1$ est non nulle car c'est un réel au moins égal à 1, et donc :

$$\mathrm{ord}_1(\zeta_{L,Y}) = \mathrm{ord}_1(\zeta_L) - \mathrm{ord}_1(\zeta_{L,F}) - \mathrm{ord}_1(\zeta_{L,Z}) = \mathrm{ord}_1(\zeta_L) = -1$$

de sorte que :

$$\mathrm{ord}_1(\zeta_{K,X}) = \frac{1}{[L:K]}\mathrm{ord}_1(\zeta_{L,Y}) = -\frac{1}{[L:K]}$$

d'après la proposition 12.44. Ainsi par le théorème 12.51 on a :

$$\delta(X) = \frac{1}{[L:K]}.$$

Revenons au cas général. Un premier $\mathfrak{p}$ de K est totalement décomposé dans L si et seulement si il est totalement décomposé dans M d'après le théorème 7.20. Le cas précédent donne donc :

$$\delta(X) = \frac{1}{[M:K]}.$$

□

Puisque tout ensemble fini de premiers a une densité de Dirichlet nulle, on en déduit le fait suivant.

Corollaire 12.55. *Soit L/K une extension de corps de nombres. Une infinité de premiers de K sont totalement décomposés dans L.*

En appliquant le théorème 5.48, on obtient un théorème de densité des premiers pour lesquels un certain polynôme est scindé à racines simples.

Théorème 12.56. *Soit K un corps de nombres et $f \in \mathcal{O}_K[X]$ irréductible unitaire. Notons X l'ensemble des premiers $\mathfrak{p}$ de K tels que la réduction de f modulo $\mathfrak{p}$ soit scindée, ou bien scindée à racines simples (ça ne change pas le résultat). Alors on a :*

$$\delta(X) = \frac{1}{[L:K]}$$

avec L l'extension de K engendrée par les racines de f.

Démonstration. Fixons $\alpha \in L$ une racine de f et notons $M = K[\alpha]$. D'après le théorème 5.48, pour tout $\mathfrak{p}$ sauf un nombre fini (par exemple pour tout $\mathfrak{p}$ ne divisant pas $(\mathcal{O}_M : \mathcal{O}_K[\alpha])$), f est scindé à racines simples modulo $\mathfrak{p}$ si et seulement si $\mathfrak{p}$ est totalement décomposé dans M. Le résultat découle alors directement du théorème 12.54 car un nombre fini de premiers ne change pas la densité de Dirichlet.
Le cas des premiers pour lesquels f est seulement scindé en découle car pour tous les premiers $\mathfrak{p}$ sauf un nombre fini, f est séparable modulo $\mathfrak{p}$. □

Théorème 12.57. *(Répartition des Frobenius dans le groupe de Galois) Soit L/K une extension galoisienne de corps de nombres de groupe de Galois G et soit H un sous-groupe distingué de G. On considère $X_H \subseteq \mathbb{P}_K$ l'ensemble des premiers $\mathfrak{p}$ de K non ramifiés dans L tels que pour un $\mathfrak{q}$ quelconque au dessus de $\mathfrak{p}$, le Frobenius $\left(\frac{L/K}{\mathfrak{q}}\right)$ soit dans H (voir 7.11).*
On a alors :

$$\delta(X_H) = \frac{1}{[G:H]}.$$

Remarque 12.58. Puisque ces Frobenius forment une classe de conjugaison de G (voir 7.13) et que H est distingué, on peut aussi définir X_H comme l'ensemble des $\mathfrak{p}$ non ramifiés tels que pour tout $\mathfrak{q}$ au dessus de $\mathfrak{p}$ on ait $\left(\frac{L/K}{\mathfrak{q}}\right) \in H$.
Ce résultat peut être amélioré en remplaçant H par une classe de conjugaison quelconque, on obtient alors le théorème de densité de Cebotarev.

Démonstration. Soit $\mathfrak{p}$ un premier de K non ramifié dans L et soit $\mathfrak{q}$ au dessus de $\mathfrak{p}$. Rappelons que dans ce cas, on a un isomorphisme $D(\mathfrak{q} \mid \mathfrak{p}) \cong \overline{G}(\mathfrak{q} \mid \mathfrak{p})$ dans les notations de 7.9, et que par cet isomorphisme, le Frobenius $\left(\frac{L/K}{\mathfrak{q}}\right) \in D(\mathfrak{q} \mid \mathfrak{p})$ correspond à $x \mapsto x^{|\mathcal{O}_K/\mathfrak{p}|}$, qui engendre le groupe $\overline{G}(\mathfrak{q} \mid \mathfrak{p})$, de sorte que le Frobenius $\left(\frac{L/K}{\mathfrak{q}}\right)$ engendre $D(\mathfrak{q} \mid \mathfrak{p})$.
Ainsi $\left(\frac{L/K}{\mathfrak{q}}\right) \in H$ si et seulement si le sous-groupe $D(\mathfrak{q} \mid \mathfrak{p})$ de G engendré par $\left(\frac{L/K}{\mathfrak{q}}\right)$ est contenu dans H, i.e. $L^H \subseteq L^{D(\mathfrak{q}|\mathfrak{p})}$, ce qui équivaut, d'après 7.18, à ce que $\mathfrak{p}$ soit totalement décomposé dans L^H. Comme L^H/K est galoisienne (car H est distingué dans G), on obtient une densité de :

$$\delta(X_H) = \frac{1}{[L^H:K]} = \frac{1}{[G:H]}.$$

□

Ce théorème a un cas particulier très concret quand $L = \mathbb{Q}(\mathbb{U}_m)$ et $K = \mathbb{Q}$.

Corollaire 12.59. *Soit $m \geq 1$ un entier et H un sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^\times$. Alors la densité de Dirichlet de l'ensemble des nombres premiers p premiers avec m dont l'image dans $\mathbb{Z}/m\mathbb{Z}$ est dans H est $\frac{|H|}{\varphi(m)}$.*

Remarque 12.60. Ce théorème se rapproche du théorème de densité de Dirichlet qui affirme que l'on peut remplacer H par un singleton $\{a\}$ de sorte que l'ensemble des nombres premiers p congrus à a modulo m a une densité de Dirichlet $1/\varphi(m)$ et en particulier est infini (c'est le théorème de la progression arithmétique de Dirichlet).

Démonstration. C'est une simple reformulation avec $L = \mathbb{Q}(\mathbb{U}_m)$ et $K = \mathbb{Q}$. Ici les premiers ramifiés sont exactement les diviseurs de m d'après 8.12, et le Frobenius modulo p (qui ne dépend pas du $\mathfrak{p}$ choisi au dessus de p car l'extension est abélienne) agit comme $x \mapsto x^p$ sur les racines de l'unité donc correspond à p dans le groupe de Galois $(\mathbb{Z}/m\mathbb{Z})^\times$. □

Quatrième partie

Théorie algébrique des nombres dans les corps locaux

Chapitre 13

Corps valués

13.1 Généralités

Définition 13.1. *Soit K un corps. Une valeur absolue sur K est une application $|\bullet| : K \longrightarrow \mathbb{R}_+$ qui vérifie les propriétés suivantes :*

— *Pour tous $x, y \in K$ on a $\big|xy\big| = |x|\big|y\big|$.*

— *Pour tout $x \in K$ on a l'équivalence suivante :*

$$|x| = 0 \iff x = 0$$

— *Il existe une constante $C > 0$ telle que pour tout $x \in K$ vérifiant $|x| \leq 1$ on a :*

$$|1 + x| \leq C$$

La valeur absolue triviale est l'application $K \longrightarrow \mathbb{R}_+$ qui envoie 0 sur 0 et tout autre élément de K sur 1.
Une valeur absolue $|\bullet|$ est dite triangulaire lorsqu'elle vérifie l'inégalité triangulaire, c'est à dire lorsque pour tous $x, y \in K$ on a $\big|x + y\big| \leq |x| + \big|y\big|$.
Un corps valué est un corps muni d'une valeur absolue. Les corps valués forment une catégorie dont les morphismes sont les morphismes de corps qui préservent la valeur absolue.

Remarque 13.2. Certains auteurs exigent qu'une valeur absolue soit triangulaire. On verra que cela n'a pas grande importance car une valeur absolue quelconque est toujours *équivalente* (en un sens précisé plus tard) à une valeur absolue triangulaire.

Remarque 13.3. Puisque $|\bullet|$ se restreint en un morphisme de groupes $K^\times \longrightarrow \mathbb{R}_+^*$, on a naturellement $|1| = 1$ et $|1/x| = 1/|x|$ pour $x \in K^\times$. De plus, si $a \in K$ est une racine de l'unité, alors $|a| = 1$. Ainsi pour tout $x \in K$ on a $|-x| = |-1| \cdot |x| = |x|$.
En revanche il n'y a aucune raison d'avoir $|n \cdot 1| = n$ pour $n \in \mathbb{Z}$ en général.

Le troisième axiome peut se reformuler de la façon suivante.

Proposition 13.4. *Soit $|\bullet| : K \longrightarrow \mathbb{R}_+$ vérifiant les deux premiers axiomes de la définition de valeur absolue sur K, et soit $C > 0$. Les énoncés suivants sont équivalents :*

(i) Pour tout $x \in K$ vérifiant $|x| \leq 1$ on a $|1+x| \leq C$.

(ii) Pour tous $x, y \in K$ on a :

$$\left|x+y\right| \leq C \max(|x|, \left|y\right|)$$

Démonstration. Il est clair que le second point entraîne le premier. Supposons le premier point. Soient $x, y \in K$, quitte à échanger leurs rôles on peut supposer $|x| \leq \left|y\right|$. Si $y = 0$, alors $x = 0$ et l'inégalité est immédiate. Sinon, on a :

$$\left|x+y\right| = \left|x/y+1\right| \cdot \left|y\right| \leq C \left|y\right| \leq C \max(|x|, \left|y\right|)$$

car $\left|x/y\right| \leq 1$. □

Exemple 13.5. Voici quelques exemples de corps valués :

— Le corps $\mathbb{R}$, muni de la valeur absolue usuelle.

— Le corps $\mathbb{C}$, muni du module.

— Le corps $\mathbb{Q}$, muni de la valeur absolue usuelle.

— Soit p un nombre premier. À tout élément $x \in \mathbb{Q}$, on peut associer une valuation p-adique, $v_p(x) \in \mathbb{Z} \cup \{\infty\}$ et on peut poser $|x|_p = p^{-v_p(x)}$. Le corps $\mathbb{Q}$, muni de la valeur absolue $|\bullet|_p$ est alors un corps valué.

— Plus généralement, si K est un corps de nombres et $\mathfrak{p}$ est un premier de K, on peut poser :

$$|x|_{\mathfrak{p}} = ||\mathfrak{p}||^{-v_{\mathfrak{p}}(x)}$$

et ainsi définir une valeur absolue sur K.

— Pour k un corps, on peut munir le corps $k(T)$ de la valuation T-adique, en considérant $k(T)$ comme le corps des fractions de l'anneau factoriel $k[T]$.

Définition 13.6. *Soit K un corps, $|\bullet|_1$ et $|\bullet|_2$ deux valeurs absolues sur K. On dit que ces deux valeurs absolues sont équivalentes s'il existe un réel strictement positif α tel que :*

$$|\bullet|_2 = (|\bullet|_1)^\alpha$$

C'est une relation d'équivalence sur l'ensemble des valeurs absolues sur K. La valeur absolue triviale est seule dans sa classe d'équivalence, et pour toute valeur absolue non triviale $|\bullet|$, l'application $\alpha \mapsto |\bullet|^\alpha$ est une bijection entre $\mathbb{R}_+^*$ et la classe d'équivalence de $|\bullet|$.

Définition 13.7. *Soit K un corps et $|\bullet|$ une valeur absolue sur K. On définit la norme de $|\bullet|$ comme :*

$$\mathcal{N}(|\bullet|) = \sup_{|x| \leq 1} |1+x|$$

qui est un réel supérieur ou égal à 1.

La norme se comporte bien vis à vis de l'action de $\mathbb{R}_+^*$ sur l'ensemble des valeurs absolues sur K :

Proposition 13.8. *Soit $|\bullet|$ une valeur absolue sur K et $\alpha > 0$ un réel. On a alors :*

$$\mathcal{N}(|\bullet|^\alpha) = \mathcal{N}(|\bullet|)^\alpha$$

Démonstration. En effet, on a :

$$\mathcal{N}(|\bullet|^\alpha) = \sup_{|x|^\alpha=1} |1+x|^\alpha = \sup_{|x|=1} |1+x|^\alpha = \left(\sup_{|x|=1} |1+x|\right)^\alpha = \mathcal{N}(|\bullet|)^\alpha$$

par croissance de $t \mapsto t^\alpha$ sur $\mathbb{R}_+^*$. □

On dispose de la caractérisation suivante des valeurs absolues triangulaires grâce à la norme.

Théorème 13.9. *Soit K un corps et $|\bullet|$ une valeur absolue sur K. Alors $|\bullet|$ est triangulaire si et seulement si sa norme est inférieure ou égale à 2.*

Démonstration. Si $|\bullet|$ est triangulaire, alors pour tous $x, y \in K$ on a :

$$|x+y| \leq |x| + |y| \leq 2\max(|x|, |y|)$$

donc $\mathcal{N}(|\bullet|) \leq 2$ d'après 13.4.
Supposons maintenant $\mathcal{N}(|\bullet|) \leq 2$. On a donc, pour tous $x, y \in K$:

$$|x+y| \leq 2\max(|x|, |y|)$$

Ainsi, par récurrence, pour tout $n \geq 0$ et tout 2^n-uplet $(x_1, \ldots, x_{2^n}) \in K^{2^n}$, on a :

$$\left|\sum_i x_i\right| \leq 2^n \max_i(|x_i|)$$

En effet, c'est vrai pour $n = 0$, et si c'est vrai pour n, alors :

$$\left|\sum_{i=1}^{2^{n+1}} x_i\right| \leq 2\max\left(\left|\sum_{i=1}^{2^n} x_i\right|, \left|\sum_{i=2^n+1}^{2^{n+1}} x_i\right|\right) \leq 2 \cdot 2^n \max_i(|x_i|)$$

par hypothèse de récurrence.
Ensuite, pour tout entier $k \geq 1$, il existe $n \geq 0$ tel que :

$$2^n \leq k < 2^{n+1}$$

Ainsi pour tout k-uplet $(x_1, \ldots, x_k) \in K^k$, en posant $x_{k+1}, \ldots, x_{2^{n+1}} = 0$, on a :

$$\left|\sum_{i=1}^{k} x_i\right| = \left|\sum_{i=1}^{2^{n+1}} x_i\right| \leq 2^{n+1} \max_i(|x_i|) \leq 2k \max_i(|x_i|)$$

En particulier on a :

$$|k \cdot 1| = |1 + \cdots + 1| \leq 2k$$

Soient alors $x, y \in K$. Pour tout $n \geq 1$, on a :

$$|x+y|^n = \left|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\right| \leq 2(n+1) \max_{0\leq i\leq n} \left|\binom{n}{i} x^i y^{n-i}\right| \leq 4(n+1)\binom{n}{i} \max_{0\leq i\leq n} |x|^i \, |y|^{n-i}$$

$$\leq 4(n+1) \sum_{i=0}^{n} \binom{n}{i} |x|^i \, |y|^{n-i} \leq 4(n+1)(|x| + |y|)^n$$

On a donc :

$$\left|x+y\right| \leq (4(n+1))^{1/n}\left(|x|+\left|y\right|\right)$$

et on en déduit l'inégalité triangulaire pour $|\bullet|$ en faisant tendre n vers l'infini.

□

Corollaire 13.10. *Toute valeur absolue sur K est équivalente à une valeur absolue triangulaire.*

Démonstration. Soit $|\bullet|$ une valeur absolue sur K de norme $C > 1$ (si $C = 1$ l'inégalité triangulaire est déjà vérifiée), alors la valeur absolue équivalente :

$$|\bullet|^{\frac{\log 2}{\log C}}$$

est de norme 2 d'après 13.8 donc est triangulaire d'après 13.10.

□

On dispose de plusieurs caractérisations de l'équivalence de valeurs absolues sur K.

Théorème 13.11. *Soient $|\bullet|_1$ et $|\bullet|_2$ des valeurs absolues non triviales sur K. Les énoncés suivants sont équivalents :*

(i) *Les valeurs absolues $|\bullet|_1$ et $|\bullet|_2$ sont équivalentes.*

(ii) *Pour tout $x \in K$, on a $|x|_1 \leq 1 \implies |x|_2 \leq 1$.*

(iii) *Pour tout $x \in K$, on a $|x|_1 < 1 \implies |x|_2 < 1$.*

(iv) *Pour tout $x \in K$, on a $|x|_1 \leq 1 \iff |x|_2 \leq 1$.*

(v) *Pour tout $x \in K$, on a $|x|_1 < 1 \iff |x|_2 < 1$.*

(vi) *Les valeurs absolues $|\bullet|_1$ et $|\bullet|_2$ définissent la même topologie sur K.*

Démonstration. Il est clair que $(i) \implies (ii)$. Montrons que (ii) entraîne (iii). Supposons (ii). Puisque $|\bullet|_2$ est non triviale, il existe $a \in K$ tel que :

$$0 < |a|_2 < 1.$$

En effet, il existe un élément de valeur absolue différente de 0 et 1, et soit cet élément convient, soit son inverse convient.
Soit $x \in K$ tel que $|x|_1 < 1$. On a donc $|x|_1^n \longrightarrow 0$ quand n tend vers l'infini. Puisque $a \neq 0$, on a $|a|_1 > 0$ et donc *pour n assez grand* :

$$|x^n|_1 \leq |a|_1$$

On a donc $|x^n/a|_1 \leq 1$ et donc, par (ii), on obtient $|x^n/a|_2 \leq 1$, et ainsi :

$$|x|_2 \leq |a|_2^{1/n} < 1$$

comme voulu.
Ensuite, on montre que (iii) entraîne (ii). Supposons (iii) et soit $x \in K$ vérifiant $|x|_1 \leq 1$.

Puisque $|\bullet|_1$ est non triviale il existe $b \in K$ vérifiant $0 < |b|_1 < 1$. Ainsi pour tout n on a $|bx^n|_1 < 1$ et donc par (iii) :

$$|bx^n|_2 < 1$$

On en déduit :

$$|x|_2 < |b|_2^{-1/n} \longrightarrow 1$$

quand n tend vers l'infini. On a donc $|x|_2 \leq 1$. Les points (ii) et (iii) sont donc équivalents. Montrons qu'à eux deux ils entraînent (iv). On suppose (ii) et (iii), et il s'agit de montrer que pour tout $x \in K$ vérifiant $|x|_2 \leq 1$, on a $|x|_1 \leq 1$. Cela s'obtient par la contraposée de (iii) appliquée à $1/x$ (quand $x \neq 0$, sinon c'est immédiat). Ensuite, il est clair que (iv) entraîne (ii). De la même façon, les points (ii) et (iii) entraînent (v), et réciproquement (v) entraîne (iii). Les points (ii) à (v) sont donc équivalents.
Supposons les points (ii) à (v) vérifiés et montrons (i). En particulier, pour tous $x, y \in K$, on a l'équivalence suivante :

$$|x|_1 \leq |y|_1 \iff |x|_2 \leq |y|_2 \quad (*)$$

qui s'obtient en appliquant les points (iv) et (v) à x/y lorsque $y \neq 0$ (c'est immédiat si $y = 0$). Par non trivialité de $|\bullet|_1$, il existe $c \in K$ vérifiant :

$$|c|_1 > 1$$

et donc :

$$|c|_2 > 1$$

On va montrer l'égalité suivante :

$$\frac{\log(|x|_1)}{\log(|c|_1)} = \frac{\log(|x|_2)}{\log(|c|_2)}$$

pour tout $x \in K^\times$. Par densité de $\mathbb{Q}$ dans $\mathbb{R}$, il suffit de montrer l'équivalence suivante pour tout $m/n \in \mathbb{Q}$ avec $m \in \mathbb{Z}$ et $n \geq 1$:

$$\frac{\log(|x|_1)}{\log(|c|_1)} \leq \frac{m}{n} \iff \frac{\log(|x|_2)}{\log(|c|_2)} \leq \frac{m}{n}$$

ou encore, puisque $\log(|c|_i) > 0$ et $n > 0$:

$$|x^n|_1 \leq |c^m|_1 \iff |x^n|_2 \leq |c^m|_2$$

ce qui est un cas particulier de $(*)$. Ainsi on a $\frac{\log(|x|_1)}{\log(|c|_1)} = \frac{\log(|x|_2)}{\log(|c|_2)}$, et donc :

$$|x|_1 = |x|_2^{\frac{\log(|c|_1)}{\log(|c|_2)}}$$

pour $x \neq 0$ (et aussi pour $x = 0$) et les deux valeurs absolues sont donc équivalentes.
Ensuite, on a clairement $(i) \implies (vi)$. Enfin, supposons (vi), et montrons (iii). Soit $x \in K$ vérifiant $|x|_1 < 1$. On a donc :

$$|x^n|_1 \longrightarrow 0$$

quand n tend vers l'infini donc $x^n \longrightarrow 0$ pour la topologie de $|\bullet|_1$ mais donc aussi pour la topologie de $|\bullet|_2$ puisque ce sont les mêmes topologies. Ainsi $|x|_2^n \longrightarrow 0$ donc $|x|_2 < 1$.
□

Définition 13.12. *On appelle place sur un corps K toute classe d'équivalence de valeurs absolues non triviales.*

On munit un corps valué d'une topologie, et même d'une structure uniforme.

Définition 13.13. *Soit $(K,|\bullet|)$ un corps valué. On définit une topologie sur K en prenant comme ouverts de base les boules ouvertes $B(a,\varepsilon) = \{x \in K \mid |a-x| < \varepsilon\}$ pour tout $a \in K$ et $\varepsilon > 0$. Cela forme bien une base d'ouverts puisqu'il s'agit de la base d'ouverts canoniquement associée à la distance $d(x,y) = \left|x-y\right|_{\text{trig}}$ avec $|\bullet|_{\text{trig}}$ une valeur absolue triangulaire équivalente à $|\bullet|$.*
Cette topologie ne dépend que de la classe d'équivalence de $|\bullet|$ (car les boules sont les mêmes pour une autre valeur absolue de la même classe d'équivalence). Muni de cette topologie, K est un corps topologique, au sens où les opérations $+ : K^2 \longrightarrow K$, $\cdot : K^2 \longrightarrow K$ et $x \mapsto x^{-1}$ de $K^\times$ vers $K^\times$ sont continues. En tant que groupe commutatif topologique, K est alors muni d'une structure uniforme. Par exemple, une suite $(x_n) \in K^{\mathbb{N}}$ est de Cauchy si elle l'est pour la distance $d(x,y) = \left|x-y\right|_{\text{trig}}$, et cette notion ne dépend pas de la valeur absolue triangulaire choisie dans la classe d'équivalence de $|\bullet|$.
On dit alors que $(K,|\bullet|)$ est complet s'il l'est pour sa structure uniforme, ce qui est ici équivalent au fait que toute suite de Cauchy sur K converge dans K.

Étant donné un corps valué, on peut toujours le *compléter*, c'est à dire l'inclure dans un corps valué complet dans lequel il est dense.

Théorème 13.14. *Soit $(K,|\bullet|)$ un corps valué. On suppose $|\bullet|$ triangulaire et on note $d(x,y) = \left|x-y\right|$. Le complété métrique $(\hat{K},\hat{d})$ de K pour la distance d ne dépend que de la classe d'équivalence de $|\bullet|$ et il existe une unique structure de corps sur $\hat{K}$ telle que l'inclusion :*

$$K \longrightarrow \hat{K}$$

soit un morphisme de corps et telle que $(\hat{K},\widehat{|\bullet|})$ soit un corps valué, en posant $\widehat{|x|} = \hat{d}(x,0)$.
De plus, le corps valué $\hat{K}$ vérifie la propriété universelle suivante : pour tout corps valué complet L et tout morphisme de corps uniformément continu $f : K \longrightarrow L$, il existe un unique morphisme de corps continu $\hat{f} : \hat{K} \longrightarrow L$ qui prolonge f.

Démonstration. Le compléte métrique de K peut être construit comme le quotient de l'anneau des suites de Cauchy sur K, noté ici $C(K)$ par l'idéal I des suites qui convergent vers 0. De plus I est un idéal maximal : en effet, soit (x_n) une suite de Cauchy qui n'est pas un élément de I. Ainsi il existe $\varepsilon > 0$ tel que pour une infinité de n on ait $|x_n| \geq \varepsilon$. Puisque (x_n) est de Cauchy, on a même à partir d'un certain rang N :

$$|x_n| \geq \varepsilon/2$$

On pose $y_n = 0$ si $n < N$ et $y_n = 1/x_n$ si $n \geq N$, et on observe que (y_n) est de Cauchy dans K car l'inversion est lipschitzienne sur $\{a \in K \mid |a| \geq \varepsilon/2\}$. Ainsi $(y_n) \in C(K)$ et on a :

$$x_n y_n \longrightarrow 1$$

donc $xy \equiv 1\ [I]$ et I est bien maximal. Ainsi $\widehat{K}$ a une structure de corps, et on vérifie facilement que la valeur absolue étendue à $\widehat{K}$ fait de $\widehat{K}$ un corps valué et que l'inclusion

$K \longrightarrow \widehat{K}$ est un morphisme de corps (car elle se factorise par $K \longrightarrow C(K) \longrightarrow C(K)/I = \widehat{K}$). Une telle structure de corps valué est unique par densité de K dans $\widehat{K}$.
Dans la construction, l'anneau $C(K)$ et son idéal I ne dépendent que de la classe d'équivalence de $|\bullet|$ donc $\widehat{K}$ et le morphisme $K \longrightarrow \widehat{K}$ ne dépendent que de la classe d'équivalence de $|\bullet|$.

La propriété universelle est facile à vérifier. □

13.2 Valeurs absolues non archimédiennes

On peut ajouter une condition très stricte à la définition de valeur absolue et obtenir la notion de valeur absolue non archimédienne. Lorsqu'un corps est muni d'une valeur absolue non archimédienne, sa géométrie est très éloignée de la géométrie euclidienne que l'on connait, et sa boule unité a une structure d'anneau de valuation.

Définition 13.15. *Soit $(K,|\bullet|)$ un corps valué. On dit que $|\bullet|$ est archimédienne si $\mathcal{N}(|\bullet|) > 1$. Autrement dit, $|\bullet|$ est non archimédienne si elle vérifie l'inégalité ultramétrique :*

$$\left|x+y\right| \leq \max(|x|, \left|y\right|)$$

pour tous $x,y \in K$. Cela ne dépend que de la place de $|\bullet|$, puisque si deux valeurs absolues sont équivalentes, l'une est une puissance de l'autre (par 13.11). On peut donc parler de places archimédiennes et de places non archimédienne sur K.

Exemple 13.16. Le corps $\mathbb{Q}$ muni de la valeur absolue $|\bullet|_p$ pour p un nombre premier, définie dans 13.5, est non archimédien (c'est clair avec la proposition suivante). On note $\mathbb{Q}_p$ sa complétion métrique (voir 13.14), appelée corps des nombres p-adiques. On étudiera ce corps plus en détail dans la suite.
Plus généralement, si K est un corps de nombres et $\mathfrak{p}$ un premier de K, la valeur absolue $|\bullet|_\mathfrak{p}$ définie dans 13.5 est non arcihmédienne.

Proposition 13.17. *Une valeur absolue $|\bullet|$ sur K est non archimédienne si et seulement si l'image de $\mathbb{Z}$ dans K est bornée pour $|\bullet|$.*

Démonstration. Si la valeur absolue est non archimédienne, alors pour tout $n \in \mathbb{N}$, on a :

$$|n| = |1 + \cdots + 1| \leq \max(|1|, \ldots, |1|) \leq |1|$$

et pour $|-n| = |n|$ donc $|\bullet|$ est bornée sur l'image de $\mathbb{Z}$ dans K.
Supposons ensuite $|\bullet|$ bornée par une constante $M > 0$ sur l'image de $\mathbb{Z}$ dans K. Soient $x,y \in K$ vérifiant $|x| \leq \left|y\right|$. On a :

$$\left|x+y\right|^n = \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \leq \mathcal{N}(|\bullet|) M n \left|y\right|^n$$

donc $\left|x+y\right| \leq (N(|\bullet|)Mn)^{1/n} \left|y\right| \longrightarrow \left|y\right|$ quand n tend vers l'infini, donc $|\bullet|$ est non archimédienne. □

Corollaire 13.18. *Toute valeur absolue sur un corps de caractéristique $p > 0$ est non archimédienne.*

Démonstration. Si K est un corps de caractéristique $p > 0$ alors l'image de $\mathbb{Z}$ dans K est finie donc bornée. □

L'inégalité ultramétrique a un cas d'égalité intéressant.

Proposition 13.19. *Soit $(K, |\bullet|)$ un corps valué non archimédien. Soient $x_1, \dots, x_n \in K$. Si l'un des x_i a une valeur absolue strictement plus grande que tous les autres, alors :*

$$\left|\sum_j x_j\right| = |x_i|.$$

Démonstration. Par l'inégalité ultramétrique on a $\left|\sum_j x_j\right| \leq |x_i|$. Ensuite, supposons par l'absurde $\left|\sum_j x_j\right| < |x_i|$. On a alors :

$$|x_i| = \left|\sum_j x_j - \sum_{j\neq i} x_j\right| \leq \max\left(\left|\sum_j x_j\right|, \left|\sum_{j\neq i} x_j\right|\right) < |x_j|$$

car les deux termes du max sont strictement inférieurs à $|x_j|$. C'est donc absurde. □

Définition 13.20. *Soit K un corps valué non archimédien. On note $\mathcal{O}_K$ ou $\mathcal{O}_{|\bullet|}$ sa boule unité fermée. Par l'inégalité ultramétrique, c'est un anneau, qu'on appelle anneau de valuation de K. Comme son nom l'indique, c'est un anneau de valuation au sens de 3.2. En particulier, c'est un anneau local d'idéal maximal :*

$$\mathfrak{m}_K = B(0,1)$$

la boule unité ouverte de K. De plus le groupe des inversibles $\mathcal{O}_K^\times$ de $\mathcal{O}_K$ est la sphère de rayon 1 de K. Notons de plus que K est le corps des fractions de $\mathcal{O}_K$.
Le corps résiduel $\mathcal{O}_K/\mathfrak{m}$ sera noté κ_K et appelé corps résiduel de K.

Démonstration. Pour chaque $x \in K \setminus \{0\}$, on a $x \in \mathcal{O}_K$ ou $1/x \in \mathcal{O}_K$ donc K est le corps des fractions de $\mathcal{O}_K$ et $\mathcal{O}_K$ est un anneau de valuation (voir 3.8). Ensuite, $x \neq 0$ est inversible dans $\mathcal{O}_K$ si et seulement si $1/x \in \mathcal{O}_K$, c'est à dire $|x| \geq 1$, donc les éléments inversibles de $\mathcal{O}_K$ sont les éléments de valeur absolue 1. L'idéal maximal est donc bien la boule ouverte de rayon 1. □

Proposition 13.21. *L'anneau $\mathcal{O}_K$ est intégralement clos et ses seuls idéaux premiers sont 0 et $\mathfrak{m}_K$, en particulier il est de dimension de Krull au plus 1.*

Démonstration. Soit $x \in K$ entier sur $\mathcal{O}_K$: on peut écrire $x^n = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ avec $|a_i| \leq 1$ donc :

$$|x|^n \leq \max_{k<n} |x|^k$$

donc $|x| \leq 1$.
Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Prenons $x \in \mathfrak{p}$ non nul. Ainsi pour tout $y \in \mathfrak{m}\setminus\{0\}$ on a $|y| < 1$ donc pour n assez grand $|y^n| \leq |x|$ donc x divise y^n et $y^n \in \mathfrak{p}$, or $\mathfrak{p}$ est premier donc $y \in \mathfrak{p}$. Ainsi $\mathfrak{p} = \mathfrak{m}_K$. □

Remarque 13.22. Avec la caractérisation du théorème 3.27, il suffit donc que $\mathcal{O}_K$ soit noethérien pour qu'il soit un anneau de Dedekind local et donc un anneau de valuation discrète. En général, ce n'est pas le cas.

Théorème 13.23. *Soit K un corps non trivialement valué non archimédien. Les énoncés suivants sont équivalents :*

(i) Le groupe des valeurs absolues $|K^\times|$ est discret dans $\mathbb{R}_+^*$.

(ii) Le groupe des valeurs absolues est monogène (i.e. isomorphe à $\mathbb{Z}$ car il n'est pas trivial).

(iii) $\mathcal{O}_K$ (ou $\mathfrak{m}_K$) est principal.

(iv) $\mathcal{O}_K$ est un anneau de valuation discrète.

(v) On a :

$$\bigcap_n \mathfrak{m}_K^n = 0$$

Dans ces conditions, on dit que K est à valuation discrète (ou à valeur absolue discrète), et on appelle uniformisante tout générateur de $\mathfrak{m}_K$.

Démonstration. Les points (iii) et (iv) sont équivalents d'après 3.18. Puisque $\mathbb{R}_+^* \cong \mathbb{R}$ comme groupes topologiques, (ii) et (i) sont équivalents.
Ensuite, voyons que (ii) entraîne (v) : on prend $a > 1$ un générateur du groupe des valeurs absolues. On a alors $\mathfrak{m}_K \subseteq B(0, 1/a)$: en effet si $|<|1$, alors $|x| < 1/a$ par choix de a. Par inégalité ultramétrique on en déduit directement :

$$\mathfrak{m}_K^n \subseteq B(0, 1/a^n)$$

pour tout n et donc l'intersection des $\mathfrak{m}_K^n$ est réduite à 0. Ensuite, on montre par contraposée que (v) entraîne (i) : supposons que la valeur absolue n'est pas discrète, le groupe des valeurs est donc dense dans $\mathbb{R}_+^*$, et ainsi on a :

$$\mathfrak{m}_K = \mathfrak{m}_K^2 = \mathfrak{m}_K^3 = \dots$$

En effet, si $x \in \mathfrak{m}_K \setminus \{0\}$, il existe $y \in K$ avec $|x| < \left|y\right| < 1$ par densité du groupe des valeurs, et donc :

$$x = (x/y)y \in \mathfrak{m}_K^2.$$

Ceci entraîne que l'intersection des $\mathfrak{m}_K^n$ n'est pas réduite à 0.
Supposons (iii) vérifié, on prend alors π un générateur de $\mathfrak{m}_K$ (non nul car $\mathcal{O}_K \neq K$ par non trivialité de la valeur absolue). Il est alors clair que le groupe des valeurs absolues est engendré par $|\pi|$ car tout élément non nul de K peut s'écrire $\pi^n u$ avec n entier et u inversible. Ainsi (iii) entraîne (ii), et la réciproque est similaire. □

Les corps valués non archimédiens ont une topologie étonnante.

Proposition 13.24. *Soit K un corps valué non archimédien. Les faits suivants sont vérifiés :*

— *Si une suite (x_n) converge vers un élément $x \in K \setminus \{0\}$, alors $|x_n| = |x|$ à partir d'un certain rang.*

— *Les boules ouvertes, les boules fermées et les sphères de K (non dégénérées) sont à la fois ouvertes et fermées.*

— *K est totalement discontinu (les seules parties connexes non vides sont les singletons).*

— *Tout point d'une boule B est un centre de B.*

— *Deux boules ouvertes (respectivement fermées) sont soit disjointes soit emboitées l'une dans l'autre.*

— *Tout triangle est isocèle.*

— *Pour tout $\varepsilon > 0$, la relation $d(x,y) < \varepsilon$ (ou $d(x,y) \leq \varepsilon$)) est une relation d'équivalence sur K et on a ainsi une partition de K en boules ouvertes (ou fermées) de rayon ε.*

Démonstration. Soit (x_n) une suite qui converge vers $x \in K \setminus \{0\}$. Puisque $|x| > 0$, à partir d'un certain rang on a :

$$|x - x_n| < |x|$$

et donc $|x_n| = |(x_n - x) + x| = |x|$ d'après le cas d'égalité ultramétrique 13.19.
Pour le second point, puisque la topologie est invariante par translations et par dilatations, on peut se contenter de montrer que la boule unité ouverte $\mathfrak{m}$, la boule unité fermée $\mathcal{O}$ et la sphère unité $\mathcal{O}^\times$ sont ouvertes et fermées. $\mathfrak{m}$ est clairement ouvert, et il est fermé car si $x_n \longrightarrow x$ avec $x_n \in \mathfrak{m}$ et $x \in K$, ou bien $x = 0$ auquel cas $x \in \mathfrak{m}$, ou bien $x \neq 0$ auquel cas par ce qui précède on a $|x_n| = |x|$ à partir d'un certain rang donc $x \in \mathfrak{m}$. $\mathcal{O}$ est clairement fermé, et il est ouvert car son complémentaire est fermé avec le même type d'argument. La sphère est ouverte et fermée car :

$$\mathcal{O}^\times = \mathcal{O} \cap (K \setminus \mathfrak{m}).$$

Ensuite K est totalement discontinu car si $A \subseteq K$ contient deux points distincts x, y, on a par exemple en notant $r = \frac{1}{2}\left|x - y\right|$:

$$A = (B(x,r) \cap A) \sqcup (A \setminus B(x,r))$$

qui est un recouvrement de A par deux ouverts disjoints et non-vides, donc A n'est pas connexe. Par contraposée, toute partie connexe contient au plus 1 point.
Soit $x \in B(y,r)$ avec $r > 0$ et $y \in K$ (cela peut aussi bien être la boule ouverte que la boule fermée, contentons nous du cas de la boule ouverte). On veut voir :

$$B(y,r) = B(x,r).$$

Autrement dit il faut montrer que pour tout $z \in K$, on a :

$$\left|z - y\right| < r \iff |z - x| < r.$$

Si $\left|z - y\right| < r$, alors $|z - x| = \left|z - y + y - x\right| \leq \max(\left|z - y\right|, \left|y - x\right|) < r$ par inégalité ultramétrique et pareil pour l'autre implication.
Soient B_1 et B_2 deux boules ouvertes (respectivement fermées) non disjointes. Sans perte de généralité on peut supposer que le rayon r_1 de la première est inférieur ou égal au rayon r_2 de la seconde. Un point d'intersection p de ces deux boules est alors un centre pour chacune d'entre elles, donc B_1 est contenue dans B_2 car c'est la boule de centre p et de rayon $r_1 \leq r_2$.
Soient $x, y, z \in K$ trois points. On veut voir que parmi les longueurs $\left|x - y\right|$, $|x - z|$ et

$\left|y-z\right|$, au moins deux sont égales. On suppose par l'absurde qu'elles sont deux à deux distinctes, de sorte que sans perte de généralité on peut les classer dans l'ordre :

$$\left|x-y\right| < |x-z| < \left|y-z\right|$$

et ainsi :

$$\left|x-y\right| = \left|x-z+z-y\right| = \left|y-z\right|$$

par le cas d'égalité ultramétrique 13.19. C'est absurde.
Le dernier point découle directement de l'inégalité ultramétrique. □

Remarque 13.25. La proposition 13.24 montre en particulier que la boule unité fermée n'est pas (en général) l'adhérence de la boule unité ouverte !

Proposition 13.26. *Soit K un corps valué non archimédien, on note $\widehat{K}$ son complété. Alors $\widehat{K}$ est non archimédien et on a les égalités suivantes (la barre horizontale désigne l'adhérence topologique dans $\widehat{K}$, ou de manière équivalente, le complété métrique) :*

$$\mathcal{O}_{\widehat{K}} = \overline{\mathcal{O}_K} \quad \mathfrak{m}_{\widehat{K}} = \overline{\mathfrak{m}_K} \quad \kappa_{\widehat{K}} = \kappa_K \quad \left|\widehat{K}^\times\right| = |K^\times|$$

où $\left|\widehat{K}\right|$ désigne le groupe des valeurs absolues, c'est à dire l'image de $K^\times$ par le morphisme $|\bullet|$. En particulier K est à valeur absolue discrète si et seulement si $\widehat{K}$ l'est.

Démonstration. Le complété est non archimédien car la formule de l'inégalité ultramétrique est continue en x et y, l'inégalité est large, et K est dense dans $\widehat{K}$. Ensuite on a $\overline{\mathcal{O}_K} \subseteq \mathcal{O}_{\widehat{K}}$ par continuité de la valeur absolue et fermeture de $\mathcal{O}_{\widehat{K}}$. De même $\overline{\mathfrak{m}_K} \subseteq \mathfrak{m}_{\widehat{K}}$. Les inclusions réciproques viennent du fait que tout élément de $\widehat{K}$ est limite d'une suite d'éléments de K et du fait que si une suite converge vers un élément non nul de $\widehat{K}$, alors à partir d'un certain rang sa valeur absolue stationne.
On a alors le diagramme suivant :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{m}_K & \longrightarrow & \mathcal{O}_K & \longrightarrow & \kappa_K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathfrak{m}_{\widehat{K}} & \longrightarrow & \mathcal{O}_{\widehat{K}} & \longrightarrow & \kappa_{\widehat{K}} & \longrightarrow & 0 \end{array}$$

et il s'agit de voir que la flèche $\kappa_K \hookrightarrow \kappa_{\widehat{K}}$ est surjective, autrement dit que :

$$\mathcal{O}_{\widehat{K}} = \mathcal{O}_K + \mathfrak{m}_{\widehat{K}}.$$

Or si $x \in \mathcal{O}_{\widehat{K}}$, on peut écrire $x = \lim x_n$ avec $x_n \in \mathcal{O}_K$ et pour n assez grand $|x_n - x| < 1$ ce qui conclut. Enfin, en utilisant encore le fait que la valeur absolue d'une suite qui converge vers un élément non nul stationne, on obtient :

$$\left|K^\times\right| = \left|\widehat{K}^\times\right|.$$

□

La convergence des séries dans un corps valué non archimédien est facile à vérifier.

Proposition 13.27. *Soit K un corps valué non archimédien et (a_n) une suite d'éléments de K. Alors (a_n) est de Cauchy si et seulement si $a_{n+1} - a_n \longrightarrow 0$.*
Si K est complet, alors la série $\sum a_n$ converge si et seulement si $a_n \longrightarrow 0$.

Démonstration. Si (a_n) est de Cauchy on a clairement $a_{n+1} - a_n \longrightarrow 0$. Réciproquement, si $a_{n+1} - a_n \longrightarrow 0$, pour tout $\varepsilon > 0$, à partir d'un certain rang on a $|a_{n+1} - a_n| < \varepsilon$ et par inégalité ultramétrique pour tout $m \geq n$ on a donc $|a_m - a_n| < \varepsilon$.
Le deuxième point est une conséquence directe du premier. □

Lemme 13.28. *Soit L/K une extension algébrique et $|\bullet|$ une valeur absolue sur L dont la restriction à K est triviale. Alors $|\bullet|$ est triviale sur L.*

Remarque 13.29. Ce n'est pas le cas pour une extension non algébrique : par exemple il existe des valeurs absolues sur $K(T)$ non triviales mais triviales sur K.

Démonstration. D'abord, $|\bullet|$ est non archimédienne car sa restriction à K est non archimédienne. On a alors :

$$\mathcal{O}_L \supseteq K$$

car la valeur absolue est triviale sur K. Par conséquent $\mathcal{O}_L$ est un corps : en effet, si $x \in \mathcal{O}_L \setminus \{0\}$, x est algébrique sur K donc $\mathcal{O}_L \supseteq K[x] = K(x)$. Ainsi $\mathcal{O}_L = L$: la valeur absolue $|\bullet|$ est triviale. □

13.3 Places sur $\mathbb{Q}$ et $K(T)$

Théorème 13.30. *(Ostrowski) Les places sur $\mathbb{Q}$ sont exactement les places suivantes (qui sont de plus deux à deux distinctes) :*

- *La place archimédienne représentée par la valeur absolue usuelle $|\bullet|_\infty$ sur $\mathbb{Q}$, définie par $|x|_\infty = \sqrt{x^2}$.*
- *Pour chaque p premier, la place non archimédienne représentée par la valeur absolue p-adique définie par :*

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

Démonstration. D'abord ces places sont deux à deux distinctes : $|\bullet|_\infty$ et $|\bullet|_p$ sont non équivalentes car l'une est archimédienne et l'autre non, et si $p \neq q$, on a $|p|_p < 1$ alors que $|p|_q = 1$, donc elles ne sont pas équivalentes.
Ensuite, soit $|\bullet|$ une valeur absolue non triviale sur $\mathbb{Q}$, qu'on peut supposer triangulaire d'après 13.10.
Si $|\bullet|$ est non archimédienne, alors $\mathfrak{m}_{|\bullet|}$ est un idéal maximal de $\mathcal{O}_{|\bullet|}$ donc $\mathfrak{m}_{|\bullet|} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ qui n'est pas nul car la valeur absolue est non triviale et non archimédienne (si tout entier non nul est de valeur absolue au moins 1, par caractère non archimédien tout entier non nul est de valeur absolue exactement 1 et donc tout rationnel non nul aussi). Ainsi $\mathfrak{m}_{|\bullet|} \cap \mathbb{Z} = p\mathbb{Z}$ pour un certain nombre premier p. On a donc $\mathbb{Z} \setminus p\mathbb{Z} \subseteq \mathcal{O}_{|\bullet|}^\times$ et donc en localisant :

$$\mathbb{Z}_{p\mathbb{Z}} \subseteq \mathcal{O}_{|\bullet|}$$

or $\mathcal{O}_{|\bullet|_p} = \mathbb{Z}_{p\mathbb{Z}}$ donc $\mathcal{O}_{|\bullet|_p} \subseteq \mathcal{O}_{|\bullet|}$, ce qui entraîne que les valeurs absolues sont équivalentes d'après 13.11.
Supposons maintenant que $|\bullet|$ est archimédienne. Soient a, b des entiers supérieurs ou égaux à 2 quelconques. On décompose a en base b :

$$a = \sum_{k=0}^{r} a_k b^k$$

avec $0 \leq a_k < b$ et $a_r \neq 0$. Puisque $a_r \neq 0$, on a $a > \sum_{k=0}^{r-1}(b-1)b^k = b^r - 1$ donc $b^r \leq a$ et :

$$r \leq \frac{\log a}{\log b}.$$

De plus, l'inégalité triangulaire donne $|a_k| = \left|\sum_{i=1}^{a_k} 1\right| \leq a_k \leq b$ de sorte que :

$$|a| \leq \sum_{k=0}^{r} b\,|b|^k \leq \sum_{k=0}^{r} b \max(1,|b|)^r \leq (1+r)b\max(1,|b|)^r \leq \left(1 + \frac{\log a}{\log b}\right) b \max(1,|b|)^{\frac{\log a}{\log b}}$$

Cette inégalité est valable pour tous $a, b \geq 2$ entiers donc elle est vraie pour a^n pour tout $n \geq 1$:

$$|a|^n \leq \left(1 + n\frac{\log a}{\log b}\right) b \max(1,|b|)^{n\frac{\log a}{\log b}}$$

et donc :

$$|a| \leq \left(1 + n\frac{\log a}{\log b}\right)^{1/n} b^{1/n} \max(1,|b|)^{\frac{\log a}{\log b}} \underset{n\to\infty}{\longrightarrow} \max(1,|b|)^{\frac{\log a}{\log b}}$$

par croissances comparées (on pourra passer au logarithme pour s'en convaincre).
Cette inégalité est vraie pour tous $a, b \geq 2$ entiers et il existe $a_0 \geq 2$ un entier tel que $|a_0| > 1$ car $\mathbb{Z}$ est non borné pour $|\bullet|$ puisqu'elle est non archimédienne. En appliquant notre inégalité à a_0, on a donc :

$$1 < |a_0| \leq \max(1,|b|)^{\frac{\log a_0}{\log b}}$$

donc $|b| > 1$. Ainsi pour tout $n \geq 2$ entier, on a $|n| > 1$, et donc on a montré, pour tous $a, b \geq 2$ entiers :

$$|a| \leq |b|^{\frac{\log a}{\log b}}$$

ce qui donne en passant au logarithme :

$$\frac{\log|a|}{\log a} \leq \frac{\log|b|}{\log b}$$

et par symétrie on a une égalité pour tous $a, b \geq 2$ entiers :

$$\frac{\log|a|}{\log a} = \frac{\log|b|}{\log b}.$$

Cette quantité est donc une constante $\alpha > 0$, et ainsi pour tout $n \geq 2$ entier on a :

$$|n| = n^\alpha.$$

On en déduit aussitôt que $|x| = |x|_\infty^\alpha$ pour tout $x \in \mathbb{Z}$ puis pour tout $x \in \mathbb{Q}$. Donc $|\bullet|$ est équivalente à la valeur absolue $|\bullet|_\infty$. □

Le théorème d'Ostrowski a une première application très intéressante : il permet de simplifier la définition de la norme d'une valeur absolue.

Corollaire 13.31. *Soit $(K,|\bullet|)$ un corps valué. On a :*

$$\mathcal{N}(|\bullet|) = \max(1,|2|).$$

En particulier, si K' est un sous-corps de K, on a :

$$\mathcal{N}(|\bullet|) = \mathcal{N}\left(|\bullet|_{|K'}\right).$$

Démonstration. D'abord, si $|\bullet|$ est non archimédienne, la norme vaut 1 et on a bien $|2| = |1+1| \leq \max(|1|,|1|) \leq 1$.
Supposons maintenant $|\bullet|$ archimédienne. Clairement, la formule à démontrer ne change pas si l'on remplace $|\bullet|$ par $|\bullet|^\alpha$ avec $\alpha > 0$, donc on peut supposer $|\bullet|$ triangulaire (d'après 13.10).
Puisque la valeur absolue est archimédienne, K est de caractéristique nulle et $\mathbb{Q} \subseteq K$ (par 13.18). La restriction de la valeur absolue à $\mathbb{Q}$ est encore archimédienne, donc elle est équivalente à $|\bullet|_\infty$ par le théorème d'Ostrowski (13.30). Il existe donc $\alpha > 0$ tel que $|\bullet|_{|\mathbb{Q}} = |\bullet|_\infty^\alpha$. Or $|\bullet|_{|\mathbb{Q}}$ est triangulaire donc :

$$2 \geq \mathcal{N}(|\bullet|_\infty^\alpha) = 2^\alpha$$

et ainsi $\alpha \leq 1$.
On a alors pour tous $x,y \in K$ et $n \geq 0$ avec $|x| \leq |y|$:

$$|x+y|^n \leq \sum_{k=0}^{n} \left|\binom{n}{k}\right|_\infty^\alpha |x^k| \cdot |y^{n-k}| \leq |y|^n \sum_{k=0}^{n} \binom{n}{k}^\alpha \leq (n+1)^{1-\alpha} |y|^n \left(\sum_{k=0}^{n} \binom{n}{k}\right)^\alpha$$

par l'inégalité de Jensen puisque $t \mapsto t^\alpha$ est concave puisque $\alpha \leq 1$. On a donc :

$$|x+y|^n \leq 2^{n\alpha}(n+1)^{1-\alpha} |y|$$

et ainsi $|x+y| \leq 2^\alpha |y| = |2| \cdot |y|$ en prenant la puissance $1/n$ et en passant à la limite. On a donc bien :

$$\mathcal{N}(|\bullet|) \leq |2|$$

et l'autre inégalité est immédiate. □

Remarque 13.32. Par conséquent, le caractère triangulaire et le caractère archimédien d'une valeur absolue ne dépendent que de la valeur absolue de 2, et donc ne dépendent que de la restriction de la valeur absolue au sous-corps premier.

Avec la même stratégie, pour K un corps quelconque, on peut lister les places sur le corps $K(T)$ qui donnent des valeurs absolues triviales en restriction à K. Si K est un corps fini, toute valeur absolue sur K est triviale et donc on liste ainsi toutes les places sur $K(T)$.

Théorème 13.33. *Soit K un corps. Pour chaque polynôme irréductible unitaire $p(T) \in K[T]$, on définit une valeur absolue (non archimédienne) sur $K(T)$ via :*

$$|f|_p = \exp(-v_p(f))$$

où la valuation p-adique vient de la structure d'anneau factoriel de $K[T]$ et est étendue par multiplicativité à $K(T)$. On définit aussi une valeur absolue (non archimédienne) dite "à l'infini" :

$$|f|_\infty = |f(1/T)|_T = \exp(\deg(f))$$

où le degré d'une fraction rationnelle a/b est $\deg a - \deg b$ et $\deg(0) = -\infty$.
Ces valeurs absolues sont deux à deux non équivalentes, non triviales, et leur restriction à K est non triviale. De plus toute valeur absolue sur $K[T]$ dont la restriction à K est triviale est équivalente à l'une de celles-ci.
Pour employer le vocabulaire de la géométrie algébrique, on a donc une correspondance entre les places sur $K[T]$ qui induisent la valeur absolue triviale sur K et les points fermés de la droite projective $\mathbb{P}^1_K$, c'est à dire les polynômes irréductibles unitaires et un point à l'infini.

Démonstration. Il est facile de vérifier que ces objets sont bien des valeurs absolues non archimédiennes sur $K[T]$ dont la restriction à K est la valeur absolue triviale. De plus, elles sont non triviales car $|p|_p = \frac{1}{e}$ et $|T|_\infty = e$.
Justifions l'égalité :

$$|f(1/T)|_T = \exp(\deg(f)).$$

Il suffit de le vérifier pour $f \in K[T]\setminus\{0\}$. On écrit $f = \sum_{i=0}^n a_i T^i$ avec $a_n \neq 0$ de sorte que $f(1/T) = \sum_{i=0}^n a_i T^{-i} = T^{-n}\sum_{i=0}^n a_i T^{n-i}$ et $v_T(f(1/T)) = -n$ car $a_n \neq 0$. Donc :

$$|f(1/T)|_T = \exp(n) = \exp(\deg(f)).$$

Ces valeurs absolues sont deux à deux non-équivalentes : si p et q sont deux polynômes unitaires irréductibles distincts (et donc premiers entre eux), on a $|p|_p = \frac{1}{e} < 1$ et $|p|_q = 1$ donc $|\bullet|_p$ et $|\bullet|_q$ ne sont pas équivalentes. De plus, $|p|_\infty = \exp(\deg p) \geq 1$ donc $|\bullet|_p$ et $|\bullet|_\infty$ ne sont pas équivalentes.
Soit maintenant $|\bullet|$ une valeur absolue non triviale sur $K(T)$ dont la restriction à K est triviale, en particulier non archimédienne. Par la remarque 13.32, $|\bullet|$ est non archimédienne et on peut considérer son anneau de valuation $\mathcal{O}$ et son idéal maximal $\mathfrak{m}$.
On traite d'abord le cas où $|T| \leq 1$. Puisque $|\bullet|$ est triviale sur K on a alors $K[T] \subseteq \mathcal{O}$ et on peut considérer l'idéal premier $\mathfrak{m} \cap K[T]$ de $K[T]$. Cet idéal est non nul sans quoi tout polynôme non nul serait de valeur absolue au moins 1, tout en étant de valeur absolue au plus 1 car dans $\mathcal{O}$, et donc la valeur absolue serait triviale car tout élément de $K(T)$ est quotient de deux polynômes.
Cet idéal premier est donc de la forme $pK[T]$ avec p un polynôme irréductible unitaire. Pour tout $q \neq p$ irréductible unitaire, $q \notin \mathfrak{m}$ car $q \notin pK[T]$ et donc $|q| = 1$. Ainsi la boule unité ouverte de $|\bullet|_p$ est contenue dans $\mathfrak{m}$ la boule unité ouverte de $|\bullet|$ donc ces valeurs absolues sont équivalentes.
Si $|T| > 1$, on considère la valeur absolue suivante :

$$|f|^\vee = |f(1/T)|$$

qui vérifie $|T|^\vee < 1$ et qui est triviale sur K donc est équivalente à une valeur absolue du type $|\bullet|^p$ pour p irréductible unitaire d'après ce qui précède. Il existe donc une constante $\alpha > 0$ telle que :

$$|f| = |f(1/T)|_p^\alpha .$$

Si $p = T$ on obtient que $|\bullet|$ est équivalente à $|\bullet|_\infty$ et si $p \neq T$ on obtient la valeur absolue associée au polynôme irréductible $T^{\deg p} p(1/T)$. Un argument plus simple est de dire que le cas $p \neq T$ est exclu car dans ce cas $|T| = 1$. □

Chapitre 14

Corps locaux

> Les théoriciens des nombres disent que la théorie des nombres est trop difficile, alors faisons comme s'il n'y avait qu'un seul nombre premier, et ensuite combinons tous ces résultats. De façon surprenante, quelque fois ça marche.
>
> Saharon Shelah

14.1 Propriétés générales des corps locaux

Définition 14.1. *Un corps local est un corps valué localement compact avec une valeur absolue non triviale.*

On va donner dans cette partie une classification complète des corps locaux, suivant s'ils sont archimédiens ou non.

Exemple 14.2. Par exemple, $\mathbb{R}$ et $\mathbb{C}$ sont des corps locaux et pour tout nombre premier p, $\mathbb{Q}_p$ est un corps local comme on le verra plus tard (voir 14.15).

Remarque 14.3. On peut remplacer l'hypothèse de locale compacité par l'hypothèse *"la boule unité fermée de K est compacte"*.
En effet, si K est localement compact, alors 0 admet un voisinage compact donc il existe $r > 0$ tel que la boule ouverte $B(0,r)$ soit d'adhérence compacte. Puisque la valeur absolue est non triviale il existe $x \in K$ tel que $\overline{B}(0,1) \subseteq x\overline{B}(0,r)$ et donc la boule unité fermée est compacte. Réciproquement, si la boule unité fermée B est compacte, tout point x de K a pour voisinage compact $x + B$.

Proposition 14.4. *Un corps local est complet.*

Démonstration. Soit (x_n) une suite de Cauchy dans K un corps local. Il existe un rang N tel que pour tout $n \geq N$ on ait $x_n - x_N \in \overline{B}(0,1)$. Or la boule $\overline{B}(0,1)$ est compacte donc

$(x_n - x_N)$ a une valeur d'adhérence, et donc (x_n) a une valeur d'adhérence, et puisqu'elle est de Cauchy, elle converge vers cette valeur d'adhérence. □

Les corps locaux permettent d'avoir accès aux résultats basiques de topologie des espaces vectoriels normés.

Proposition 14.5. *Soit K un corps valué complet et V un K-espace vectoriel normé de dimension finie. Alors toutes les normes sur V sont équivalentes (et donc définissent la même structure uniforme et la même topologie) et V est complet pour n'importe laquelle de ces normes.*

Démonstration. On peut supposer que $V = K^d$. Observons d'abord que V est complet pour la norme infinie $\|\bullet\|_\infty$ définie par :

$$\|x\|_\infty = \sup_i |x_i|$$

En effet, si une suite de Cauchy converge pour cette norme, chaque coordonnée de cette suite est de Cauchy dans K qui est complet donc chaque coordonnée converge, or la topologie induite par cette norme est la topologie produit donc la suite de départ converge.
De plus, observons que toute norme équivalente à la norme infinie fait de V un espace *complet* : en effet, deux normes équivalentes définissent la même structure uniforme.
À présent, soit $\|\bullet\|$ une norme sur V. Il est clair que $\|\bullet\|$ est *plus fine* que $\|\bullet\|_\infty$:

$$\|x\| = \left\| \sum_i x_i e_i \right\| \leq \sum_i \|e_i\| \cdot \|x\|_\infty \leq C \|x\|_\infty$$

en posant $C = \sum_i \|e_i\|$ qui ne dépend pas de x.
On montre ensuite par récurrence sur $d = \dim V$ que $\|\bullet\|_\infty$ est plus fine que $\|\bullet\|$.
Le cas $d = 0$ est clair. Traitons le cas d en supposant que le cas $d-1$ est vérifié. On suppose par l'absurde que $\|\bullet\|_\infty$ n'est pas plus fine que $\|\bullet\|$. Il existe alors une suite (x^n) de points de V qui vérifie :

$$\|x^n\|_\infty = 1$$

pour tout n et :

$$\|x^n\| \longrightarrow 0.$$

Puisque $\|x^n\|_\infty = 1$, il existe une coordonnée de x^n qui vaut 1 en valeur absolue, et puisqu'il y a un nombre fini de coordonnées, le principe des tiroirs entraîne qu'il existe i tel que $\left|x_i^n\right| = 1$ pour une *infinité* de n. Quitte à extraire, quitte à renuméroter les coordonnées et quitte à multiplier x_n par $1/x_i^n$, on peut supposer :

$$x_d^n = 1.$$

La suite $(x_n - e_d)$ est donc à valeurs dans K^{d-1} et est de Cauchy pour la norme $\|\bullet\|$ (car elle converge dans K^d), or par hypothèse de récurrence $(K^{d-1}, \|\bullet\|)$ est complet donc $x_n - e_d \longrightarrow y$ avec $y \in K^{d-1}$. Or x_n tend vers 0 dans $(K^d, \|\bullet\|)$, donc $e_d \in K^{d-1}$: c'est absurde.

□

Proposition 14.6. *Soit K un corps local et V un K-espace vectoriel normé de dimension finie. Alors les parties compactes de V sont exactement les parties fermées et bornées de V.*

Démonstration. Un compact de V est clairement fermé et borné. Réciproquement, soit A une partie fermée et bornée de V. On peut supposer $V = K^d$ et que V est muni de la norme infinie d'après 14.5 puisque toutes les normes sur V sont équivalentes. Puisque A est bornée pour la norme infinie, il existe $M > 0$ tel que :

$$A \subseteq \overline{B}(0, M)^n$$

et donc A est compacte en tant que partie fermée d'un compact. □

Les applications linéaires entre deux espaces vectoriels de dimension finie sur un corps valué complet sont toutes continues :

Proposition 14.7. *Soit K un corps valué complet, V un K-espace vectoriel normé de dimension finie et W un K-espace vectoriel normé. Alors toute application K-linéaire $V \longrightarrow W$ est lipschitzienne (et donc continue).*

Démonstration. Prenons $(e_1, \ldots, e_d)$ une K-base de V. Soit $f : V \longrightarrow W$ une application K-linéaire. On peut supposer que la norme sur V est la norme infinie associée à $(e_1, \ldots, e_d)$ car toutes les normes sur V sont équivalentes et ainsi cela ne change pas le caractère lipschitz de f. Soit $x = \sum \lambda_i e_i \in V$. On a :

$$\|f(x)\| \leq \sum |\lambda_i| \cdot \|f(e_i)\| \leq \|x\|_\infty \cdot \Big(\sum \|f(e_i)\| \Big)$$

donc f est lipschitzienne. □

On mentionne enfin la version du théorème de Riesz pour les corps locaux.

Théorème 14.8. *Soit K un corps local et V un K-espace vectoriel normé. Les énoncés suivants sont équivalents :*

(i) V est de dimension finie.

(ii) La boule unité fermée de V est compacte.

(iii) V est localement compact.

Démonstration. L'équivalence entre les deux derniers points est facile à obtenir, en imitant la remarque 14.3. Puisque la valeur absolue sur K est non triviale, il existe $u \in K^\times$ tel que $0 < |u| < 1$.
Ensuite, la proposition 14.6 entraîne l'implication $(i) \implies (ii)$ car la boule unité fermée est fermée et bornée dans V.
Enfin, supposons que la boule unité fermée B est compacte. En particulier B est *précompacte* et donc il existe F une partie *finie* de B telle que :

$$B \subseteq \bigcup_{x \in F} \overline{B}(x, |u|)$$

Soit maintenant $y \in B$. Il existe $x_0 \in F$ avec $\left\|x_0 - y\right\| \leq |u|$ donc $\frac{y-x_0}{u} \in B$. Il existe ensuite $x_1 \in F$ tel que $\frac{1}{u}\left(\frac{1}{u}(y-x_0)-x_1\right) \in B$ et ainsi de suite. On construit donc une suite (x_n) de points de F tels que pour tout n :

$$u^{-(n+1)}y - \sum_{k=0}^{n} u^{-(n-k+1)}x_k \in B$$

Ainsi on obtient :

$$\left\| y - \sum_{k=0}^{n} u^k x_k \right\| \leq |u|^{n+1} \longrightarrow 0$$

Ceci montre que y est dans l'adhérence de $W = \mathrm{Vect}_K(F)$, or W est de dimension finie sur un corps local donc *complet* (par 14.5) et donc W est fermé dans V. Ainsi $y \in W$ et donc $B \subseteq W$, et puisque la valeur absolue sur K est non triviale :

$$V = W$$

donc V est de dimension finie. □

Théorème 14.9. *Soit $(K, |\bullet|)$ un corps local avec une valeur absolue triangulaire et L/K une extension algébrique. Alors il existe une unique valeur absolue $|\bullet|_*$ sur L qui prolonge $|\bullet|$. De plus, pour tout $x \in L$ et tout $M \subseteq L$ extension finie de K contenant x, on a la formule :*

$$|x|_* = \left|N_{M/K}(x)\right|^{1/[M:K]}$$

Enfin, si L/K est finie, L est encore un corps local pour cette valeur absolue.

Démonstration. On commence par montrer ce théorème dans le cas où L/K est finie. On pose alors, pour tout $x \in L$:

$$|x|_* = \left|N_{L/K}(x)\right|^{1/d}$$

avec $d = [L : K]$. Ainsi pour $x \in K$ on retrouve $|x|_* = |x|$ donc $|\bullet|_*$ étend $|\bullet|$. Montrons que $|\bullet|_*$ est une valeur absolue sur L. On a :

$$|x|_* = 0 \iff N_{L/K}(x) = 0 \iff x = 0$$

Ensuite $|\bullet|_*$ est clairement multiplicative. On fixe à présent (e_i) une K-base de L et $\|\bullet\|$ la norme infinie associée sur le K-espace vectoriel de dimension finie L. La particularité d'une telle norme est qu'elle est à valeurs dans $|K|$, et donc pour tout $x \in L \setminus \{0\}$, il existe $\lambda \in K$ tel que :

$$\|\lambda x\| = 1.$$

La sphère $S = \{x \in L \mid \|x\| = 1\}$ est fermée et bornée donc compacte (par 14.6), et $|\bullet|_*$ est continue pour la norme $\|\bullet\|$ car $N_{L/K}$ est polynomiale sur L. Ainsi l'image par $|\bullet|_*$ de S est compacte et ne contient pas 0 donc il existe $C > 0$ qui vérifie :

$$\|x\| = 1 \implies |x|_* \geq C$$

pour tout $x \in L$. Ainsi, pour tout $x \in L \setminus \{0\}$, en prenant un $\lambda \in K$ tel que $\|\lambda x\| = 1$, on obtient $|\lambda| \cdot |x|_* \geq C$, or $|\lambda| \cdot \|x\| = 1$ donc :

$$|x|_* \geq C \|x\|$$

On pose à présent $B = \{x \in L \mid |x|_* \leq 1\}$, on obtient que B est compacte pour la topologie donnée par $\|\bullet\|$: en effet B est fermée car $|\bullet|_*$ est continue et B est bornée pour $\|\bullet\|$ d'après l'inégalité précédente. Ainsi $1 + B$ est compacte et donc $|\bullet|_*$ est majorée sur $1 + B$, ce qui est la condition voulue pour avoir une valeur absolue (proposition 13.4).

Voyons l'unicité (toujours dans le cas L/K finie). Soient $|\bullet|_1$ et $|\bullet|_2$ qui prolongent $|\bullet|$ sur L. Ces valeurs absolues sont équivalentes à des valeurs absolues triangulaires, donc à des normes sur le K-espace vectoriel de dimension finie L, qui sont équivalentes (par 14.5), donc ces valeurs absolues sont équivalentes. Or elles coïncident sur le sous-corps K et sont non triviales sur K donc elles sont égales (en effet l'une est une puissance de l'autre, et l'exposant vaut 1 car il existe des éléments de K de valeur absolue différente de 0 et de 1).

Enfin, traitons le cas de L/K algébrique. Dans ce cas, L est recouvert par les extensions intermédiaires finies M/K. De plus, si M_1 et M_2 sont deux extensions finies de K, il existe une unique valeur absolue $|\bullet|_1$ sur M_1 et une unique valeur absolue $|\bullet|_2$ sur M_2 qui prolongent $|\bullet|$, et ces deux valeurs absolues coïncident sur le corps $M_1 \cap M_2$ par unicité. Ainsi il existe une unique valeur absolue sur L qui prolonge toutes les valeurs absolues des extensions finies intermédiaires, obtenue en les recollant.

Enfin, si L/K est finie, alors la valeur absolue $|\bullet|_*$ fait de L un corps local car la valeur absolue est non triviale et L est localement compact car de dimension finie sur K (par 14.8).

□

14.2 Corps locaux archimédiens

La liste des corps locaux archimédiens est très simple.

Théorème 14.10. *Tout corps local archimédien est isomorphe à $\mathbb{R}$ ou à $\mathbb{C}$ (munis d'une valeur absolue équivalente à la valeur absolue ou au module usuel). Réciproquement, $\mathbb{R}$ et $\mathbb{C}$ sont bien des corps locaux archimédiens.*

Démonstration. Soit K un tel corps. On peut supposer que la valeur absolue sur K est triangulaire. Puisque K est archimédien, K est de caractéristique nulle et donc on peut considérer que $\mathbb{Q} \subseteq K$. La restriction de la valeur absolue de K à $\mathbb{Q}$ est encore archimédienne, donc par le théorème d'Ostrowski (13.30), c'est (à équivalence près) la valeur absolue usuelle sur $\mathbb{Q}$. Or K est complet donc le complété métrique de $\mathbb{Q}$ pour la valeur absolue usuelle, c'est à dire $\mathbb{R}$, se plonge dans K par propriété universelle du complété métrique. On peut donc supposer $\mathbb{R} \subseteq K$ avec la valeur absolue de K qui prolonge la valeur absolue usuelle sur $\mathbb{R}$ (toujours à équivalence près). Ainsi K est un $\mathbb{R}$-espace vectoriel normé localement compact, donc par le théorème de Riesz, K

est de dimension finie sur $\mathbb{R}$. C'est donc une extension finie de $\mathbb{R}$, c'est à dire $\mathbb{R}$ ou $\mathbb{C}$, et l'isomorphisme est compatible avec la valeur absolue puisqu'il n'existe qu'un seul prolongement d'une valeur absolue le long d'une extension finie de corps local (théorème 14.9).
Il est clair que $\mathbb{R}$ et $\mathbb{C}$ sont des corps locaux archimédiens. □

Pour étudier les corps locaux non archimédiens, on a besoin d'un outil fondamental en analyse non archimédienne : le lemme de Hensel.

14.3 Lemme de Hensel

On fixe K un corps non archimédien complet. Le lemme de Hensel est un analogue en analyse non archimédienne de la méthode de Newton qui permet d'approcher les zéros d'une fonction en analyse réelle.

Théorème 14.11. *(Lemme de Hensel) Soit $f \in \mathcal{O}_K[X]$ et $\alpha \in \mathcal{O}_K$ tel que :*

$$|f(\alpha)| < \left|f'(\alpha)\right|^2$$

Alors il existe un unique $\beta \in \mathcal{O}_K$ tel que :

$$f(\beta) = 0$$

et :

$$\left|\alpha - \beta\right| < \left|\frac{f(\alpha)}{f'(\alpha)}\right|.$$

De plus, cet élément vérifie $\left|f'(\beta)\right| = |f'(\alpha)|$.

Démonstration. On imite la méthode de Newton. Pour cela on pose $x_0 = \alpha$ et lorsque c'est bien défini :

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

On pose :

$$M = \left|\frac{f(\alpha)}{f'(\alpha)^2}\right| < 1$$

et on va montrer récursivement que la suite (x_n) est bien définie, à valeurs dans $\mathcal{O}_K$, et qu'elle vérifie :

$$|f(x_n)| \leq M^{2^n} \left|f'(\alpha)\right|^2$$

et :

$$|x_{n+1} - x_n| \leq M^{2^n} \left|f'(\alpha)\right|$$

ainsi que :

$$\left|f'(x_n)\right| = \left|f'(\alpha)\right|.$$

D'abord on a bien $|f(x_0)| \leq M^{2^0} |f'(\alpha)|^2$. Supposons $x_0, \ldots, x_n$ construits et vérifiant ce qu'on veut. Puisque $|f'(x_n)| = |f'(\alpha)| > 0$, x_{n+1} est bien défini. On a ensuite :

$$|x_{n+1} - x_n| = |f(x_n)| / \left|f'(x_n)\right| \leq M^{2^n} \left|f'(\alpha)\right|^2 / \left|f'(\alpha)\right| \leq M^{2^n} \left|f'(\alpha)\right| \leq 1$$

et en particulier $|x_{n+1}| \leq 1$ par inégalité ultramétrique donc $x_{n+1} \in \mathcal{O}_K$. La formule de Taylor permet ensuite d'écrire :

$$f(x_{n+1}) = f(x_n) + f'(x_n)(x_{n+1} - x_n) + g(x_{n+1} - x_n) \cdot (x_{n+1} - x_n)^2$$

avec g un polynôme à coefficients dans $\mathcal{O}_K$. Notons que cela est toujours possible même en caractéristique positive. On a donc :

$$f(x_{n+1}) = g(x_{n+1} - x_n) \cdot (x_{n+1} - x_n)^2$$

et par inégalité ultramétrique :

$$|f(x_{n+1})| \leq 1 \cdot M^{2^{n+1}} \left|f'(\alpha)\right|^2 \leq M^{2^{n+1}} \left|f'(\alpha)\right|$$

car $g \in \mathcal{O}_K[X]$ et $f'(\alpha) \in \mathcal{O}_K$. Enfin il reste à voir que $|f'(x_{n+1})| = |f'(\alpha)|$. On écrit :

$$f'(x_{n+1}) = f'(x_n) + (x_{n+1} - x_n)h(x_n)$$

avec $h \in \mathcal{O}_K[X]$. On a alors $|(x_{n+1} - x_n)h(x_n)| \leq M^{2^n} |f'(\alpha)| < |f'(\alpha)|$ car $M < 1$. Par le cas d'égalité de l'inégalité ultramétrique on a donc bien :

$$\left|f'(x_{n+1})\right| = \left|f'(x_n)\right| = \left|f'(\alpha)\right|.$$

La suite (x_n) est de Cauchy dans K puisque $x_{n+1} - x_n \longrightarrow 0$ et K est non archimédien (voir 13.27), et K étant complet, elle converge vers un $\beta \in \mathcal{O}_K$ car $\mathcal{O}_K$ est fermé dans K. En passant à la limite les différentes inégalités et égalités obtenues et par continuité de f et f', on obtient $f(\beta) = 0$, $\left|\alpha - \beta\right| < \left|\frac{f(\alpha)}{f'(\alpha)}\right|$ car les boules ouvertes sont fermées (voir 13.24) et $\left|f'(\beta)\right| = |f'(\alpha)|$.

Il reste à montrer l'unicité. Soit $\gamma \in \mathcal{O}_K$ une racine de f telle que $\left|\alpha - \gamma\right| < |f'(\alpha)|$. On a donc $\left|\beta - \gamma\right| < |f'(\alpha)|$, or :

$$f(\gamma) = f(\beta) + f'(\beta)(\gamma - \beta) + (\gamma - \beta)^2 p(\gamma - \beta)$$

avec $p \in \mathcal{O}_K[X]$ donc, si $\gamma \neq \beta$, on a :

$$\left|f'(\beta)\right| = \left|\gamma - \beta\right| \times \left|p(\gamma - \beta)\right| \leq \left|\gamma - \beta\right| < \left|f'(\alpha)\right|$$

ce qui contredit $\left|f'(\beta)\right| = |f'(\alpha)|$.

□

La plupart du temps on retiendra ce corollaire qui permet de remonter des racines de polynôme du corps résiduel au corps K.

Corollaire 14.12. *Soit $f \in \mathcal{O}_K[X]$ et $\alpha \in \kappa_K$ une racine simple de $\overline{f} \in \kappa_K[X]$. Alors il existe un unique $\beta \in \mathcal{O}_K$ tel que $\overline{\beta} = \alpha$ et $f(\beta) = 0$.*

Démonstration. On choisit x un représentant de α, et on a $f(x) \in \mathfrak{m}_K$ donc $|f(x)| < 1$ et $f'(x) \in \mathcal{O}_K \setminus \mathfrak{m}_K$ car α est une racine simple de $\overline{f}$ donc on a $|f'(x)| = 1$. On est bien dans les conditions du lemme de Hensel (14.11) et la conclusion du lemme de Hensel donne bien ce que l'on souhaite ici. □

14.4 Corps locaux non archimédiens

On cherche ici à classifier les corps locaux non archimédiens.

Proposition 14.13. *Soit K un corps local non archimédien. Les parties $\mathcal{O}_K$, $\mathfrak{m}_K$ et $\mathcal{O}_K^\times$ sont compactes. De plus K est à valeur absolue discrète (voir 13.23).*

Démonstration. Ces trois parties sont compactes car fermées et bornées dans un corps local. Ensuite, si $|x_n| \longrightarrow \ell > 0$, alors (x_n) est bornée dans K local donc quitte à extraire on peut supposer qu'elle converge vers un élément x de valeur absolue ℓ, et par 13.24 on a $|x_n| = \ell$ à partir d'un certain rang, donc la suite des valeurs absolues stationne. □

On dispose d'une caractérisation intéréssante des corps non archimédiens locaux parmi les corps complets à valeur absolue discrète.

Théorème 14.14. *Soit K un corps non archimédien complet et à valeur absolue discrète. Alors K est local si et seulement si κ_K est un corps fini.*

Démonstration. Supposons que K est local. Alors le quotient $\kappa_K = \mathcal{O}_K/\mathfrak{m}_K$ est compact comme image par une application continue d'un compact dans un espace séparé (car $\mathfrak{m}$ est fermé dans $\mathcal{O}_K$), et ce quotient est aussi *discret* car pour tout $x \in \mathcal{O}_K$, $x + \mathfrak{m}_K$ est un voisinage ouvert de x dans $\mathcal{O}_K$, et donc $\{\overline{x}\}$ est ouvert dans κ_K. Ainsi κ_K est compact et discret donc fini.

Réciproquement, on suppose κ_K fini. Puisque K est complet et $\mathcal{O}_K$ est fermé dans K, $\mathcal{O}_K$ est complet. Pour montrer que $\mathcal{O}_K$ est compact, il suffit donc de montrer que pour tout $\varepsilon > 0$ il peut être recouvert par un nombre fini de boules de rayon ε. Pour cela, il suffit de constater que $\mathcal{O}_K/\mathfrak{m}_K^n$ est fini pour tout $n \geq 1$ car, K étant à valeur absolue discrète, les $\mathfrak{m}_K^n$ forment une base de voisinage de 0. Or d'après 3.20, on a :

$$\left|\mathcal{O}_K/\mathfrak{m}_K^n\right| = |\kappa_K|^n < \infty.$$

□

Exemple 14.15. En particulier le corps $\mathbb{Q}_p$ est local pour tout p premier car son corps résiduel $\mathbb{F}_p$ est fini.
De même, si k est un corps fini, toute complétion de $k(T)$ en une place est un corps local. En effet, si v est une place, il suffit de vérifier que le corps résiduel $\mathcal{O}_v/\mathfrak{m}_v$ est fini (car le corps résiduel est le même avant et après complétion d'après 13.26). Pour p un polynôme irréductible unitaire, on a $\mathcal{O}_v = k[T]_{(p)}$ et $\mathcal{O}_v/\mathfrak{m}_v = k[T]_{(p)}/(p)_{(p)} = k[T]/(p)$ qui est une extension finie de k. Quant à la place à l'infini, on peut l'envoyer sur la place associée à T via l'automorphisme de corps $f \mapsto f(1/T)$ de $k(T)$ donc son corps résiduel est k.
D'après le théorème 14.9, les extensions finies de ces corps-ci sont aussi des corps locaux.

Le corollaire du lemme de Hensel (voir 14.12) a une application intéréssante pour les corps locaux non archimédiens.

Théorème 14.16. *Soit K un corps local non archimédien, on note q le cardinal du corps résiduel κ_K (fini d'après 14.14) et π une uniformisante (i.e. un générateur de $\mathfrak{m}_K$). Le polynôme $X^q - X$ est alors scindé à racines simples dans $\mathcal{O}_K$, et on note $\mathbb{F}$ l'ensemble de ses racines. On a ainsi $\mathbb{F} = \mathbb{U}_{q-1}(K) \cup \{0\}$ et le produit direct interne suivant :*

$$K^\times = \pi^{\mathbb{Z}} \odot \mathcal{O}_K^\times = \pi^{\mathbb{Z}} \odot \mathbb{U}_{q-1}(K) \odot (1+\mathfrak{m}) \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times (1+\mathfrak{m}).$$

Démonstration. Notons $f = X^q - X$ de sorte que $\overline{f}$ est scindé à q racines simples dans $\kappa_K = \mathbb{F}_q$. Par le corollaire du lemme de Hensel 14.12, ces q racines induisent q racines distinctes de f dans $\mathcal{O}_K$. Ainsi $X^q - X$ est scindé à racines simples et $\mathbb{F}$ est de cardinal q. Les racines non nulles sont exactement les racines de $X^{q-1} - 1$ donc il y a $q-1$ racines $q-1$-èmes de l'unité dans K. On a clairement :

$$K^\times = \pi^{\mathbb{Z}} \odot \mathcal{O}_K^\times$$

car tout élément de $K^\times$ s'écrit de façon unique $\pi^n u$ avec u inversible. De plus, la réduction modulo $\mathfrak{m}$ donne un isomorphisme :

$$\mathbb{U}_{q-1}(K) \longrightarrow \kappa_K^\times$$

surjectif par construction et bijectif pour cause de cardinalité. Or le noyau de $\mathcal{O}_K^\times \longrightarrow \kappa_K^\times$ est $1+\mathfrak{m}$ donc :

$$\mathcal{O}_K^\times = (1+\mathfrak{m}) \odot \mathbb{U}_{q-1}(K).$$

□

Dans le cas où K est de caractéristique non nulle, l'ensemble $\mathbb{F}$ est un sous-corps de K. Ainsi dans cette situation le corps résiduel peut-être vu comme un sous-corps de K.

Corollaire 14.17. *Soit K un corps local de caractéristique non nulle. Alors $\mathbb{F} = \{x \in K \mid x^q = x\}$ est un sous-corps de K isomorphe au corps résiduel κ_K.*

Démonstration. D'abord K est non archimédien car de caractéristique non nulle. Il suffit ensuite de constater que K et κ_K sont nécessairement de même caractéristique et que $\mathbb{F}$ est stable par somme puisque $x \mapsto x^q$ est additive. □

Chaque élément d'un corps local non archimédien admet un *développement hensélien*, au sens suivant.

Proposition 14.18. *(Développement Henselien) Soit K un corps local non archimédien, et $\mathcal{R}$ un système de représentants du corps fini κ_K de cardinal q (par exemple on peut prendre $\mathcal{R} = \mathbb{F}$). Soit π une uniformisante. On a alors une bijection ensembliste :*

$$\kappa_K((T)) \longrightarrow K$$

qui envoie $\sum_{k \geq n} a_k T^k$ sur $\sum_{k \geq n} s(a_k)\pi^k$ (la série convergeant absolument), en notant $s(a)$ le représentant de a dans $\mathcal{R}$.
De plus, en notant $|\bullet|$ la valeur absolue sur $\kappa_K((T))$ définie comme la complétion de la valeur absolue $|f| = q^{-v_T(f)}$ sur $\kappa_K(T)$, on a , pour tout $f \in \kappa_K(T)$:

$$|\Phi(f)| = |f|^\alpha$$

pour un $\alpha > 0$.

Démonstration. On note Φ cette application. Montrons d'abord que Φ est bien définie. Soit $\sum_{k\geq n} a_k T^k \in \kappa_K((T))$, la série $\sum_{k\geq n} s(a_k)\pi^k$ converge *absolument* car $\mathcal{R}$ est un ensemble fini donc borné et $|\pi| < 1$. Puisque K est complet, cette série converge.

Montrons que Φ est injective. On suppose que $\Phi(\sum_{k\geq n} a_k T^k) = \Phi(\sum_{k\geq n} b_k T^k)$, on a donc :

$$\sum_{k\geq n} (s(a_k) - s(b_k))\pi^k = 0.$$

On suppose par l'absurde que les séries $\sum_{k\geq n} a_k T^k$ et $\sum_{k\geq n} a_k T^k$ sont distinctes, il existe donc un entier N minimal tel que $a_N \neq b_N$. Ainsi on a :

$$\sum_{k\geq N+1} (s(a_k) - s(b_k))\pi^k = (s(b_N) - s(a_N))\pi^N$$

On en déduit :

$$|s(b_N) - s(a_N)| \leq \sup_{k\geq N+1} \left|\pi^{k-N}\right| \leq |\pi|$$

car $s(a_k) - s(b_k) \in \mathcal{O}_K$ et par inégalité ultramétrique. On a donc :

$$|s(b_N) - s(a_N)| < 1$$

et par conséquent $b_N = a_N$ dans le corps résiduel, ce qui est absurde.

Enfin, montrons que Φ est surjective. Soit $x \in K$. Quitte à multiplier par π^n avec n assez grand, on se ramène facilement au cas où $x \in \mathcal{O}_K$. On pose alors :

$$x_0 = x$$

et pour tout n :

$$x_{n+1} = \frac{x_n - s(\overline{x_n})}{\pi} \in \mathcal{O}_K$$

car $x_n - s(\overline{x_n}) \in \mathfrak{m}_K$. On a donc pour tout n :

$$x = \sum_{k=0}^{n} (\pi^k x_k - \pi^{k+1} x_{k+1}) + \pi^{n+1} x_{n+1} = \sum_{k=0}^{n} s(\overline{x_k})\pi^k + \pi^{n+1} x_{n+1}$$

Or $\left|\pi^{n+1} x_{n+1}\right| \leq |\pi|^{n+1} \longrightarrow 0$ donc :

$$x = \sum_{k\geq 0} s(\overline{x_k})\pi^k \in \Phi(\kappa_K((T))).$$

Montrons la dernière égalité, pour $f = \sum_{k\geq n} a_k T^k$ avec $a_n \neq 0$:

$$\left|\sum_{k\geq n} s(a_k)\pi^k\right| = |s(a_n)| \cdot |\pi^n|$$

par le cas d'égalité ultramétrique (car $a_n \neq 0$ donc $|s(a_n)| = 1$). On a ainsi :

$$|\Phi(f)| = |\pi|^{v_T(f)} = |f|^\alpha$$

pour un $\alpha > 0$.

□

Remarque 14.19. En général, Φ n'est pas un isomorphisme : en effet, $\kappa_K((T))$ est un corps de caractéristique non nulle alors que K peut être de caractéristique nulle. Cela vient du fait que les additions dans K se font avec *retenues* dans le développement henselien. En revanche, comme le stipule le théorème suivant, c'est un isomorphisme lorsque K est de caractéristique non nulle.

Théorème 14.20. *(Classification des corps locaux non archimédiens) Soit K un corps local non archimédien. On note q le cardinal du corps résiduel.*
Si K est de caractéristique nulle, alors K est une extension finie d'un certain $\mathbb{Q}_p$ avec p la caractéristique du corps résiduel de K à équivalence de valeurs absolues près.
Sinon, K est isomorphe à $\kappa_K((T))$, le complété de $\kappa_K(T)$ avec la valeur absolue $|f| = q(-v_T(f))$ à équivalence de valeurs absolues près.
Réciproquement, comme vu dans l'exemple 14.15, ces corps-ci sont tous des corps locaux non-archimédiens.

Démonstration. Si K est de caractéristique 0, il contient $\mathbb{Q}$ et la valeur absolue de K resteinte à $\mathbb{Q}$ est non triviale (si elle est triviale, on a $\mathbb{Q} \subseteq \mathcal{O}_K$ et $\mathbb{Q}$ est fermé dans $\mathcal{O}_K$ car il est complet pour la valeur absolue triviale donc il est compact, or $\mathbb{Q}$ avec la topologie discrète n'est pas compact), et non archimédienne donc par le théorème d'Ostrowski (13.30) on peut supposer que c'est la valeur absolue p-adique pour p un nombre premier puisqu'on travaille à équivalence de valeurs absolues près. Par propriété universelle du complété, le corps $\mathbb{Q}_p$ se plonge dans K en respectant la valeur absolue, et K est alors un $\mathbb{Q}_p$-espace vectoriel localement compact, or $\mathbb{Q}_p$ est un corps local (par 14.14), donc par le théorème de Riesz K est de dimension finie sur $\mathbb{Q}_p$.

Si K est de caractéristique p, on a une bijection :

$$\kappa_K((T)) \xrightarrow{\Phi} K$$

en choisissant le corps $\mathbb{F}$ comme système de représentants de κ_K, d'après 14.18. Il reste à prouver que c'est un isomorphisme de corps valués (à équivalence de valeurs absolues près).
L'application Φ est *additive* car $\mathbb{F}$ est stable par somme, et un calcul montre qu'elle est multiplicative, car $\mathbb{F}$ est stable par somme et produit. Enfin on a clairement $\Phi(1) = 1$. Ainsi Φ est un isomorphisme de corps, et Φ préserve la valeur absolue à équivalence près d'après 14.18. □

Mentionnons enfin qu'en caractéristique 0, le groupe apparaissant dans le théorème 14.16, $1 + \mathfrak{m}_K$, est en fait isomorphe au groupe additif $\mathcal{O}_K$. Pour le voir, on a besoin de définir le logarithme et l'exponentielle.

Définition 14.21. *Soit K un corps valué non archimédien complet contenant $\mathbb{Q}_p$ et dont la valeur absolue étend celle de $\mathbb{Q}_p$.*
Étant donnée $f \in K[[T]]$ une série formelle, $f = \sum_{n\geq 0} a_n T^n$, on définit son rayon de convergence $R \in [0, +\infty]$ comme la borne supérieure de l'ensemble des $r > 0$ tels que pour tout $x \in K$, avec $|x| < r$, on a $a_n x^n \longrightarrow 0$.
Comme en analyse réelle ou complexe, f définit alors, par convergence normale sur tout compact, une fonction continue sur la boule ouverte $B(0, R)$, et on a les mêmes résultats

qu'en analyse réelle concernant la somme, le produit et la composition de telles fonctions (ils sont même plus faciles à démontrer en analyse non-archimédienne car l'inégalité ultramétrique est plus forte).
Par exemple, si $a_n \in \mathcal{O}_K$, le rayon de convergence est au moins égal à 1 car si $|x| < 1$, alors $|a_n x^n| \leq |x|^n \longrightarrow 0$.

Proposition 14.22. *Soit K un corps valué non archimédien complet contenant $\mathbb{Q}_p$ et dont la valeur absolue étend celle de $\mathbb{Q}_p$. Comme d'habitude, on pose :*

$$\exp = \sum_{n\geq 0} \frac{T^n}{n!}$$

et

$$\log(1+T) = \sum_{n\geq 1} (-1)^{n+1} \frac{T^n}{n}.$$

Ce sont des séries entières à coefficients rationnels, donc à coefficients dans K, et exp *a pour rayon de convergence :*

$$R_{\exp} = p^{\frac{1}{1-p}} < 1$$

tandis que $\log(1+T)$ *a pour rayon de convergence :*

$$R_{\log(1+T)} = 1.$$

De plus, si $|x| < R_{\exp}$, alors $|\log(1+x)| = |x|$ et :

$$\exp(\log(1+x)) = 1+x$$

et on a $|\exp(x) - 1| < 1$ et :

$$\log(\exp(x)) = x.$$

Démonstration. Soit $x \in K$. On a :

$$\left|\frac{x^n}{n!}\right| = \frac{|x|^n}{p^{-v_p(n!)}} = p^{n\ell + v_p(n!)}$$

avec $\ell = \log_p |x|$. On retrouve rapidement la formule de Legendre :

$$v_p(n!) = \sum_{i=1}^{n} v_p(i) = \sum_{i=1}^{n} \sum_{k\geq 1,\ p^k | i} 1 = \sum_{k\geq 1} \sum_{1\leq i\leq n,\ p^k | i} 1 = \sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k\geq 1} \frac{n}{p^k} \leq \frac{n}{p-1}.$$

Asymptotiquement, on a :

$$v_p(n!) = \sum_{k\geq 1} \frac{n}{p^k} + O\left(\sum_{k\geq 1,\ p^k \leq n} 1 \right) = \frac{n}{p-1} + O(\log_p n) \sim \frac{n}{p-1}.$$

On a $|x| < R_{\exp}$ si et seulement si :

$$n\ell + v_p(n!) \longrightarrow -\infty.$$

Or on a :

$$n\ell + v_p(n!) = n\left(\ell + \frac{1}{p-1}\right) + o(n).$$

Ainsi on veut $\ell < -\frac{1}{p-1}$ et donc :

$$R_{\exp} = p^{\frac{1}{1-p}}.$$

Ensuite, on a :

$$\left|\frac{x^n}{n}(-1)^{n+1}\right| = p^{n\ell - v_p(n)}$$

de sorte que $|x| < R_{\log(1+T)}$ si et seulement si :

$$n\ell - v_p(n) \longrightarrow -\infty.$$

Or $v_p(n) \leq \log_p(n)$ donc $n\ell - v_p(n) = n\ell + O(\log_p(n))$ donc la condition (si $\ell \neq 0$) est $\ell < 0$ et ainsi :

$$R_{\log(1+T)} = 1.$$

Supposons à présent $|x| < R_{\exp}$, de sorte que :

$$\ell = \log_p |x| < -\frac{1}{p-1}.$$

Ainsi :

$$\frac{|x|^n}{|n|} = p^{n\ell + v_p(n)} \leq p^{n\ell + \log_p(n)} \leq np^{n\ell}.$$

On a :

$$\frac{d}{dx}\left(\log_p(x) + x\ell\right) = \frac{1}{x\log(p)} + \ell$$

qui s'annule en $\frac{-1}{\ell\log(p)}$, est positif avant et négatif après. Ainsi $\log_p(x) + x\ell$ a un maximum pour $x_0 = \frac{-1}{\ell\log(p)}$ et on a :

$$x_0 < \frac{p-1}{\log(p)} \leq p$$

car :

$$\frac{d}{dx}\left(x\log(x) - (x-1)\right) = \log(x)$$

de sorte que $x\log(x) - (x-1)$ a un minimum en $x = 1$ et $x\log(x) - (x-1) \geq 0$, d'où l'inégalité voulue pour $x \geq 2$. Puisque le maximum de $\log_p(x) + x\ell$ est atteint strictement avant p, on en déduit pour $n > p$:

$$\frac{|x|^n}{|n|} \leq p^{\log_p(p) + p\ell} = \frac{|x|^p}{|p|} < |x|.$$

De plus, si $n < p$ on a $v_p(n) = 0$ et donc :

$$\frac{|x|^n}{|n|} = |x|^n < |x|.$$

Ainsi on a, par le cas d'égalité de l'inégalité ultramétrique :

$$|\log(1+x)| = |x| < R_{\exp}$$

L'égalité $\exp(\log(1+x)) = 1+x$ est vraie formellement et se déduit pour $|x| < R_{\exp}$ par manipulations de séries absolument convergentes.
De même, on montre que $|e^x - 1| < 1$ en constatant que pour $n \geq 1$:

$$\frac{|x^n|}{|n!|} \leq p^{n\ell + \frac{n}{p-1}} < 1$$

en utilisant la formule de Legendre. Encore une fois, l'égalité $\log(\exp(x)) = x$ est formelle. □

Corollaire 14.23. *Soit K comme ci-dessus. Pour tout $r > 0$ suffisament petit, on a :*

$$\exp(B(0,r)) = 1 + B(0,r)$$

et l'exponentielle et le logarithme fournissent des isomorphismes de groupes topologiques entre le groupe multiplicatif $1 + B(0,r)$ et le groupe additif $B(0,r)$.
Ici la notation $B(0,r)$ peut aussi bien désigner la boule ouverte que la boule fermée (en gardant la cohérence le long de l'énoncé).

Démonstration. Par continuité de exp sur son domaine de convergence, il existe $R > 0$ assez petit pour que :

$$\exp(B(0,R)) \subseteq B(1, R_{\exp})$$

avec la notation $B(x,R)$ pour la boule ouverte centrée en x de rayon R. Or, pour tout $x \in B(0,R)$, on a :

$$|x| = |\log(e^x)| = |e^x - 1|$$

d'après la proposition précédente. On a donc, pour tout $r > 0$ strictement plus petit que R :

$$\exp(B(0,r)) \subseteq B(1,r)$$

que l'on considère des boules ouvertes ou fermées. Réciproquement, si $x \in B(1,r)$, on a :

$$x = \exp(\log(x))$$

et $|\log(x)| = |x-1|$, donc finalement :

$$\exp(B(0,r)) = B(1,r)$$

et le fait que exp soit un morphisme vient du fait que :

$$e^{a+b} = e^a e^b$$

pour tous a, b dans le domaine de convergence, ce qui s'obtient comme en analyse réelle par manipulation de sommes absolument convergentes. □

On en déduit la proposition suivante pour les corps locaux non archimédiens de caractéristique nulle.

Proposition 14.24. *Soit K une extension finie de $\mathbb{Q}_p$ (dont la valeur absolue étend celle de $\mathbb{Q}_p$) et n un entier suffisament grand. Alors l'exponentielle et le logarithme donnent un isomorphisme de groupes topologiques :*

$$1 + \mathfrak{m}_K^n \cong \mathfrak{m}_K^n \cong \mathcal{O}_K$$

et on a $\exp\left(\mathfrak{m}_K^n\right) = 1 + \mathfrak{m}_K^n$.
Si $K = \mathbb{Q}_p$ et p est impair, c'est valable pour $n = 1$ et ainsi :

$$1 + p\mathbb{Z}_p \cong \mathbb{Z}_p.$$

Démonstration. Cela découle directement du corollaire.
Dans le cas particulier où $K = \mathbb{Q}_p$ avec p impair, on constate déjà que :

$$R_{\exp} = p^{\frac{-1}{p-1}} > |p|$$

car $p \geq 3$. Ainsi l'exponentielle est bien définie sur $p\mathbb{Z}_p$ et on a :

$$\exp(p\mathbb{Z}_p) \subseteq 1 + p\mathbb{Z}_p$$

car pour tout $k \geq 1$ et tout $x \in {}_{|}Z_p$:

$$v_p(x^k) - v_p(k!) \geq k v_p(x) - \frac{k}{p-1} \geq k\frac{p-2}{p-1} > 0$$

donc $\frac{x^k}{k!} \in p\mathbb{Z}_p$ et $\exp(x) \in 1 + p\mathbb{Z}_p$. On a alors :

$$\exp(p\mathbb{Z}_p) = 1 + p\mathbb{Z}_p$$

car si $x \in p\mathbb{Z}_p$, on a $\log(1 + x) \in p\mathbb{Z}_p$ car $\log(1 + T)$ préserve la valeur absolue si elle est strictement inférieure à $R_{\exp}$. □

14.5 Extensions finies de corps locaux non archimédiens

14.5.1 Généralités

Soit L/K une extension *finie séparable* de corps locaux non archimédiens. En vertu du théorème 14.9, la valeur absolue sur L est entièrement déterminée par celle de K. Clairement $\mathcal{O}_K \subseteq \mathcal{O}_L$ et $\mathfrak{m}_K \subseteq \mathfrak{m}_L$ donc on a une extension des corps résiduels :

$$\mathcal{O}_K/\mathfrak{m}_K \subseteq \mathcal{O}_L/\mathfrak{m}_L.$$

On note ℓ/k cette extension des corps résiduels (qui sont des corps finis).
La proposition suivante fait le lien avec la théorie des anneaux de Dedekind.

Proposition 14.25. *Soit L/K une extension finie séparable de corps locaux non archimédiens. Alors $\mathcal{O}_L/\mathcal{O}_K$ est une extension de Dedekind de corps des fractions L/K. En particulier, puisque $\mathcal{O}_K$ est un anneau de valuation discrète, $\mathcal{O}_L$ est un $\mathcal{O}_K$-réseau de L, et donc un $\mathcal{O}_K$-module libre de rang $[L : K]$.*

Démonstration. La seule chose à montrer est que $\mathcal{O}_L$ est la clôture intégrale de $\mathcal{O}_K$ dans L. On note d le degré de l'extension L/K. Prenons (e_i) une K-base de L, quitte à multiplier par une uniformisante, on peut suppoer $e_i \in \mathcal{O}_L$. On note $\|\bullet\|_\infty$ la norme infinie associée à cette base sur L. La boule unité fermée pour cette norme est :

$$B = \bigoplus_i \mathcal{O}_K e_i$$

qui est contenue dans $\mathcal{O}_L$. Par le théorème d'équivalence des normes sur un K-espace vectoriel de dimension finie avec K complet (voir 14.5), B contient une boule centrée en 0 pour $|\bullet|_L$, donc on a :

$$\pi^n \mathcal{O}_L \subseteq B$$

pour un certain n, avec π une uniformisante de L. Ainsi :

$$\bigoplus_i \mathcal{O}_K e_i \subseteq \mathcal{O}_L \subseteq \bigoplus_i \mathcal{O}_K \pi^{-n} e_i$$

ce qui montre que $\mathcal{O}_L$ est fini sur $\mathcal{O}_K$ car $\mathcal{O}_K$ est noéthérien, et ainsi $\mathcal{O}_L$ est contenu dans la clôture intégrale de $\mathcal{O}_K$ dans L. Or $\mathcal{O}_L$ est intégralement clos donc tout élément de L entier sur $\mathcal{O}_K$ est aussi dans $\mathcal{O}_L$. □

Puisque $\mathcal{O}_K$ et $\mathcal{O}_L$ ont un seul idéal maximal, on notera $e(L \mid K)$ et $f(L \mid K)$ pour $e(\mathfrak{m}_L \mid \mathfrak{m}_K)$ et $f(\mathfrak{m}_L \mid \mathfrak{m}_K)$. Ainsi $f(L \mid K) = [\ell : k]$. Notons que $\mathcal{O}_K$ est localement fini et donc localement parfait au sens de 5.38 puisque k est un corps fini. La formule des degrés 5.17 donne alors :

$$[L : K] = e(L \mid K) f(L \mid K).$$

La proposition suivante donne une interprétation de $e(L \mid K)$ en termes des valeurs absolues sur K et L.

Proposition 14.26. *Le groupe $|K^\times|$ est d'indice fini dans $|L^\times|$, et cet indice est exactement l'indice de ramification $e(L \mid K)$.*
En d'autres termes, si π_L est une uniformisante de L et π_K est une uniformisante de K, on a :

$$|\pi_K| = |\pi_L|^{e(L|K)}.$$

Démonstration. Clairement $|K^\times|$ est d'indice fini dans $|L^\times|$ car ce sont deux groupes monogènes non triviaux. Par définition de l'indice de ramification, on a :

$$\mathfrak{m}_K \mathcal{O}_L = \mathfrak{m}_L^{e(L|K)}$$

et en prenant des uniformisantes comme dans l'énoncé, cela se réécrit :

$$\pi_K \mathcal{O}_L = \pi_L^{e(L|K)} \mathcal{O}_L$$

et donc $\pi_K \pi_L^{-e(L|K)}$ est inversible dans $\mathcal{O}_L$, autrement dit :

$$|\pi_K| = |\pi_L|^{e(L|K)}.$$

Or $|\pi_K|$ et $|\pi_L|$ engendrent respectivement $|K^\times|$ et $|L^\times|$, donc :

$$\left|L^\times\right| / \left|K^\times\right| \cong \mathbb{Z}/e(L \mid K)\mathbb{Z}$$

ce qui conclut. □

Définition 14.27. *Une extension finie séparable L/K de corps locaux non archimédiens est non ramifiée si $e(L \mid K) = 1$ (ou de façon équivalente si $f(L \mid K) = [L : K]$) et elle est totalement ramifiée si $e(L \mid K) = [L : K]$ (ou de façon équivalente si $f(L \mid K) = 1$, i.e. $\ell = k$). De plus, L/K est dite modérément ramifiée si $e(L \mid K)$ est premier à la caractéristique de k et sauvagement ramifiée dans le cas contraire (on avait déjà rencontré ce concept dans 9.7).*

Si L/K est une extension finie *galoisienne* de corps locaux non archimédiens de groupe G, puisque $\mathfrak{m}_K$ n'a qu'un seul premier au dessus de lui, à savoir $\mathfrak{m}_L$, le groupe de décomposition $D(\mathfrak{m}_L \mid \mathfrak{m}_K)$ est égal à G : tout élément de G stabilise $\mathfrak{m}_L$. On note $E(L \mid K)$ le groupe d'inertie de $\mathfrak{m}_L$ au dessus de $\mathfrak{m}_K$, et on a alors la suite exacte 7.9 :

$$1 \longrightarrow E(L \mid K) \longrightarrow G \longrightarrow \overline{G} \longrightarrow 1$$

avec $\overline{G} = \mathrm{Gal}(\ell/k)$. Le théorème 7.7 donne la situation suivante :

$$\begin{array}{ccccc}
G & & L & \supseteq & \mathfrak{m}_L \\
{\scriptstyle f}\big| & & {\scriptstyle e}\big| & & {\scriptstyle e}\big\{ \big|{\scriptstyle 1} \\
E & & L^E & \supseteq & \mathfrak{m}_{L^E} \\
{\scriptstyle e}\big| & & {\scriptstyle f}\big| & & {\scriptstyle 1}\big\{ \big|{\scriptstyle f} \\
1 & & K & \supseteq & \mathfrak{m}_K
\end{array}$$

avec $E = E(L \mid K)$, avec une vague pour l'indice de ramification et un trait droit pour l'indice d'inertie. Ainsi L est une extension totalement ramifiée d'une extension non ramifiée de K, et on verra plus tard 14.39 que c'est vrai même si L/K n'est pas galoisienne. De plus L^E est l'extension non ramifiée maximale de K contenue dans L d'après 7.18.
De plus, pour tout $n \in \mathbb{Z}$ et tout $\sigma \in G$, on a $\sigma(\mathfrak{m}_L^n) = \mathfrak{m}_L^n$ donc σ préserve la valeur absolue : le groupe de Galois G agit donc par *isométries* sur le corps L, et $E(L \mid K)$ est le sous-groupe des $\sigma \in G$ qui vérifient, pour tout $x \in \mathcal{O}_L$:

$$\sigma(x) - x \in \mathfrak{m}_L$$

autrement dit $|\sigma x - x| < 1$. On peut aussi interpréter les groupes de ramification supérieure (voir 9.1) en terme de distance :

$$E_m(L \mid K) = \left\{\sigma \in G \mid \forall x \in \mathcal{O}_L \ |\sigma x - x| \leq |\pi_L|^{m+1}\right\}.$$

Notons que par le corollaire 9.5, le groupe de Galois G est toujours résoluble dans ce contexte.
Enfin, d'après 9.7, la ramification dans L/K est sauvage si et seulement si $E_1(L \mid K) \neq 1$, autrement dit s'il existe $\sigma \in G$ tel que pour tout $x \in \mathcal{O}_L$ on ait $|\sigma x - x| \leq |\pi_L|^2$.

14.5.2 Extensions non ramifiées

On s'intéresse ici aux extensions (finies séparables) non ramifiées de corps locaux non archimédiens. Le résultat clé que l'on va démontrer est le suivant : si K est un corps local non archimédien de corps résiduel k, il y a une équivalence de catégories entre les extensions finies séparables non ramifiées de K et les extensions finies de k. Cela fera l'objet du théorème 14.29.

Lemme 14.28. *Soit K un corps local non archimédien de corps résiduel k et soit ℓ/k une extension finie. Il existe une extension finie séparable non ramifiée L/K telle que le corps résiduel de L soit isomorphe à ℓ comme extension de k.*

Démonstration. Par théorème de l'élément primitif, on peut écrire $\ell = k[\alpha] = k[X]/(\overline{P})$ avec $P \in \mathcal{O}_K[X]$ unitaire tel que $\overline{P}$ est irréductible et séparable. En particulier P est irréductible (dans $K[X]$ ou dans $\mathcal{O}_K[X]$, c'est équivalent d'après 1.29 pour un polynôme unitaire) et séparable. On considère alors :

$$L = K[X]/(P) = K[\beta]$$

qui est une extension finie séparable de K, et β est entier sur $\mathcal{O}_K$ donc $\beta \in \mathcal{O}_L$. Notons $\tilde{\ell}$ le corps résiduel de L. Le polynôme $\overline{P}$ est scindé dans $\tilde{\ell}$ (car $\overline{\beta}$ en est une racine et c'est une extension normale). Ainsi on peut définir un morphisme k-linéaire :

$$\ell \hookrightarrow \tilde{\ell}$$

qui envoie α sur $\overline{\beta}$. On obtient :

$$[\ell : k] \leq [\tilde{\ell} : k] = f(L \mid K) \leq [L : K]$$

mais par construction $[\ell : k] = \deg \overline{P} = \deg P = [L : K]$, donc ces inégalités sont des égalités et ainsi :

$$\ell = \tilde{\ell}$$

et

$$[L : K] = f(L \mid K)$$

donc L/K est non ramifiée. □

Théorème 14.29. *Soit K un corps local non archimédien de corps résiduel k. Notons FSU_K la catégorie des extensions finies séparables non ramifiées (pour finite separable unramified)) de K et F_k la catégorie des extensions finies de k. Alors le foncteur*

$$\mathrm{FSU}_K \longrightarrow \mathrm{F}_k$$

qui à L/K associe l'extension ℓ/k avec ℓ le corps résiduel de L (et dont l'action sur les morphismes est détaillée dans la preuve) est une équivalence de catégories.
Plus précisément, si L et M sont deux extensions finies séparables de K de corps résiduels ℓ et m et si L/K est non ramifiée, alors on a une bijection canonique :

$$\mathrm{Hom}_K(L, M) \cong \mathrm{Hom}_k(\ell, m).$$

Démonstration. Commençons par expliciter ce que fait ce foncteur au niveau des morphismes. Soit $L \xrightarrow{\varphi} M$ un morphisme d'extensions finies séparables non ramifiées de K. Les applications $|\bullet|_M \circ \varphi$ et $|\bullet|_L$ sont deux valeurs absolues sur L qui prolongent la valeur absolue de K. Par unicité on a donc :

$$|\bullet|_M \circ \varphi = |\bullet|_L$$

autrement dit φ est une isométrie (pas nécessairement surjective). En particulier φ envoie $\mathcal{O}_L$ dans $\mathcal{O}_M$ et $\mathfrak{m}_L$ dans $\mathfrak{m}_M$ donc définit un morphisme k-linéaire $\mathcal{O}_L/\mathfrak{m}_L$ vers $\mathcal{O}_M/\mathfrak{m}_M$. On vérifie facilement que cela définit un foncteur. On utilise le théorème 1.6, il s'agit donc de montrer que ce foncteur est pleinement fidèle et essentiellement surjectif sur les objets. Le lemme précédent 14.28 assure que le foncteur est essentiellement surjectif sur les objets, et on montre maintenant la deuxième affirmation de l'énoncé, qui entraîne en particulier que le foncteur est pleinement fidèle : soient L, M deux extensions séparables finies K de corps résiduels respectifs ℓ et m, avec L non ramifiée. Par le théorème de l'élément primitif, on écrit $\ell = k[\alpha]$ et on choisit $\beta \in \mathcal{O}_L$ un représentant de α. On observe alors que :

$$[L : K] \geq [K[\beta] : K] = \deg \pi_\beta \geq \deg \pi_\alpha = [\ell : k]$$

car $\pi_\beta(\alpha) = 0$ et donc $\pi_\alpha \mid \overline{\pi_\beta}$. Or L/K est non ramifiée donc $[\ell : k] = [L : K]$ et donc les deux inégalités sont des égalités :

$$L = K[\beta]$$

et

$$\overline{\pi_\beta} = \pi_\alpha$$

et en particulier π_β est séparable car π_α l'est. On a alors un diagramme commutatif :

$$\begin{array}{ccc} \mathrm{Hom}_K(L, M) & \longrightarrow & \mathrm{Hom}_k(\ell, m) \\ \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \sim} \\ \left\{x \in M \mid \pi_\beta(x) = 0\right\} & \longrightarrow & \{y \in m \mid \pi_\alpha(y) = 0\} \end{array}$$

où la flèche de gauche est donnée par $\varphi \mapsto \varphi(\beta)$ et celle de droite est donnée par $\varphi \mapsto \varphi(\alpha)$. La flèche du bas est une bijection d'après le lemme de Hensel 14.12 car α est une racine simple de π_α. On en déduit que la flèche du haut est une bijection et que le foncteur est pleinement fidèle. □

Corollaire 14.30. *Toute extension non ramifiée (finie séparable) de K (corps local non archimédien) est galoisienne de groupe $G \cong \overline{G}$ puisque l'indice de ramification vaut 1. En particulier une telle extension est cyclique car $\overline{G}$ est cyclique.*

Démonstration. Soient L/K une telle extension, et ℓ/k les corps résiduels. Par l'équivalence de catégories précédente on a :

$$|\mathrm{Aut}_K(L)| = |\mathrm{Aut}_k(\ell)| = [\ell : k] = [L : K]$$

car ℓ/k est galoisienne (ce sont des corps finis) et L/K est non ramifiée. Donc $|\mathrm{Aut}_K(L)| = [L : K]$ et ainsi l'extension est galoisienne. □

14.5.3 Extensions totalement ramifiées

On va à présent étudier l'autre extrême : les extensions totalement ramifiées (finies et séparables) L/K de corps locaux. Dans ce cas les corps résiduels sont égaux :

$$\ell = k.$$

On commence par rappeler la notion de polynôme d'Eisenstein dans le contexte des corps non archimédiens à valeur absolue discrète.

Définition 14.31. *(Polynôme d'Eisenstein) Soit K un corps valué non archimédien à valeur absolue discrète non triviale. Un polynôme $P \in \mathcal{O}_K[X]$ est dit d'Eisenstein s'il est de la forme :*

$$P = a_n X^n + \cdots + a_0$$

avec $a_0, \ldots, a_{n-1} \in \mathfrak{m}_K$, $a_n \notin \mathfrak{m}_K$ et $a_0 \in \mathfrak{m}_K \setminus \mathfrak{m}_K^2$.

Proposition 14.32. *Tout polynôme d'Einsenstein est irréductible.*

Démonstration. On note k le corps résiduel de K. Puisque $\mathcal{O}_K$ est un anneau de valuation discrète, il est factoriel et on peut donc utiliser le critère d'irréductibilité 1.29. Si P est d'Einsenstein, il est primitif car a_n est inversible, et il suffit donc de montrer qu'il est irréductible dans $\mathcal{O}_K[X]$. Notons qu'on a nécessairement $n \geq 1$ pour un tel polynôme. Si $P = QR$ dans $\mathcal{O}_K[X]$ avec Q et R non constants, la réduction dans $k[X]$ donne :

$$\overline{a_n} X^n = \overline{Q}\,\overline{R}$$

donc $\overline{Q}$ et $\overline{R}$ sont des monômes de degrés respectifs q et r avec $q + r = n$. Or les coefficients dominants de Q et R sont inversibles car leur produit est a_n, donc $q = \deg Q$ et $r = \deg R$. Les coefficients de degré 0 et $\overline{Q}$ et $\overline{R}$ sont nuls car $\overline{Q}$ et $\overline{R}$ sont des monômes de degré au moins 1 (on a $q \geq 1$ et $r \geq 1$ car Q et R ne sont pas constants). Ainsi $P(0), Q(0) \in \mathfrak{m}_K$ et :

$$a_0 = P(0) = Q(0)R(0) \in \mathfrak{m}_K^2$$

ce qui est absurde. □

Remarque 14.33. Cette version du critère d'Eisenstein implique facilement la version bien connue : dire que $P \in \mathbb{Z}[X]$ est p-Eisenstein pour un nombre premier p revient à dire qu'il est d'Eisenstein dans le corps local $\mathbb{Q}_p$, et il est donc irréductible dans $\mathbb{Q}_p[X]$, et donc dans $\mathbb{Q}[X]$. On peut aussi généraliser cette observation à tout anneau factoriel.

Les polynômes d'Eisenstein permettent la caractérisation suivante des extensions totalement ramifiées. Dans ce qui suit, la lettre ϖ est un π écrit différemment pour ne pas confondre avec la notation du polynôme minimal.

Théorème 14.34. *Soit K un corps local non archimédien et L/K une extension finie séparable de corps résiduels ℓ/k. Les énoncés suivants sont équivalents :*

(i) *L/K est totalement ramifiée.*

(ii) *Les corps ℓ et k sont égaux.*

(iii) *Il existe $\alpha \in L$ tel que $L = K[\alpha]$ avec π_α un polynôme d'Eisenstein.*

(iv) Toute uniformisante ϖ_L de L engendre L comme extension de K et le polynôme minimal de ϖ_L est d'Eisenstein.

De plus, dans le cas (iii), un tel α est alors une uniformisante de L et pour toute uniformisante ϖ_L, on a :

$$\mathcal{O}_L = \mathcal{O}_K[\varpi_L]$$

.

Démonstration. On fixe M une extension finie galoisienne de L. Il est clair que les points (i) et (ii) sont équivalents.
Voyons $(iii) \implies (i)$: On écrit $\pi_\alpha = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ avec $a_0 \in \mathfrak{m}_K \setminus \mathfrak{m}_K^2$ et $a_1, \ldots, a_{d-1} \in \mathfrak{m}_K$. Le polynôme π_α se scinde dans $M[X]$:

$$\pi_\alpha = \prod_\beta (X - \beta)$$

où le produit porte sur les conjugués de α. Ces conjugués ont tous la même valeur absolue que α car le groupe de Galois de M/K agit par isométries. Ainsi en évaluant en 0 :

$$|a_0| = |\pi_\alpha(0)| = |\alpha|^d$$

avec $d = [L : K]$. Comme π_α est Eisenstein, a_0 est une uniformisante de K, et si ϖ_L est une uniformisante de L, la proposition 14.26 donne :

$$|a_0| = |\varpi_L|^{e(L|K)}$$

ce qui donne, en terme de valuations ϖ_L-adiques :

$$v_{\varpi_L}(a_0) = e(L \mid K) = d v_{\varpi_L}(\alpha).$$

Ainsi $d \mid e(L \mid K) \mid d$ donc $d = e(L \mid K)$, ainsi l'extension est totalement ramifiée, et α est une uniformisante de L car sa valuation ϖ_L- adique vaut 1.
Ensuite voyons $(ii) \implies (iv)$: on suppose $\ell = k$ et on se donne ϖ_L une uniformisante de L et on prend $\mathbb{F}$ le système de représentants de $\ell = k$ décrit dans 14.16. Ainsi $\mathbb{F} \subseteq \mathcal{O}_K$. Soit $x \in \mathcal{O}_L$, le développement hensélien de x (voir 14.18) donne :

$$x = \sum_{n \geq 0} a_n \varpi_L^n$$

avec $a_n \in \mathbb{F}$. En particulier $\mathcal{O}_K[\varpi_L]$ est dense dans $\mathcal{O}_L$, or c'est aussi fermé car c'est un $\mathcal{O}_K$-réseau de $K[\varpi_L]$ (qui est un K-espace vectoriel de dimension finie donc complet). Notons d'ailleurs que tout $\mathcal{O}_K$-réseau d'un K-espace vectoriel de dimension finie est en fait une boule unité fermée (car de la forme $\mathcal{O}_K^n$ quitte à choisir une base) pour une certaine norme (et toutes les normes sont équivalentes par 14.5). On a donc montré :

$$\mathcal{O}_K[\varpi_L] = \mathcal{O}_L$$

et on en déduit aussi $K[\varpi_L] = L$. Il reste à voir que P, le polynôme minimal de ϖ_L, est d'Eisenstein. Or on a :

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

le produit portant sur les conjugués de ϖ_L, et P est de degré $d = [L : K]$ car $K[\varpi_L] = L$. On réduit P dans $k[X] \subseteq m[X]$ avec m le corps résiduel de M :

$$\overline{P} = \prod_{\beta} X = X^d$$

car les β sont tous dans $\mathfrak{m}_M$ puisqu'ils ont la même valeur absolue que ϖ_L. Il reste à voir que $a_0 \notin \mathfrak{m}_K^2$. Pour cela on observe que :

$$|a_0| = |P(0)| = |\varpi_L|^d = |\varpi_L|^{e(L|K)} = |\varpi_K|$$

pour ϖ_K une uniformisante de K, car L/K est totalement ramifiée.
Enfin on a clairement $(iv) \implies (iii)$. □

Dans le cas où la ramification est totale et modérée (au sens où l'indice de ramification est non-nul dans le corps résiduel, voir 9.7), on peut dire mieux : l'extension s'obtient en ajoutant une racine n-ème d'une certaine uniformisante.

Proposition 14.35. *(Extensions totalement modérément ramifiées) Soit L/K une extension finie séparable totalement et modérément ramifiée de corps résiduels $\ell = k$ et de degré n. Il existe alors une uniformisante π de K et une uniformisante $\pi^{1/n}$ de L, qui comme son nom le suggère est une racine n-ème de π, et on a $\mathcal{O}_L = \mathcal{O}_K[\pi^{1/n}]$ et $L = K[\pi^{1/n}]$.*

Démonstration. Commençons par choisir π_L une uniformisante de L et π_K une uniformisante de K. Il existe $u \in \mathcal{O}_L^\times$ tel que $u\pi_L^n = \pi_K$ car $n = e(L \mid K)$ par hypothèse. Quitte à changer π_K, on peut alors supposer $u \equiv 1\ [\pi_L]$ puisque $\ell = k$, l'extension étant totalement ramifiée. En appliquant le lemme de Hensel au polynôme $X^n - u \in \mathcal{O}_L[X]$ dont la réduction à $\ell = k$ est $X^n - 1$ qui est séparable puisque $n \neq 0$ dans k et qui a une racine dans k, on obtient un élément $v \in \mathcal{O}_L$ tel que $v^n = u$. En remplaçant π_L par $v\pi_L$, on peut donc supposer :

$$\pi_L^n = \pi_K$$

et le reste découle du théorème précédent. □

Remarque 14.36. *Dans la proposition précédente, on ne peut pas choisir π et $\pi^{1/n}$ comme on veut. Cependant, si k est algébriquement clos (ou du moins stable par extraction de racines n-èmes), il n'y a plus besoin de supposer $u \equiv 1\ [\pi_L]$ pour trouver une racine à $X^n - u$ dans le corps résiduel, et donc on peut choisir l'uniformisante de K que l'on veut.*

Grâce à cela, nous allons pouvoir déterminer très facilement une clôture algébrique du corps $k((T))$ avec k de caractéristique nulle.

Définition 14.37. *(Séries de Puiseux)*
Soit k un corps. On considère, pour tout n, l'extension $k((T))[T^{1/n}]$ du corps $k((T))$ et on forme la réunion de ces corps, que l'on note $k\langle\langle T\rangle\rangle$. C'est une extension algébrique de $k((T))$, dont les éléments s'appellent séries de Puiseux à coefficients dans k. Notons qu'une série de Puiseux f peut s'écrire de façon unique :

$$f = \sum_{q \in \mathbb{Q}} a_q T^q$$

avec $a_q = 0$ quand q est inférieur à une certaine borne, et avec tous les q tels que $a_q \neq 0$ qui admettent un dénominateur commun.

Théorème 14.38. *(Puiseux)*
Si k est algébriquement clos de caractéristique nulle, le corps $k\langle\langle T\rangle\rangle$ est une clôture algébrique de $k((T))$.
Si k est simplement de caractéristique nulle, alors une clôture algébrique de $k((T))$ est donnée par le corps $\overline{k}\langle\langle T\rangle\rangle'$ qui est le sous-corps de $\overline{k}\langle\langle T\rangle\rangle$ formé des séries de Puiseux $f = \sum a_q T^q$ avec tous les a_q dans une même extension finie de k.

Démonstration. Le premier point découle directement de la proposition et de la remarque précédentes : toutes les extensions finies de $k((T))$ sont modérement totalement ramifiées donc de la forme $k((T^{1/n}))$ et ces extensions sont galoisiennes car k contient les racines n-èmes de l'unité.
À présent, on ne suppose plus k algébriquement clos. Le corps $\overline{k}\langle\langle T\rangle\rangle$ est algébriquement clos et contient $k((T))$ cependant il n'est a priori pas algébrique sur $k((T))$ car $\overline{k}((T))$ n'est a priori pas algébrique sur $k((T))$, le problème étant que les coefficients d'une série de Laurent f sur $\overline{k}$ ne vivent pas nécessairement tous dans une même extension finie de k.
Cependant, l'extension $\overline{k}\langle\langle T\rangle\rangle'/k((T))$ est algébrique car c'est la réunion des $\ell\langle\langle T\rangle\rangle$ avec ℓ/k finie et une telle extension est algébrique sur $\ell((T))$ donc sur $k((T))$.
Soit maintenant $f \in \overline{k}\langle\langle T\rangle\rangle$ algébrique sur $k((T))$. Il s'agit de voir que les coefficients de f vivent tous dans une même extension finie de k. On peut supposer f entier sur $k[[T]]$.
On peut alors écrire :

$$f^n(T) = a_0(T) + a_1(T)f(T) + \cdots + a_{n-1}(T)f^{n-1}(T)$$

avec $a_i \in k[[T]]$. En écrivant $f = \sum_q b_q T^q$ et en traduisant l'égalité précédente sur les b_q, on obtient bien ce qu'on voulait.

□

14.5.4 Cas général

On a classifié les extensions non ramifiées et totalement ramifiées d'un corps local non archimédien, et le théorème suivant montre que cette étude suffit pour comprendre toutes les extensions (finies séparables) d'un tel corps.

Théorème 14.39. *Soit L/K une extension finie séparable de corps locaux non archimédiens. Il existe une unique extension non ramifiée maximale de K contenue dans L, notée K^u. De plus L/K^u est totalement ramifiée.*
Dans le cas où L/K est galoisienne, on a $K^u = L^{E(L|K)}$.

Démonstration. Une telle extension existe, car un compositum d'extensions non ramifiées de K contenues dans L est une extension non ramifiée de K d'après 7.19, et il suffit alors de prendre le compositum de toutes ces extensions. Une telle extension est clairement unique.
Il reste à voir que L/K^u est totalement ramifiée. Notons $\ell/k^u/k$ les corps résiduels $L/K^u/K$. Par l'équivalence de catégories 14.29, il existe F/K une extension non ramifiée séparable dont le corps résiduel s'identifie à ℓ. Puisque F/K est non ramifiée, on a :

$$\mathrm{Hom}_K(F, L) \cong \mathrm{Hom}_k(\ell, \ell)$$

car F et L ont comme corps résiduel ℓ (on utilise le théorème 14.29). Par cette bijection, id_ℓ correspond à un morphisme K-linéaire $F \longrightarrow L$, et ainsi on peut supposer que :

$$K \subseteq F \subseteq L.$$

Comme F/K est non ramifiée, on a $F \subseteq K^u$ et donc $\ell \subseteq k^u \subseteq \ell$, donc $k^u = \ell$. Puisque F et K^u ont le même corps résiduel, d'après l'équivalence de catégories, l'inclusion $F \subseteq K^u$ est une égalité :

$$F = K^u.$$

On en déduit :

$$f(K^u \mid K) = [\ell : k] = f(L : K)$$

et donc $f(L \mid K^u) = 1$: l'extension L/K^u est totalement ramifiée. □

On cherche à présent à démontrer que $\mathbb{Q}_p$ n'a qu'un nombre fini, à isomorphisme près, d'extensions de degré fixé (théorème 14.43). Pour ce qui est des extensions non ramifiées, il y en a une seule de degré fixé, d'après l'équivalence de catégories 14.29, car elles sont en bijection avec les extensions finies du corps fini $\mathbb{F}_p$.
Il reste à traiter le cas des extensions totalement ramifiées pour ensuite conclure avec le théorème précédent. Pour cela, on commence par établir le lemme suivant.

Lemme 14.40. *(Krasner) Soit K un corps local non archimédien et L/K une extension galoisienne de K, sur laquelle on prolonge la valeur absolue de K d'une unique façon (par exemple, en caractéristique 0, on peut prendre une clôture algébrique de K). Soient $a, b \in L$ tels que pour tout conjugué a' de a (par le groupe des automorphismes de L sur K) différent de a on ait :*

$$|b - a| < |b - a'|.$$

Alors $a \in K(b)$.

Démonstration. Notons G le groupe de Galois de L/K et H le groupe de Galois de $L/K(b)$ de sorte que :

$$K(b) = L^H.$$

Il suffit donc de voir que pour tout $\sigma \in L^H$, on a $\sigma a = a$. Mais si $\sigma a \neq a$, on a :

$$|\sigma a - b| > |b - a|$$

et d'autre part :

$$|b - a| = |\sigma b - \sigma a| = |b - \sigma a|$$

car le groupe de Galois agit par isométries (car l'image d'une uniformisante est une uniformisante) et car $\sigma b = b$. Ainsi $|b - a| < |b - a|$: c'est absurde. □

Lemme 14.41. *(Continuité des racines) Soit K un corps valué de caractéristique nulle et $\overline{K}$ une clôture algébrique de K. On munit $K[X]$ de la norme infinie des coefficients :*

$$\|P\| = \sup_k |a_k|$$

avec $P = \sum_k a_k X^k$. Alors pour tout $P \in K[X]$ unitaire séparable et pour tout $\varepsilon > 0$, il existe $\delta > 0$ tel que, si $\|P - Q\| < \delta$ avec $Q \in K[X]$ unitaire, alors Q est séparable du même degré

que P et il existe une bijection $\sigma : Z_P \longrightarrow Z_Q$ de l'ensemble Z_P des racines de P (dans $\overline{K}$) vers l'ensemble Z_Q des racines de Q telle que pour tout $z \in Z_P$:

$$|z - \sigma(z)| < \varepsilon.$$

Démonstration. On note L la complétion métrique de $\overline{K}$. Posons $d = \deg P$ et considérons l'ouvert de L^d suivant :

$$U = \{(x_1, \dots, x_d) \in L^d \mid \forall i \neq j,\ x_i \neq x_j\}.$$

On note aussi E le L-espace affine de dimension d des polynômes unitaires de degré d à coefficients dans L. On a une application continue :

$$f : L \longrightarrow E$$

qui à $(x_i)_i$ associe $\prod_i (X - x_i)$.
Cette application, entre L-espaces affines de dimension finie, est même de classe C^1 et on a :

$$df_{(x_i)_i} = -\sum_i \prod_{j \neq i} (X - x_j) dx_i.$$

La différentielle en $(x_i)_i$ est inversible car les espaces au départ et à l'arrivée ont même dimension et si $\sum_i \prod_{j \neq i} (X - x_j) h_i = 0$ pour tout $h = (h_i)_i \in L^d$, on obtient en évaluant en x_k :

$$\prod_{j \neq k} (x_k - x_j) h_i = 0$$

donc $h_i = 0$ car $(x_i)_i \in U$.
Le théorème d'inversion locale s'applique ici car L est complet, et donc f est un difféomorphisme local. Ainsi, si $\alpha_1, \dots, \alpha_d$ sont les racines de P, pour $\delta > 0$ suffisament petit, f induit un difféomorphisme :

$$B(\underline{\alpha}, \eta) \longrightarrow V$$

avec V un ouvert de E contenant $P = f(\underline{\alpha})$ et $\eta < \varepsilon$. On prend la norme que l'on veut sur L^d car elles sont toutes équivalentes d'après 14.5 (L étant complet). Ici, on prend la norme infinie. Ainsi, pour δ assez petit, si $\|P - Q\| < \delta$, alors $Q \in V$ et donc $f^{-1}(Q) \in B(\underline{\alpha}, \eta)$, ce qui permet de conclure. □

Corollaire 14.42. *Soit K un corps local non archimédien de caractéristique 0 et $d \geq 1$ un entier.*
Il n'y a, à isomorphisme près, qu'un nombre fini d'extensions L/K de degré d et totalement ramifiées.

Démonstration. On considère E l'ensemble des polynômes unitaires Eisenstein de degré d sur K, vu comme un sous-ensemble de $\mathcal{O}_K^d$ avec la topologie de K^d. C'est un espace compact car il est fermé dans le compact $\mathcal{O}_K^d$.
À tout $P \in E$, on associe L_P le corps $K[X]/(P)$: c'est une extension de degré d de K totalement ramifiée d'après le théorème 14.34 et elles s'obtiennent toutes de cette façon.
Montrons que le corps L_P est "localement constant" lorsque P varie, au sens où pour tout $P \in E$, il existe un voisinage de P dans E tel que, pour tout Q dans ce voisinage,

on ait $L_Q \cong L_P$.
On fixe $\overline{K}$ une clôture algébrique de K et on note $\alpha_1, \ldots, \alpha_d$ les racines de P dans $\overline{K}$. Il existe $\eta > 0$ tel que, pour tout $b \in \overline{K}$ et pour tout i, si $|b - \alpha_i| < \eta$, alors :

$$|b - \alpha_i| < \left|b - \alpha_j\right|$$

pour tout $j \neq i$.
Par le théorème de continuité des racines 14.41, il existe U un voisinage de P dans E tel que pour tout $Q \in U$, on puisse écrire $Q = \prod_i (X - \beta_i)$ avec $\left|\alpha_i - \beta_i\right| < \eta$. Ainsi, pour tout $Q \in U$, d'après le lemme de Krasner 14.40, on a $K(\alpha_i) \subseteq K(\beta_i)$, or ils sont tous deux de degré d sur K donc $K(\alpha_i) = K(\beta_i)$ et :

$$L_P \cong K(\alpha_i) \cong K(\beta_i) \cong L_Q.$$

Noter qu'on peut choisir n'importe quelle norme sur l'espace des polynômes de degré au plus d car c'est un espace vectoriel de dimension finie sur un corps complet, et on utilise le théorme 14.5.
Par compacité de E, on extrait un recouvrement fini de ces ouverts U et on conclut. □

On en déduit le théorème suivant.

Théorème 14.43. *Soit K un corps local non archimédien de caractéristique 0 et $d \geq 1$ un entier.*
Il n'y a, à isomorphisme près, qu'un nombre fini d'extensions L/K de degré d.

Démonstration. D'après le théorème 14.39, toute extension finie L/K est une extension totalement ramifiée d'une extension non ramifiée de K.
Or K n'a qu'un nombre fini d'extensions non ramifiées de degré borné d'après l'équivalence de catégories donnée par le théorème 14.29 car son corps résiduel n'a qu'un nombre fini d'extensions non ramifiées de degré borné.
À son tour, chacune de ces extensions n'a qu'un nombre fini d'extensions totalement ramifiées d'après le corollaire précédent. On en déduit le résultat. □

Voyons par exemple le cas des extensions quadratiques.

Exemple 14.44. De façon générale, si K est un corps de caractéristique différente de 2, toute extension quadratique de K est de la forme $K(\sqrt{d})$ avec $d \in K$ qui n'est pas un carré. On peut multiplier d par un carré sans changer l'extension $K(\sqrt{d})$, et deux extensions quadratiques $K(\sqrt{d})$ et $K(\sqrt{s})$ sont isomorphes si et seulement si d/s est un carré : en effet, si c'est le cas, on peut écrire $\sqrt{d} = a + b\sqrt{s}$ donc $d = a^2 + sb^2 + 2ab\sqrt{s}$ de sorte que $ab = 0$ et donc $a = 0$ et $d = sb^2$.
Ainsi les extensions quadratiques sont paramétrées, à isomorphisme près, par $d \in \left(K^\times/(K^\times)^2\right) \setminus \{1\}$.
Ainsi, pour p premier impair, on a, d'après 14.16 :

$$\mathbb{Q}_p^\times = \mathbb{U}_{p-1}(\mathbb{Q}_p) \odot (1 + p\mathbb{Z}_p) \odot p^{\mathbb{Z}}$$

et donc :

$$\left(\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2\right) \cong \frac{\mathbb{U}_{p-1}}{\mathbb{U}_{\frac{p-1}{2}}} \times \frac{1 + p\mathbb{Z}_p}{(1 + p\mathbb{Z}_p)^2} \times p^{\mathbb{Z}/2\mathbb{Z}} \cong (\mathbb{Z}/2\mathbb{Z})^2$$

car $1 + p\mathbb{Z}_p \cong \mathbb{Z}_p$ d'après 14.24, et $2\mathbb{Z}_p = \mathbb{Z}_p$.
Pour p impair, le corps $\mathbb{Q}_p$ a donc exactement trois extensions quadratiques à isomorphisme près.

Chapitre 15

Corps globaux

> Entre les deux principales et plus importantes disciplines des mathématiques modernes, la théorie des fonctions et la théorie des nombres, existe une étrange et considérable analogie de résultats, mais une grande différence dans leurs méthodes.
>
> Kurt Hensel, la Théorie des Nombres Algébriques

Il existe de nombreuses similarités entre les corps de nombres et les corps de fonctions à une variable sur un corps fini. On regroupe ces deux familles de corps sous le nom de *corps globaux*, par opposition aux corps locaux qui s'obtiennenten complétant les corps globaux en des places (de la même façon que les anneaux locaux s'obtiennent en général en localisant un anneau en un idéal premier).

Définition 15.1. *Un corps global est une extension finie séparable de $\mathbb{Q}$ ou de $k(T)$ avec k un corps fini.*

Notation 15.2. *Si K est un corps et v est une place sur K, on note K_v le complété de K pour n'importe quelle valeur absolue représentant v, puisque le complété ne dépend que de la place.*

Théorème 15.3. *Soit K un corps et v une place sur K telle que le complété K_v est un corps local. Soit L une extension finie et séparable de K. Alors il y a un nombre fini de places sur L qui prolongent v, et on a un isomorphisme canonique de K_v-algèbres topologiques :*

$$L \otimes_K K_v \cong \prod_{w|v} L_w$$

où le produit porte sur les places de L qui prolongent v, et en plaçant sur le membre de gauche la topologie de K_v-espace vectoriel de dimension finie (puisque K_v est un corps complet), et

sur le membre de droite la topologie produit. De plus, les L_w sont des extensions finies de K_v et des corps locaux. On a enfin la formule suivante :

$$[L : K] = \sum_{w|v} [L_w : K_v]$$

Démonstration. Par le théorème de l'élément primitif, on peut écrire $L = K[a] = K[X]/(f)$ avec f le polynôme minimal de a, irréductible et séparable. On factorise f dans K_v en $f = \prod f_i$ avec les f_i irréductibles sur K_v, distincts et séparables. On note $\tilde{L} = L \otimes_K K_v$. Ainsi on a un isomorphisme :

$$\tilde{L} = L \otimes_K K_v \cong K_v[X]/(f) \cong \prod_i K_v[X]/(f_i) = \prod_i K_i$$

avec $K_i = K[X]/(f_i)$. Ici K_i est une extension finie du corps local K_v donc par 14.9, il existe une unique place v_i sur K_i au dessus de v sur K_v. En munissant le membre de gauche de sa topologie de K_v-espace vectoriel de dimension finie et le membre de droite de la topologie produit des topologies provenant de chaque v_i, l'isomorphisme précédent est K_v-linéaire entre des K_v-espaces vectoriels de dimension finie donc c'est un *homéomorphisme* d'après 14.7.

Pour chaque i, on a un morphisme de K-algèbres $L \longrightarrow \tilde{L} \longrightarrow K_i$ avec la projection sur le i-ème facteur, et ainsi K_i est une extension de L. On note w_i la restriction de v_i à L, c'est bien une place (non triviale) car elle prolonge la place v de K (qui est non triviale).
On observe que $L = L \otimes_K K$ est *dense* dans $\tilde{L}$, donc en projetant, L est dense dans K_i. Ainsi K_i est le complété métrique de L pour w_i :

$$K_i = L_{w_i}$$

Ensuite, montrons que les places w_i sont deux à deux distinctes. Soient $i \neq j$ tels que $w_i = w_j = w$. On a donc $K_i = K_j = L_w$ et en projetant, $\Delta_L = \{(x, x) \mid x \in L\}$ est dense dans $L_w \times L_w$ (muni de la topologie produit), or $\Delta_L \subseteq \Delta_{L_w}$ qui est un fermé de $L_w \times L_w$ car L_w est séparé. En prenant l'adhérence sur cette inclusion, on a $L_w \times L_w = \Delta_{L_w}$ ce qui est absurde.

Il reste à montrer que toute place w sur L qui prolonge v est une des w_i. Soit donc w une place sur L qui prolonge v, et prenons $|\bullet|_w$ une valeur absolue triangulaire représentant w. On munit la K_v-algèbre de dimension finie $\widetilde{L}$ de la norme infinie $\|\bullet\|$ associée à la K_v-base $(1 \otimes 1, a \otimes 1, \ldots, a^{d-1} \otimes 1)$ avec $d = [L : K]$, de sorte que cette norme redéfinit la topologie de $\widetilde{L}$ par équivalence des normes (voir 14.5). Pour tout $x \in L$, écrivons $x = \sum_k \lambda_k a^k$ et observons que :

$$|x|_w \leq \sum_k |\lambda_k|_v \, |a|_w^k \leq C \cdot \|x \otimes 1\|$$

avec $C > 0$ une constante indépendante de x. Ainsi $|\bullet|_w$ est *uniformément continue* sur $L \subseteq \widetilde{L}$ vis à vis de la topologie de $\widetilde{L}$. Or L est dense dans $\widetilde{L}$, donc il existe une unique application N_w uniformément continue sur $\widetilde{L}$ qui prolonge $|\bullet|_w$. Cette application est *positive* et vérifie les propriétés suivantes (que l'on obtient en raisonnant par densité) :

— Pour tous $\alpha, \beta \in \widetilde{L}$ on a $N_w(\alpha\beta) = N_w(\alpha)N_w(\beta)$.
— Pour tout $\alpha \in \widetilde{L}$ et tout $\lambda \in K_v$, on a $N_w(\lambda\alpha) = |\lambda|_v N_w(\alpha)$.
— Pour tous $\alpha, \beta \in \widetilde{L}$ on a $N_w(\alpha+\beta) \leq N_w(\alpha) + N_w(\beta)$.

On remarquera que N_w ne vérifie pas l'axiome de séparation en général, ce n'est donc a priori pas une norme sur $\widetilde{L}$.
Posons à présent $\gamma_i = (0,\dots,1,\dots,0) \in \widetilde{L} = \prod_i K_i$. Puisque $N_w(\sum_i \gamma_i) = N_w(1 \otimes 1) = 1$, il existe un indice k tel que $N_w(\gamma_k) > 0$. De plus, pour tout $i \neq k$ on a $\gamma_i\gamma_k = 0$ donc $N_w(\gamma_i)N_w(\gamma_k) = 0$ et donc $N_w(\gamma_i) = 0$.

Pour $x \in K_k$, notons $\nu(x) = N_w(x\gamma_k)$ et observons que ν est une valeur absolue sur K_k qui prolonge la valeur absolue $|\bullet|_v$. Par les propriétés précédentes sur N_w, la multiplicativité, la positivité et l'inégalité triangulaire sont bien vérifiées. De plus, si $x \neq 0$, on a $\nu(x)\nu(1/x) = N_w(\gamma_k) > 0$, et donc ν est une valeur absolue sur K_k qui prolonge $|\bullet|_v$ (car $\nu(\gamma_k) = 1$ puisqu'on a une valeur absolue). Or il y a unicité d'une telle valeur absolue sur K_k d'après 14.9, et ainsi :

$$\nu = v_k$$

et en restreignant à $L \subseteq K_k$:

$$w = w_k$$

et donc finalement on a un isomorphisme topologique de K_v-algèbres :

$$L \otimes_K K_v \cong \prod_i K_i \cong \prod_{w|v} L_w.$$

En particulier le nombre de places sur L qui prolongent v est fini car elles sont en bijection avec les facteurs irréductibles de f dans $K_v[X]$. Enfin, en prenant la dimension en tant que K_v-espace vectoriel, on obtient :

$$[L : K] = \sum_{w|v} [L_w : K_v].$$

□

Corollaire 15.4. *On se place sous les mêmes hypothèses que le théorème précédent. Alors pour tout $x \in L$ on a :*

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

et :

$$\mathrm{Tr}_{L/K}(x) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(x)$$

Démonstration. Soit $x \in L$. On a :

$$N_{L/K}(x) = N_{L \otimes_K K_v/K_v}(x)$$

car l'endomorphisme de multiplication par x dans $L \otimes_K K_v$ est $\mu_x \otimes \mathrm{id}_{K_v}$ avec μ_x l'endomorphisme de multiplication par x dans L.

Or on a $L \otimes_K K_v \cong \bigoplus_{w|v} L_w$ comme K_v-espaces vectoriels et la multiplication par x sur cette somme directe est diagonale et donc :

$$N_{L\otimes_K K_v/K_v}(x) = \prod_{w|v} N_{L_w/K_v}(x)$$

dont on déduit la première formule. La seconde se démontre de la même façon. □

Proposition 15.5. *Si K est un corps global, alors tous ses complétés en des places sont des corps locaux. En particulier le théorème 15.3 s'applique toujours si K est un corps global.*

Démonstration. Notons F le corps $\mathbb{Q}$ ou le corps $k(T)$ avec k un corps fini. Alors tous les complétés de F en des places sont des corps locaux d'après le théorème d'Ostrowski 13.30 et la classification des places sur $k(T)$ avec k fini 13.33.
Maintenant, si K est une extension finie de F, le théorème 15.3 entraîne que les complétés de K en des places (nécessairement au dessus de places sur F par le lemme 13.28) sont des corps locaux. □

Le théorème suivant fait le lien avec la théorie des corps de nombres.

Théorème 15.6. *Soit K un corps de nombres. Les places non archimédiennes sur K sont représentées par les $|\bullet|_\mathfrak{p}$ pour $\mathfrak{p}$ un premier de $\mathcal{O}_K$, définies par :*

$$|x|_\mathfrak{p} = \|\mathfrak{p}\|_{K/\mathbb{Q}}^{-v_\mathfrak{p}(x)}$$

et la correspondance entre places non archimédiennes sur K est premiers de $\mathcal{O}_K$ est bijective. Ensuite, pour chaque plongement (de corps) $\sigma : K \longrightarrow \mathbb{C}$, on a une valeur absolue :

$$|x|_\sigma = |\sigma(x)|$$

et $\sigma \mapsto |\bullet|_\sigma$ induit une bijection entre les places archimédiennes sur K et les plongements de K dans $\mathbb{C}$ modulo conjugaison complexe.

Remarque 15.7. Si K est un corps de nombres, $\mathcal{O}_K$ est toujours la notation pour l'anneau des entiers, et si v est une place non archimédienne sur K, on notera plutôt $\mathcal{O}_v$ l'anneau de valuation pour la place v. On a toujours :

$$\mathcal{O}_K \subseteq \mathcal{O}_v$$

car $\mathcal{O}_v$ est intégralement clos.

Démonstration. D'abord il est clair que les valeurs absolues décrites dans l'énoncé sont des valeurs absolues sur K, et que $|\bullet|_\mathfrak{p}$ est non archimédienne et $|\bullet|_\sigma$ est archimédienne. De plus, on a $|\bullet|_{\overline{\sigma}} = |\bullet|_\sigma$. Par le théorème de l'élément primitif, on peut écrire $K = \mathbb{Q}[X]/(f)$ avec f irréductible sur $\mathbb{Q}$.
Soit v une place sur K et $|\bullet|$ une valeur absolue représentant v. La restriction de $|\bullet|$ à $\mathbb{Q}$ est non triviale en vertu du lemme 13.28.
Si v est archimédienne, alors $v_{|\mathbb{Q}}$ est la place usuelle sur $\mathbb{Q}$. Or le complété $\mathbb{R}$ est local donc le théorème précédent s'applique et les places sur K au dessus de la place usuelle

(c'est à dire les places archimédiennes) correspondent bijectivement aux facteurs irréductibles de f dans $\mathbb{R}[X]$, c'est à dire aux racines complexes de f modulo conjugaison, c'est à dire aux plongements complexes de K dans $\mathbb{C}$ modulo conjugaison. On vérifie facilement que dans cette correspondance, $|\bullet|_\sigma$ correspond à σ.
Traitons à présent le cas non archimédien. Par les arguments usuels (théorème d'Ostrowski et lemme 13.28), les places non archimédiennes sur K sont les places qui étendent la place p-adique pour un certain p premier. Si v est une telle place, $\mathfrak{m}_v$ est un idéal maximal de $\mathcal{O}_v$ contenant p donc $\mathfrak{m}_v \cap \mathcal{O}_K = \mathfrak{p}$ avec $\mathfrak{p}$ un premier de $\mathcal{O}_K$ au dessus de p. Il s'agit alors de montrer que $|\bullet|_v$ et $|\bullet|_\mathfrak{p}$ sont équivalentes. Soit $x \in \mathcal{O}_{|\bullet|_\mathfrak{p}}$. On a donc :

$$v_\mathfrak{p}((x)) \geq 0$$

et par le théorème de spécification finie 3.42, il existe $y \in K \setminus \{0\}$ tel que pour tout $\mathfrak{q} \neq \mathfrak{p}$ tel que $v_\mathfrak{q}(x) \neq 0$ on ait :

$$v_\mathfrak{q}(y) \geq \max(0, -v_\mathfrak{q}(x))$$

et

$$v_\mathfrak{p}(y) = 0$$

et pour tout autre $\mathfrak{q}$, $v_\mathfrak{q}(y) \geq 0$. Ainsi $y \in \mathcal{O}_K \setminus \mathfrak{p}$ et $xy \in \mathcal{O}_K$. Puisque $\mathcal{O}_K \subseteq \mathcal{O}_v$, on a donc $\left|xy\right|_v \leq 1$.
Or $y \notin \mathfrak{m}_v$ car $\mathfrak{m}_v \cap \mathcal{O}_K = \mathfrak{p}$ et $y \notin \mathfrak{p}$. Donc $\left|y\right|_v \geq 1$ et ainsi :

$$|x|_v = \frac{\left|xy\right|_v}{\left|y\right|_v} \leq \frac{1}{\left|y\right|_v} \leq 1$$

donc $x \in \mathcal{O}_v$ et on a montré $\mathcal{O}_{|\bullet|_\mathfrak{p}} \subseteq \mathcal{O}_v$ donc ces deux places sont les mêmes.
Il reste à voir qu'elles sont deux à deux non équivalentes, mais c'est clair car si $\mathfrak{m}_{|\bullet|_\mathfrak{p}} = \mathfrak{m}_{|\bullet|_\mathfrak{q}}$, alors en intersectant avec $\mathcal{O}_K$ on obtient $\mathfrak{p} = \mathfrak{q}$. □

Sur un corps local K, on peut toujours choisir un représentant canonique de la place de K.

Définition 15.8. *Soit K un corps local non archimédien de place v. Il existe une unique valeur absolue $|\bullet|_{K,\text{can}}$ sur K de la classe d'équivalence v telle que pour toute uniformisante π on ait :*

$$|\pi|_{K,\text{can}} = |\kappa_K|^{-1}.$$

On appelle cette valeur absolue la normalisation de la place v.
Pour un corps local archimédien, c'est à dire $\mathbb{R}$ ou $\mathbb{C}$, les valeurs absolues normalisées sont la valeur absolue usuelle sur $\mathbb{R}$ et le carré du module sur $\mathbb{C}$. Si v est une place sur un corps global K, $|\bullet|_{v,\text{can}}$ désigne la place normalisée associée à v sur le corps local K_v.
Si K est un corps global, on note $\mathcal{P}_K$ l'ensemble des places sur K.

Si K est un corps local, on veillera à ne pas confondre la valeur absolue initiale sur K et la valeur absolue normalisée $|\bullet|_{K,\text{can}}$.

Exemple 15.9. Sur $\mathbb{Q}_p$, la valeur absolue p-adique est normalisée car le corps résiduel est de cardinal p et $|p|_p = p^{-1}$.
Si k est un corps fini et p est un polynôme irréductible unitaire, on normalise la valeur absolue p-adique de la façon suivante :

$$|f| = |k|^{-v_p(f)\deg p}$$

car le corps résiduel est $k[T]/(p)$ qui est de cardinal $|k|^{\deg p}$. Pour la place à l'infini, le corps résiduel est de cardinal k donc on normalise ainsi :

$$|f| = |k|^{\deg f}.$$

Si K est un corps de nombres et $\mathfrak{p}$ un premier de K, la bonne normalisation pour la valeur absolue $\mathfrak{p}$-adique est :

$$|x|_{\mathfrak{p}} = \|\mathfrak{p}\|^{-v_{\mathfrak{p}}(x)}$$

car le corps résiduel est de cardinal $\|\mathfrak{p}\|$.

Si L/K est une extension de corps locaux, la valeur absolue normalisée sur L ne se restreint pas en la valeur absolue normalisée sur K, mais elles sont reliées par le degré de l'extension.

Proposition 15.10. *Soit L/K une extension finie de corps locaux. Pour tout $x \in K$, on a :*

$$|x|_{L,\mathrm{can}} = |x|_{K,\mathrm{can}}^{[L:K]}.$$

Si on note $|\bullet|_{L/K}$ l'unique prolongement de $|\bullet|_{K,\mathrm{can}}$ à L, on a donc :

$$|x|_{L,\mathrm{can}} = |x|_{L/K}^{[L:K]}$$

pour tout $x \in L$. Enfin, on peut écrire la norme $|\bullet|_{L,\mathrm{can}}$ de la façon suivante :

$$|x|_{L,\mathrm{can}} = \left|N_{L/K}(x)\right|_{K,\mathrm{can}}$$

pour tout $x \in L$.

Démonstration. Si K est archimédien, c'est clairement vrai si $K = L$ et sinon on peut supposer $K = \mathbb{R}$ et $L = \mathbb{C}$, auquel cas l'énoncé est immédiat.
La valeur absolue normalisée est équivalente à $|\bullet|_{L/K}$, donc il existe $\alpha > 0$ tel que :

$$|x|_{L,\mathrm{can}} = |x|_{L/K}^{\alpha}$$

pour tout $x \in L$. Le but est de montrer que $\alpha = [L : K]$. Pour cela, on considère π_L une uniformisante de L et π_K une uniformisante de K, de sorte que, d'après 14.26 :

$$|\kappa_K|^{-1} = |\pi_K|_{K,\mathrm{can}} = |\pi_L|_{L/K}^{e(L|K)}.$$

De plus on a :

$$|\pi_L|_{L,\mathrm{can}} = |\kappa_L|^{-1} = |\kappa_K|^{-[\kappa_L:\kappa_K]} = |\kappa_K|^{-f(L|K)} = \left(|\pi_L|_{L/K}^{e(L|K)}\right)^{f(L|K)} = |\pi_L|_{L/K}^{e(L|K)f(L|K)} = |\pi_L|_{L/K}^{[L:K]}$$

donc $\alpha = [L:K]$ puisque $|\pi_L|_{L/K} < 1$.
Enfin, on sait d'après le théorème 14.9 que :

$$|x|_{L/K} = \left|N_{L/K}(x)\right|_{K,\mathrm{can}}^{\frac{1}{[L:K]}}$$

donc :

$$|x|_{L,\mathrm{can}} = \left|N_{L/K}(x)\right|_{K,\mathrm{can}}.$$

□

Les valeurs absolues normalisées permettent d'avoir la formule suivante.

Théorème 15.11. *(Formule du produit) Soit K un corps global. Pour tout $x \in K^\times$, on a $|x|_v = 1$ pour presque toute place (i.e. toutes sauf un nombre fini) $v \in \mathcal{P}_K$ et :*

$$\prod_{v \in \mathcal{P}_K} |x|_{v,\mathrm{can}} = 1.$$

Démonstration. On traite d'abord le cas de $\mathbb{Q}$. Soit $x \in \mathbb{Q}^\times$, on a $v_p(x) = 0$ sauf pour un nombre fini de nombre premiers, et :

$$x = \pm \prod_p p_p^v(x).$$

Ainsi :

$$|x|_\infty = \prod_p p^{v_p(x)} = \prod_p |x|_p^{-1}$$

donc $\prod_{v \in \mathcal{P}_\mathbb{Q}} |x|_{v,\mathrm{can}} = 1$ d'après le théorème d'Ostrowski 13.30.
On traite maintenant le cas de $\kappa(T)$ avec κ un corps fini. Par multiplicativité, il suffit de voir que pour $f \in \kappa[T] \setminus \{0\}$, on a $|f|_v = 1$ pour presque toute place v et que la formule est vraie pour f. D'après le théorème 13.33, les places sur $\kappa(T)$ sont les places associées aux polynômes irréductibles unitaires ainsi que la place à l'infini, or f n'est divisible que par un nombre fini de polynômes unitaires irréductibles donc $|f|_{v,\mathrm{can}} = 1$ pour presque toute place v. Ensuite on écrit :

$$f = \alpha \prod_p p^{v_p(f)}$$

avec un produit qui porte sur les polynômes irréductibles unitaires et $\alpha \in \kappa \setminus \{0\}$. On a donc :

$$\deg f = \sum_p v_p(f) \deg p.$$

Ainsi :

$$\prod_v |f|_{v,\mathrm{can}} = \left(\prod_p |\kappa|^{-\deg p \cdot v_p(f)} \right) |\kappa|^{\deg f} = 1$$

comme souhaité.
Dans le cas général, K est une extension finie séparable de $F = \mathbb{Q}$ ou $F = \kappa(T)$ avec κ un

corps fini, et on a vu que la formule était vraie pour F. Soit $x \in K^\times$. De ce qui précède, puisque $N_{K/F}(x) \neq 0$, on a :

$$\begin{aligned}
1 &= \prod_{v \in \mathcal{P}_F} \left|N_{K/F}(x)\right|_{v,\mathrm{can}} \\
&= \prod_{v \in \mathcal{P}_F} \left| \prod_{w|v} N_{K_w/F_v}(x) \right|_{v,\mathrm{can}} && \text{par 15.4} \\
&= \prod_{v \in \mathcal{P}_F} \prod_{w|v} \left|N_{K_w/F_v}(x)\right|_{v,\mathrm{can}} \\
&= \prod_{v \in \mathcal{P}_F} \prod_{w|v} |x|_{w,\mathrm{can}} && \text{par 15.10} \\
&= \prod_{w \in \mathcal{P}_K} |x|_{w,\mathrm{can}}
\end{aligned}$$

ce qui montre que $|x|_{w,\mathrm{can}} = 1$ pour presque tout w, puisque le premier produit porte sur un nombre fini de facteurs. □

On peut appliquer le théorème 15.3 pour étudier la ramification des premiers dans une extension de corps de nombres dans le cas où le théorème de Kummer-Dedekind 5.48 ne s'applique pas.
En effet, si $L = K[\alpha]$ est une extension finie d'un corps de nombre α, avec P le polynôme (unitaire) minimal de α sur L, et si $\mathfrak{p}$ est un premier de K, le théorème 15.3 donne :

$$L \otimes_{\mathbb{Q}} K_{\mathfrak{p}} \cong \prod_{\mathfrak{q} \supseteq \mathfrak{p}} L_{\mathfrak{q}}$$

où $K_{\mathfrak{p}}$ désigne le corps complété $K_{v_{\mathfrak{p}}}$. Or on a vu, dans la preuve de 15.3, que si $P = \prod_i Q_i$ est la décomposition en produit d'irréductibles de P dans le corps local $K_{\mathfrak{p}}$, alors chaque $L_{\mathfrak{q}}$ correspond à un $K_{\mathfrak{p}}[X]/(Q_i)$ et on a ainsi :

$$e(\mathfrak{q} \mid \mathfrak{p}) = e(K_{\mathfrak{p}}[X]/(Q_i) \mid K_{\mathfrak{p}})$$

et

$$f(\mathfrak{q} \mid \mathfrak{p}) = f(K_{\mathfrak{p}}[X]/(Q_i) \mid K_{\mathfrak{p}})$$

de sorte que :

$$e(\mathfrak{q} \mid \mathfrak{p}) f(\mathfrak{q} \mid \mathfrak{p}) = \deg Q_i.$$

La suite

Nous n'avons dans ce texte fait que commencer à étudier la théorie algébrique des nombres. On en a posé les bases et il reste à présent de nombreux paysages à découvrir dans des directions très diverses, ainsi que de nombreux outils intéressants à apprendre à utiliser.

D'abord, il reste à étudier la théorie de Galois pour des extensions infinies, en lien avec la théorie des groupes profinis, ce qui permet d'introduire des outils *cohomologiques* très puissants. Si K est un corps, on dispose d'un groupe profini G_K qui est le groupe de Galois d'une clôture séparable (ou algébrique si on est en caractéristique nulle) de K, et pour tout groupe abélien A muni d'une action raisonnable de G_K, on peut associer des invariants $H^n(K,A)$ dotés d'une multitude de bonnes propriétés fonctorielles. Ces outils mènent par exemple à la théorie du corps de classe, qui permet (entre-autres) d'étudier les extensions abéliennes d'un corps de nombres. On renvoie à Neukirch pour les fondements de cette théorie [11]. Ils sont aussi primordiaux dans le domaine de la géométrie arithmétique qui s'intéresse à l'existence de solutions dans des corps de nombres à des équations algébriques avec beaucoup de variables. Le lecteur intéressé pourra lire le superbe ouvrage d'introduction de Poonen à ce sujet [12].

Notre étude des anneaux de Dedekind fait souvent référence à des propriétés géométriques du spectre associé, ce qui peut sembler très mystérieux au départ. On encourage le lecteur à se familiariser avec la théorie des schémas pour comprendre en quoi cette analogie est si importante. On renvoie par exemple au livre de Vakil, *The Rising Sea* pour cela [16].

Dans l'étude des corps globaux K, un outil important est l'anneau des adèles de K ainsi que le groupe des idèles associé. Ces objets permettent de rassembler toutes les places de K et sont omniprésents dans les travaux de Tate par exemple, qui leur applique la théorie de Fourier sur les groupes localement compacts. Concrètement, l'anneau des adèles $\mathbb{A}_K$ de K est un sous-anneau du produit des complétés K_v en toutes les places, constitué des éléments qui pour presque toute place v sont des unités. L'analogie géométrique à avoir en tête, si l'on considère un corps de nombres comme le corps des fonctions d'une courbe lisse $\operatorname{Spec}\mathcal{O}_K$, est celle des (germes de) fonctions méromorphes sur une surface de Riemann.

Enfin, la partie III sur la théorie analytique des corps de nombres ouvre des portes vers la théorie des formes modulaires et des représentations du groupe de Galois absolu d'un corps de nombres. Tout ceci mène au fameux programme de Langlands, qui vise à relier des objets analytiques à des représentations galoisiennes.

En bref, il serait possible de continuer ce texte sur encore des centaines de pages tellement le domaine que nous avons introduit ici est vaste, mais cela nécessiterait

encore de nombreux prérequis du point de vue algébrique : il faudrait notamment développer toute la batterie d'algèbre homologique et de géométrie algébrique qui sont omniprésentes dans ces questions. Je laisse donc au lecteur le soin de trouver d'autres références pour continuer.

Bibliographie

[1] Manjul Bhargava, Arul Shankar, Takashi Taniguchi, Frank Thorne, Jacob Tsimerman, and Yongqiang Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves, 2017. arXiv:1701.02458.

[2] Sid Ali Bousla. *Introduction à la fonction zêta de Riemann*. PhD thesis, 06 2017.

[3] Gaëtan Chenevier. Théorie algébrique des nombres, cours de m1 à polytechnique. 2011-2019. URL : http://gaetan.chenevier.perso.math.cnrs.fr/TAN_chenevier.pdf.

[4] Jürgen Klüners and Jiuya Wang. ℓ-torsion bounds for the class group of number fields with an ℓ-group as galois group, 2020. arXiv:2003.12161.

[5] Manfred Kolster. The 2-part of the narrow class group of a quadratic number field. *Annales des Sciences Mathématiques du Québec*, 29, 01 2005.

[6] Peter Koymans and Carlo Pagano. A sharp upper bound for the 2-torsion of class groups of multiquadratic fields, 2020. arXiv:2009.08399.

[7] Tom Leinster. Basic category theory, 2016. arXiv:1612.09375.

[8] Louis Mallet-Burgues. Explicit bounds for 2-torsion in class groups of number fields. URL : https://www.normalesup.org/~lmalletb/bounds%20on%202%20torsion.pdf.

[9] Daniel A Markus. *Number Fields, Second Edition*. Springer, 2010.

[10] Pascal Monin. Cours de m2 de théorie algorithmique des nombres. URL : https://master-math-fonda.imj-prg.fr/2024-25/fiches/MOLIN-spe.html.

[11] Jürgen Neukirch. *Class Field Theory*. Springer, 2015.

[12] Bjorn Poonen. *Rational points on varieties*. AMS, 2023.

[13] Joseph Rabinoff. Discriminants in towers. URL : https://services.math.duke.edu/~jdr/1516f-4803/disctower.pdf.

[14] G.A. Chicas Reyes. Structure theorems for projective modules. URL : https://algant.eu/documents/theses/chicas%20reyes.pdf.

[15] John R. Silvester. Determinants of block matrices. *The Mathematical Gazette*, 84(501) :460–467, 2000. doi:10.2307/3620776.

[16] Ravi Vakil. The rising sea. URL : https://math.stanford.edu/~vakil/216blog/FOAGjul2724public.pdf.