M2 2026-2027 : Théorie des nombres (I)

David Harari

Table des matières

1. Anneaux de valuation discrète, Anneaux de Dedekind **2**
1.1. Anneaux de valuation discrète 2
1.2. Anneaux de Dedekind 7

2. Extensions d'anneaux de Dedekind, ramification **12**
2.1. Rappels sur les normes et traces 12
2.2. Extensions d'anneaux de Dedekind ; exemples 14
2.3. Décomposition des idéaux dans une extension, ramification . . 16
2.4. Cas d'une extension galoisienne 20

3. Extensions d'anneaux de Dedekind : compléments **22**
3.1. Discriminant et différente 22
3.2. Substitution de Frobenius 28
3.3. Extensions cyclotomiques 29

4. Corps complets pour une valuation discrète **30**
4.1. Valuations ultramétriques 30
4.2. Corps valués complets 32
4.3. Extensions d'un corps complet 36
4.4. Lemme de Hensel 39
4.5. Extensions non ramifiées 42
4.6. Classification des corps locaux 44

5. Corps globaux **46**
5.1. Extensions des valeurs absolues 46
5.2. Places d'un corps de nombres et d'un corps de fonctions . . . 48
5.3. Formule du produit 51

6. Adèles et idèles **52**
6.1. Adèles 52
6.2. Théorème d'approximation forte 55
6.3. Idèles 57
6.4. Idèles et idéaux 59
6.5. Le théorème des unités de Dirichlet 60

Ces notes correspondent à la première moitié du cours de M2 de théorie des nombres. La deuxième moitié sera faite par J. Anschütz. Sauf mention expresse du contraire, le terme d'"anneau" désignera toujours un anneau commutatif (et de même pour un corps).

On supposera connues les résultats de base de la théorie des modules sur un anneau commutatif, ainsi que les notions suivantes d'algèbre commutative : produit tensoriel, localisation, anneaux noethériens et factoriels, idéaux premiers et maximaux. Les résultats principaux de la théorie de Galois des extensions de corps seront également considérés comme acquis. Le groupe multiplicatif des inversibles d'un anneau A est noté A^*.

1. Anneaux de valuation discrète, Anneaux de Dedekind

La notion d'anneau de Dedekind est apparue naturellement en théorie de nombres comme un substitut de la notion d'anneau principal, afin de pallier le fait que les anneaux d'entiers de corps de nombres (comme par exemple $\mathbf{Z}[\sqrt{-5}]$ ne sont en géneral pas principaux (ni même factoriels). Grosso modo, on va voir que les propriétés liées aux éléments irréductibles dans un anneau factoriel (typiquement l'unicité de la décomposition en produit d'irréductibles) vont se conserver dans un anneau de Dedekind, à condition de remplacer la notion d'élément irréductible par celle d'idéal premier.

1.1. Anneaux de valuation discrète

Définition 1.1 On dit que A est un *anneau de valuation discrète* (a.v.d. en abrégé) si c'est un anneau principal, possédant un unique idéal premier non nul $\mathcal{M}$.

Noter qu'avec cette définition, un corps n'est pas un anneau de valuation discrète (il n'a pas d'idéal premier non nul).

Proposition 1.2 *Soit A un anneau de valuation discrète d'idéal premier $\mathcal{M}$. Alors A est un anneau local, qui possède (à inversible près) un unique élément irréductible. Si π est un tel élément, alors les idéaux non nuls de A sont de la forme $\pi^n A$ avec $n \in A$.*

Démonstration : Comme A a un seul idéal premier, il a a fortiori un seul idéal maximal $\mathcal{M}$ et c'est donc un anneau local. Soit π un générateur de $\mathcal{M}$, alors π est irréductible puisque $\mathcal{M}$ est premier. Si π' est un autre élement irréductible, alors $\pi' A$ est un idéal premier (car A est factoriel), donc $\pi' A = \mathcal{M} = \pi A$, ce qui montre que π et π' sont associés. Enfin, si I est un idéal non nul de A, il est engendré par un élément $a \neq 0$. En utilisant la décomposition de a en produits d'irréductibles (valable dans tout anneau factoriel), on a $a = u\pi^n$ avec $n \in \mathbf{N}$ et $u \in A^*$, d'où $I = aA = \pi^n A$.

□

Définition 1.3 On appelle *uniformisante* d'un anneau de valuation discrète A tout élément irréductible de A. Soit $K = \mathrm{Frac}\, A$ et soit π une uniformisante de A, alors tout élément x de K s'écrit de manière unique $x = u\pi^n$ avec $u \in A^*$ et $n \in \mathbf{Z}$. L'entier $n := v(x)$ s'appelle la *valuation* de x (elle ne dépend pas du choix de π vu que deux uniformisantes quelconques sont associées dans A).

On peut étendre v à K en posant $v(0) = +\infty$.

Proposition 1.4 *Soit A un anneau de valuation discrète de corps des fractions K et d'idéal maximal $\mathcal{M}$. Alors la fonction valuation $v : K^* \to \mathbf{Z}$ est un morphisme de groupes surjectif, qui vérifie $v(x+y) \geq \min(v(x), v(y))$ pour tous x, y de K. On a :*

$$A = \{x \in K, v(x) \geq 0\};\ \mathcal{M} := \{x \in K, v(x) > 0\}.$$

Démonstration : Soient x, y dans K^*, si $x = u\pi^m$ et $y = s\pi^n$ avec $u, s \in A^*$, alors $xy = (us)\pi^{m+n}$ avec $us \in A^*$, ce qui montre que $v(xy) = v(x)+v(y)$, donc v est un morphisme de groupes. Comme $v(\pi^n) = n$ pour tout $n \in \mathbf{Z}$, ce morphisme est surjectif. Les éléments non nuls de K qui sont dans A sont ceux de la forme $w\pi^r$ avec $r \geq 0$ et $w \in A^*$, ce qui montre que ce sont ceux de valuation positive ou nulle. Ils sont de plus dans $\mathcal{M}$ si et seulement s'ils ne sont pas inversibles, i.e. si $r > 0$. Enfin, si par exemple $m \geq n$, on a $(x+y) = \pi^n(u\pi^{m-n} + s)$ avec $(u\pi^{m-n} + s) \in A$, d'où $v(x+y) \geq n = v(y)$.

□

On a une réciproque à la proposition précédente, qui permet de définir un a.v.d. en partant d'une valuation. C'est d'ailleurs le plus souvent par ce procédé qu'on construit des anneaux de valuation discrète intéressants.

Proposition 1.5 *Soit K un corps. Soit $v : K^* \to \mathbf{Z}$ un homomorphisme surjectif vérifiant $v(x+y) \geq \min(v(x), v(y))$ pour tous x, y de K (en posant $v(0) = +\infty$). Alors l'ensemble A des x de K vérifiant $v(x) \geq 0$ est un anneau de valuation discrète, de valuation v, et de corps des fractions K.*

Une telle v s'appelle une valuation discrète sur le corps K. Noter que si $v(x) \neq v(y)$, on a automatiquement $v(x+y) = \min(v(x), v(y))$ car si par exemple $v(x) > v(y)$, alors $v(y) = v(x+y-x) \geq \min(v(x), v(x+y))$ d'où $v(y) \geq v(x+y)$.

Démonstration : Il est immédiat que A est un sous-anneau de K, dont les éléments inversibles sont ceux de valuation nulle. Choisissons alors π un élément de K avec $v(\pi) = 1$ (ainsi $\pi \in A$). Soit x non nul dans A de valuation n, alors $v(x) = v(\pi^n)$, donc x/π^n est inversible (car de valuation nulle), ce qui permet d'écrire $x = u\pi^n$ avec $u \in A^*$. Ainsi, tout idéal non nul de A est de la forme $\pi^m A$ avec $m \in \mathbf{N}$ (où m est la plus petite valuation des éléments de A), ce qui montre que A est principal d'unique idéal premier non nul πA. L'égalité $K = \operatorname{Frac} A$ est évidente.

□

Exemple 1.6 a) Soit p un nombre premier. On définit une valuation discrète v sur $\mathbf{Q}$ en posant $v(x) = m$ si x est un entier non nul de la forme $x = p^m u$ avec u entier non divisible par p, puis $v(x/y) = v(x) - v(y)$ pour x, y entiers avec $y \neq 0$. L'anneau de valuation discrète correspondant se note $\mathbf{Z}_{(p)}$, c'est donc l'ensemble des r/s avec $r \in \mathbf{Z}$ et $s \in \mathbf{Z}$ non divisible par p.

b) Soit k un corps, prenons $K = k((t))$, corps des séries de Laurent constitué des séries formelles du type $f = \sum_{n=n_0}^{+\infty} a_n t^n$ avec $n_0 \in \mathbf{Z}$. On définit une valuation discrète sur K en posant $v(f) = m$, où m est le plus petit entier tel que $a_m \neq 0$. L'a.v.d. associé est l'anneau des séries formelles $k[[t]]$.

Proposition 1.7 *Soit A un anneau intègre. Alors, A est un a.v.d. si et seulement si c'est un anneau local noethérien dont l'idéal maximal est engendré par un élément π non nul de A.*

Démonstration : On a déjà vu qu'un a.v.d. est local, principal (donc noethérien), dont l'idéal maximal est engendré par un élément non nul.

Montrons la réciproque. L'intersection des $\pi^n A$ ($n \geq 0$) est réduite à zéro : en effet, si x est dans cette intersection, on peut écrire $x = \pi^n x_n$ avec $x_n \in A$ pour chaque $n \geq 0$, en particulier $x_n = \pi x_{n+1}$ par intégrité de A. On observe que la suite des idéaux (x_n) est alors croissante (vu que x_{n+1} divise x_n), donc stationnaire, ce qui implique que pour n assez grand, $x_{n+1} = ax_n$ avec $a \in A$. On en déduit que $x_n = a\pi x_n$, d'où $x_n = 0$ vu que A est intègre et π non inversible dans A, et finalement $x = 0$.

Maintenant, pour tout x non nul de A, il existe un plus grand $n \geq 0$ tel que $x \in (\pi^n)$, ce qui siginifie que $x = \pi^n u$ avec $u \in A^*$. Posons $v(x) = n$ et prolongeons v à K^* en posant $v(x/y) = v(x) - v(y)$, il est alors immédiat que v est une valuation discrète sur K d'anneau A.

□

Remarque 1.8 On peut en fait remplacer l'hypothèse A intègre par celle plus faible que l'idéal maximal est engendré par un élément non nilpotent, cf. [5], chapitre I, proposition 2.

Définition 1.9 Soit A un anneau intègre de corps des fractions K. Un *idéal fractionnaire* de K (sous-entendu : relativement à A ; on peut aussi dire "idéal fractionnaire de A") est un sous-A-module I de K tel qu'il existe x non nul dans A avec $xI \subset A$.

Noter que tout sous A-module M de type fini de K est un idéal fractionnaire (si $z_1, ..., z_r$ sont des générateurs non nuls de M, il suffit d'écrire $z_i = x_i/y_i$ avec x_i, y_i non nuls dans A et de poser $x = \prod y_i$). La réciproque est vraie si A est noethérien, puisqu'alors un idéal fractionnaire I est un sous-A-module de $x^{-1}A$, lequel est de type fini car engendré par x^{-1}.

Définition 1.10 Soit A un anneau intègre de corps des fractions K. Soit I un idéal fractionnaire de K. On dit que I est *inversible* s'il existe un idéal fractionnaire J de K tel que $IJ = A$, où IJ désigne l'ensemble des sommes finies $\sum x_i y_i$ avec $x_i \in I$ et $y_i \in J$.

Un tel J est unique vu que si J' a cette propriété, alors

$$J' = J'A = J'(IJ) = (J'I)J = AJ = J.$$

Remarque 1.11 Si I est un idéal fractionnaire non nul de K, définissons $I' := (A : I)$ comme l'idéal fractionnaire de K constitué des $x \in K$ tels que $xI \subset A$. Alors, si I est inversible, son inverse est forcément I' vu que

la propriété $IJ = A$ implique $J \subset I'$ par définition de I', mais alors a fortiori $II' = A$, d'où $J = I'$ par unicité de l'inverse. Par ailleurs, un idéal fractionnaire inversible I est un A-module de type fini, car on peut dans ce cas écrire $1 = \sum_{i=1}^{r} x_i y_i$ avec $x_i \in I$ et $y_i \in I'$, ce qui montre que $(x_1, ..., x_n)$ engendre I vu que tout x de I s'écrit alors $x = \sum_{i=1}^{r} (xy_i)x_i$, où chaque xy_i est dans A par définition de I'.

Lemme 1.12 *Soit A un anneau local intègre d'idéal maximal $\mathcal{M}$. Si $\mathcal{M}$ est inversible, alors c'est un idéal principal (et donc A est un a.v.d. si on le suppose de plus noethérien).*

Démonstration : On peut par hypothèse écrire $1 = \sum x_i y_i$ avec $x_i \in \mathcal{M}$ et $y_i \in \mathcal{M}'$. En particulier, l'un des $x_i y_i$ (qui est dans A) n'est pas dans $\mathcal{M}$, et est donc un inversible u de A. En remplaçant le x_i correspondant par $x_i u^{-1}$, on obtient une relation $1 = xy$ avec $x \in \mathcal{M}$ et $y \in \mathcal{M}'$. Montrons alors que $\mathcal{M} = xA$. Soit $z \in \mathcal{M}$, alors $z = (xy)z = x(yz)$, mais $yz \in A$ par définition de $\mathcal{M}'$, ce qui achève la preuve du lemme.

□

Rappelons qu'un anneau intègre A de corps des fractions K est *intégralement clos* ou *normal* si tout élément de K entier sur A (i.e. qui annule un polynôme unitaire à coefficient dans A) est dans A. Tout anneau factoriel est intégralement clos, mais la réciproque est fausse, ex. $\mathbf{Z}[\sqrt{-5}]$.

Lemme 1.13 *Soit A un anneau local d'idéal maximal $\mathcal{M}$. On suppose A noethérien et intégralement clos. Si $\mathcal{M}\mathcal{M}' = \mathcal{M}$, alors $\mathcal{M}' = A$.*

Démonstration : Soit $x \in \mathcal{M}'$. Alors $x\mathcal{M} \subset \mathcal{M}$, d'où en itérant $x^n \mathcal{M} \subset \mathcal{M}$ pour tout $n \geq 0$, ce qui donne $x^n \in \mathcal{M}'$. Soit I_n le sous A-module de K engendré par les $x^n, n \in \mathbf{N}$; la suite des I_n est croissante, donc stationnaire car ils sont tous contenus dans le module de type fini $\mathcal{M}'$ (qui est un idéal fractionnaire) et A est noethérien. On obtient $x^n \in I_{n-1}$ pour n assez grand, ce qui montre que x est entier sur A, et donc $x \in A$ puisque A est intégralement clos.

□

Le théorème suivant donne une caractérisation abstraite des a.v.d. :

Theorème 1.14 *Soit A un anneau noethérien, intégralement clos, possédant un unique idéal premier non nul. Alors, A est un anneau de valuation discrète.*

Démonstration : On sait déjà que A est un anneau local. Soit $\mathcal{M}$ son idéal maximal ; d'après le lemme 1.12 et la proposition 1.7, il suffit de montrer que $\mathcal{M}$ est un idéal fractionnaire inversible. Or, comme $\mathcal{M}\mathcal{M}'$ est un idéal de A qui contient $\mathcal{M}$ (puisque $\mathcal{M}'$ contient A), il ne peut être égal qu'à A ou à $\mathcal{M}$. Il suffit donc de montrer par l'absurde que $\mathcal{M}\mathcal{M}' \neq \mathcal{M}$. Supposons donc $\mathcal{M}\mathcal{M}' = \mathcal{M}$. D'après le lemme 1.13, ceci entraîne que $\mathcal{M}' = A$. Nous allons montrer que cela contredit le fait que $\mathcal{M}$ est l'unique idéal premier de A.

On commence par montrer que pour tout x non nul de $\mathcal{M}$, le localisé $A_x = A[1/x]$ est égal à K. Si tel n'était pas le cas, ce localisé aurait un idéal maximal non nul $\wp$. Alors $x \notin \wp$ (vu que x devient inversible dans A_x) d'où $\wp \cap A \neq \mathcal{M}$, ce qui produirait un deuxième idéal premier non nul de A (noter que $\wp \cap A$ est non nul, vu qu'il contient un élément y non nul si y/x^n est un élément non nul de $\wp$ avec $y \in A$), d'où une contradiction.

Fixons maintenant z non nul dans A. Pour tout x non nul de $\mathcal{M}$, on peut donc écrire $1/z = y/x^n$ avec $y \in A$ et $n \geq 0$, d'où $x^n = yz \in zA$. En appliquant ceci à des générateurs $x_1, ...x_r$ de $\mathcal{M}$, on obtient $x_i^n \in zA$ pour n assez grand et tout i, et finalement $\mathcal{M}^N \subset zA$ si $N > k(n-1)$ (pour un tel n). Si en particulier $z \in \mathcal{M}$, il y a un plus petit entier $N \geq 1$ tel que $\mathcal{M}^N \subset zA$. Soit alors y dans $\mathcal{M}^{N-1}$ non dans zA, alors $y\mathcal{M} \subset zA$ d'où $y/z \in \mathcal{M}'$ mais $y/z \notin A$, ce qui contredit $\mathcal{M}' = A$.

□

Exercice 1.15 Soit $A = \mathbf{Z}_{(3)}[\sqrt[3]{2}]$. Montrer que A est un anneau de valuation discrète, d'idéal maximal engendré par $(1 +^3 \sqrt{2})$; on pourra commencer par montrer que si $\mathcal{M}$ est un idéal maximal de A, alors $3 \in \mathcal{M}$ et $\mathcal{M}/(3)$ est l'idéal de $A/(3)$ engendré par l'image de $(1 +^3 \sqrt{2})$.

1.2. Anneaux de Dedekind

La notion d'anneau de Dedekind est en quelque sorte une version "globale" de celle d'anneau de valuation discrète.

Définition 1.16 Soit un anneau intègre noethérien A. On dit que A est un *anneau de Dedekind* si pour tout idéal premier non nul $\wp$ de A, le localisé $A_\wp$ est un a.v.d.

Noter qu'un corps est bien un anneau de Dedekind (mais pas un a.v.d.). Par ailleurs, l'hypothèse que A est noethérien n'est pas impliquée par celle que tous les $A_\wp$ (pour $\wp$ idéal premier non nul de A) sont des a.v.d., un contre-exemple (dû à Nakano en 1953) est fourni par la fermeture intégrale

de $\mathbf{Z}$ dans le corps obtenu en adjoignant à $\mathbf{Q}$ les racines p-ièmes de l'unité pour tout p premier.

Theorème 1.17 *Un anneau A est de Dedekind si et seulement s'il est noethérien, intégralement clos, et de dimension ≤ 1.*

Démonstration : Supposons A de Dedekind. Si $\wp$ et $\wp'$ sont des idéaux premiers non nuls de A avec $\wp \subset \wp'$, alors $\wp A_{\wp'}$ est un idéal premier de $A_\wp$, lequel a pour seul idéal premier non nul son idéal maximal $\wp' A_{\wp'}$, d'où $\wp' = \wp$. Ainsi, A est de dimension ≤ 1. Par ailleurs, si un élément a de K est entier sur A, il l'est a fortiori sur tous les $A_\wp$, et il est donc dans tous les $A_\wp$ (puisque ceux-ci sont intégralement clos), ce qui implique $a \in A$ (si on écrit $a = b/c$ avec b, c dans A et $c \neq 0$, l'idéal des x tels que $xb \subset cA$ n'est dans aucun idéal premier, donc c'est A tout entier).

Si maintenant A est noethérien, intégralement clos, et de dimension ≤ 1, on a en fait que tout localisé $S^{-1}A$ de A par rapport à une partie multiplicative S de A possède également ces propriétés : c'est classique pour noethérien ; le fait que $S^{-1}A$ reste de dimension 1 résulte de ce que $\wp \mapsto \wp(S^{-1}A)$ est une bijection de l'ensemble des idéaux premiers de A ne rencontrant pas S sur l'ensemble des idéaux premiers de $S^{-1}A$. Enfin, le passage aux anneaux de fractions commute à la fermeture intégrale : plus précisément, si $x \in K$ est entier sur $S^{-1}A$, on obtient une relation du type

$$sx^n + a_1 x^{n-1} + ... + a_n = 0$$

avec les a_i dans A et $s \in S$. En multipliant par s^{n-1}, on trouve que sx est entier sur A, donc $sx \in A$, donc $x \in S^{-1}A$, ce qui implique que $S^{-1}A$ reste normal. Ainsi, $A_\wp$ est un a.v.d. pour tout idéal premier non nul $\wp$ de A par le théorème 1.14, donc A est bien un anneau de Dedekind.

□

Exemple 1.18 a) Tout anneau principal est un anneau de Dedekind.

b) Si A est un anneau de Dedekind et S une partie multiplicative de A, le localisé $S^{-1}A$ est un anneau de Dedekind.

c) On verra (théorème 2.6) que si K est un corps de nombres (i.e. une extension finie de $\mathbf{Q}$), l'anneau $\mathcal{O}_K$ des entiers de K (i.e. l'ensemble des éléments de K entiers sur $\mathbf{Z}$) est un anneau de Dedekind. Ceci n'implique pas que $\mathcal{O}_K$ soit principal, ni même factoriel, comme le montre l'exemple de $\mathbf{Z}[\sqrt{-5}]$.

On aura souvent besoin dans la suite du lemme suivant :

Lemme 1.19 *Soit A un anneau. Soient M et N des A-modules vérifiant $M \subset N$. Alors $M = N$ si et seulement si $M_\wp = N_\wp$ pour tout idéal maximal $\wp$ de A. Si M_1 et M_2 sont des sous-modules d'un A-module M vérifiant $(M_1)_\wp \subset (M_2)_\wp$ pour tout idéal maximal $\wp$ de A, alors $M_1 \subset M_2$.*

Démonstration : Comme la localisation est un foncteur exact, il suffit de montrer (en appliquant ensuite le résultat à M/N) que si $M \neq \{0\}$, il existe un idéal maximal $\wp$ de A tel que $M_\wp \neq 0$. Soit x non nul dans M et soit $I = \{a \in A, ax = 0\}$ son annulateur. Alors $I \neq A$, donc par le théorème de Krull I est contenu dans un certain idéal maximal $\wp$. Alors xA est isomorphe à A/I, avec $(A/I)_\wp \neq 0$ (puisque I ne rencontre pas le complémentaire de $\wp$, la classe de 1 dans $(A/I)_\wp$ est non nulle). Ainsi $(xA)_\wp \neq 0$, et a fortiori $M_\wp \neq 0$.

La seconde assertion résulte de la première appliquée à $M_2 \subset (M_1 + M_2)$. □

Proposition 1.20 *Soit A un anneau de Dedekind de corps des fractions K. Alors :*

a) Tout idéal fractionnaire non nul de A est inverible.

b) Les idéaux fractionnaires non nuls de A forment un groupe pour la multiplication, appelé groupe des idéaux de A. On le note $I(A)$.

Démonstration : a) On observe d'abord que dans un a.v.d. R d'uniformisante π, tout idéal fractionnaire est de la forme $\pi^n R$ avec $n \in \mathbf{Z}$, qui admet pour inverse $\pi^{-n}A$. Soit maintenant I un idéal fractionnaire de A, définissons $I' = (A : I)$ comme dans la proposition 1.11. Alors, si $\wp$ est un idéal premier de A, on a $I'_\wp = (A_\wp : I_\wp)$: en effet I est de type fini, vu que A est noethérien, ce qui permet d'écrire $I = \sum_{i=1}^r x_i A$ avec x_i non nul dans A, puis

$$(A : I)_\wp = (\bigcap_{i=1}^r (A : x_i A))_\wp = \bigcap_{i=1}^r (A : x_i A)_\wp$$

car la localisation commute avec les intersections finies. On en déduit

$$(A : I)_\wp = \bigcap_{i=1}^r (x_i^{-1} A)_\wp = \bigcap_{i=1}^r x_i^{-1} A_\wp = (A_\wp : \sum_{i=1}^r x_i A_\wp) = (A_\wp : I_\wp)$$

comme on voulait. D'où alors

$$(II')_\wp = I_\wp I'_\wp = I_\wp (I_\wp)' = A_\wp$$

pour tout $\wp$, ce qui donne $II' = A$ via le lemme 1.19.

b) résulte immédiatement de a).

□

Remarque 1.21 Réciproquement, un anneau intègre A dans lequel tout idéal fractionnaire non nul est inversible est bien un anneau de Dedekind. En effet A est noethérien (vu que tout idéal inversible est de type fini) et $A_\wp$ est donc un anneau de valuation discrète pour tout idéal premier $\wp$ non nul de A via le lemme 1.12, vu que son idéal maximal $\wp A_\wp$ a pour inverse $\wp' A_\wp$, où $\wp'$ est l'inverse de $\wp$ dans A.

Lemme 1.22 *Soit A un anneau de Dedekind. Soit x non nul dans A. Alors il n'y a qu'un nombre fini d'idéaux premiers qui contiennent x. En particulier, si $y \in K^*$, on a $v_\wp(y) = 0$ pour presque tout idéal premier $\wp$ non nul de A, où $v_\wp$ est la valuation de $A_\wp$.*

Démonstration : On observe d'abord que les idéaux de A qui contiennent x vérifient la condition de chaîne descendante. En effet, si on a des inclusions d'idéaux

$$xA \subset I \subset J \subset A,$$

on a des inclusions d'idéaux fractionnaires

$$A \subset J^{-1} \subset I^{-1} \subset x^{-1}A,$$

or l'anneau A est noethérien et le A-module $x^{-1}A$ est de type fini. Du coup, si x est contenu dans des idéaux premiers non nuls $\wp_1, ..., \wp_r, ...$, la suite décroissante

$$\wp_1 \supset \wp_1 \cap \wp_2 \supset ... \supset \bigcap_{i=1}^{r} \wp_i \supset ...$$

est stationnaire, ce qui donne un entier k tel que pour tout $j \geq k$, on a :

$$\wp_j \supset \bigcap_{i=1}^{k} \wp_i \supset \prod_{i=1}^{k} \wp_i,$$

ce qui implique que $\wp_j$ (qui est premier) contient l'un des $\wp_1, ..., \wp_k$, donc est l'un d'eux puisque A est de dimension ≤ 1. La deuxième assertion s'obtient en écrivant $y = x/z$ avec x, z non nuls dans A.

□

On arrive enfin à l'analogue pour un anneau de Dedekind de la décomposition en produits de facteurs irréductibles dans un anneau factoriel :

Theorème 1.23 *Soit A un anneau de Dedekind. Tout idéal fractionnaire non nul I de A s'écrit de manière unique*

$$I = \prod_{\wp} \wp^{v_\wp(I)},$$

où $\wp$ décrit l'ensemble des idéaux premiers non nuls de A et la famille des entiers $(v_\wp(I))$ est presque nulle.

Démonstration : On sait que I est contenu dans yA avec y non nul dans A. Le lemme 1.22 donne alors que I et I^{-1} ne sont contenus que dans un nombre fini d'idéaux premiers de A. Du coup, le localisé $I_\wp$ de I est de la forme $(\wp A_\wp)^{v_\wp(I)}$, avec $v_\wp(I) \in \mathbf{Z}$ et la famille des entiers $(v_\wp(I))$ est presque nulle. On voit alors que les trois idéaux fractionnaires I, $\prod_\wp \wp^{v_\wp(I)}$, et l'ensemble des x tel que $v_\wp(x) \geq v_\wp(I)$ pour tout $\wp$, sont égaux, car leur localisé (en tant que sous $A_\wp$-module de K) est le même pour tout $\wp$. Le résultat en découle. □

Corollaire 1.24 *Soient I et J deux idéaux fractionnaires non nuls d'un anneau de Dedekind A. Alors, pour tout idéal premier non nul $\wp$ de A et tout x non nul de A, on a :*

$$v_\wp(IJ) = v_\wp(I) + v_\wp(J);\ v_\wp(I+J) = \min(v_\wp(I), v_\wp(J));\ v_\wp(I^{-1}) = -v_\wp(I);$$

$$v_\wp(xA) = v_\wp(x).$$

Définition 1.25 Soit A un anneau de Dedekind. Le quotient du groupe des idéaux fractionnaires non nuls $I(A)$ par les idéaux fractionnaires principaux (i.e. ceux de la forme aA avec $a \in K^*$) s'appelle le *groupe des classes d'idéaux* de A. On le note $\mathrm{Cl}(A)$. Il est trivial si et seulement si A est principal. On verra plus tard que si K est un corps de nombres, le groupe des classes de son anneau d'entiers est fini.

Exercice 1.26 Montrer que si un anneau de Dedekind A est factoriel, il est principal (on pourra commencer par montrer que si $\wp$ est un idéal premier non nul de A, alors il existe un élément irréductible p de A qui engendre $\wp$).

On termine ce paragraphe par un lemme qui sera souvent utile par la suite :

Lemme 1.27 *Soit A un anneau de Dedekind. Soit $\wp$ un idéal premier non nul de A. Soit I un idéal fractionnaire non nul de A. Alors les A-modules $I/I\wp$ et $A/\wp$ sont isomorphes.*

Démonstration : Le A-module $I/I\wp$ est simple car comme I est inversible et $\wp$ maximal dans A, il n'y a pas de A-module strictement compris entre $I\wp$ et I. Ainsi $I/I\wp$ est engendré par n'importe lequel de ses éléments non nuls, et donc isomorphe à A/J avec J idéal de A distinct de A. Mais comme $I/I\wp$ est annulé par $\wp$, on a $\wp \subset J$, d'où $J = \wp$ puisque $\wp$ est maximal.

□

2. Extensions d'anneaux de Dedekind, ramification

2.1. Rappels sur les normes et traces

Soit L/K une extension finie de corps. Pour tout $\alpha \in L$, on note m_α la multiplication par α dans L, qui est une application K-linéaire.

Définition 2.1 La *norme* de α est le déterminant de m_α. Sa *trace* est la trace de m_α. On les note respectivement $N_{L/K}(\alpha)$ et $\mathrm{Tr}_{L/K}(\alpha)$ (ou simplement $N(\alpha)$ et $\mathrm{Tr}(\alpha)$ si l'extension L/K est sous-entendue).

En particulier, la trace est une application K-linéaire de L dans L et la norme est multiplicative. L'application $\mathrm{Tr}_{L/K}$ est nulle dès que L/K n'est pas séparable (se ramener à une extension radicielle). Si L/K est séparable et M est la clôture galoisienne de L sur K, alors $\mathrm{Tr}_{L/K}(\alpha)$ est la somme des conjugués de α (qui sont dans M) sur K et $N_{L/K}(\alpha)$ est leur produit, vu que ces conjugués sont les racines distinctes du polynôme minimal de α (qui est aussi celui de m_α).

Proposition 2.2 *Supposons l'extension L/K séparable. Alors la forme K-bilinéaire $b_{L/K} : (x, y) \mapsto \mathrm{Tr}(xy)$ est non dégénérée sur L.*

Noter que l'énoncé est évident en caractéristique zéro, car pour tout x non nul, $\mathrm{Tr}(x.x^{-1}) = \mathrm{Tr}(1) = [L : K]$ est non nul. Voir la proposition 12 de [1], §10, no 6 pour le cas général.

Si maintenant A est une K-algèbre de dimension finie (dont on sait qu'elle est isomorphe à un produit $\prod_{i=1}^{r} A/\wp_i^{m_i}$, où les $\wp_i$ sont les idéaux maximaux de A et $m_i \geq 1$), on définit de même la forme bilinéaire $b_{A/K}$ sur A en posant $b_{A/K}(x, y) = \mathrm{Tr}_{A/K}(xy)$, où pour $a \in A$, $\mathrm{Tr}_{A/K}(a)$ est la trace de la multiplication par a dans A. On étend alors facilement la proposition précédente :

Proposition 2.3 *La forme $b_{A/K}$ est non dégénérée si et seulement si A est une K-algèbre séparable (i.e. un produit de corps qui sont des extensions séparables de K).*

La proposition suivante, bien que s'appliquant aux anneaux normaux de dimension quelconque, sera surtout utile pour les anneaux de Dedekind :

Proposition 2.4 *Soit A un anneau noethérien et normal, de corps des fractions K. Soit L une extension finie de K. Soit B la fermeture intégrale de A dans L. Supposons L/K séparable. Alors B est un A-module de type fini.*

Notons que $K.B = L$ via le fait que la fermeture intégrale commute à la localisation, en particulier $L = \mathrm{Frac}\, B$.

Démonstration : Pour tout x de B, $\mathrm{Tr}_{L/K}(x)$ est dans A : en effet, si F est une clôture galoisienne de L sur K, on a

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

et si x annule un polynôme unitaire de $A[X]$, c'est aussi le cas de chaque $\sigma(x)$, ce qui montre que $\mathrm{Tr}_{L/K}(x)$ est un élément de K qui est entier sur A, or A est normal.

Soit $\mathcal{B} = (e_1, ..., e_n)$ une base du K-espace vectoriel L, on peut supposer que les e_i sont dans B (quitte à multiplier tous les e_i par un λ non nul de B, ce qui ne change pas le caractère libre sur K de la famille). Soit V le A-module engendré par les e_i, il est libre de base $\mathcal{B}$. Pour tout sous A-module M de L, notons $M^\vee$ le A-module constitué des $x \in L$ tels que $\mathrm{Tr}_{L/K}(xy) \in A$ pour tout $y \in M$. On a clairement

$$V \subset B \subset B^\vee \subset V^\vee.$$

Mais $V^\vee$ est libre de type fini (de base la base duale de $\mathcal{B}$ relativement à la forme bilinéaire non dégénéréee $\mathrm{Tr}_{L/K}$), donc B est un A-module de type fini vu que A est noethérien.

□

Remarque : a) Noter que la preuve montre aussi que $B^\vee$ (qui est un B-module) est de type fini sur A (et a fortiori sur B).

b) Si on ne suppose pas L/K séparable, on a encore des cas où on peut conclure que B est un A-module de type fini ; c'est le cas par exemple si A est

une algèbre de type fini sur un corps, ou si c'est un anneau local noethérien complet (les deux sont des exemples d'*anneaux de Nagata*, cf. [3], chapitre 12). On verra plus tard (théorème 4.20) le cas particulier où A est un a.v.d. complet.

Définition 2.5 Soit L/K une extension finie. Pour toute base $\mathcal{B}$ du K-espace vectoriel L, on note $\Delta_{L/K}(\mathcal{B})$ (ou simplement $\Delta(\mathcal{B})$ si L et K sont sous-entendus) le déterminant de la forme bilinéaire $b_{L/K}$ dans la base $\mathcal{B}$.

2.2. Extensions d'anneaux de Dedekind ; exemples

Theorème 2.6 *Soit A un anneau de Dedekind de corps des fractions K. Soient L une extension finie de K et B la fermeture intégrale de A dans L. On suppose que B est un A-module de type fini (c'est le cas si par exemple L/K est séparable). Alors, B est un anneau de Dedekind.*

Démonstration : On sait déjà que B est intégralement clos (comme fermeture intégrale), et noethérien (car de type fini sur un anneau noethérien). Reste à montrer que B est de dimension ≤ 1. Comme A est de dimension ≤ 1, il suffit de montrer le

Lemme 2.7 *Soit A un anneau. Soit B une A-algèbre, on suppose B entier sur A. Si I et J sont des idéaux distincts de B avec I premier et $I \subset J$, alors les idéaux images réciproques de I et J dans A (qu'on notera pour simplifier $I \cap A$ et $J \cap A$) sont distincts.*

Preuve du lemme : Quitte à remplacer B par B/I et J par J/I, on peut supposer $I = 0$ avec B intègre, et tout revient alors à montrer que si J est non nul, $J \cap A$ est non nul. Prenons x non nul dans J, alors il vérifie une équation du type

$$x^n + a_{n-1}x^{n-1} + ... + a_0 = 0,$$

avec les a_i dans A, équation qu'on peut prendre de degré minimal. En particulier $a_0 \neq 0$ par intégrité de B, mais l'image de a_0 dans B est aussi dans J via l'équation, donc a_0 est un élément non nul de $J \cap A$.

□

Remarque 2.8 Sous les hypothèses du théorème, le A-module B est projectif (=facteur direct d'un A-module libre ; c'est équivalent aussi à dire que B est plat sur A, vu que B est de type fini et A noethérien). En effet B est localement libre (pour tout idéal premier $\wp$ de A, le $A_\wp$-module $B \otimes_A A_\wp$ est sans torsion car B l'est et la localisation est un foncteur exact) et de type fini sur l'anneau principal $A_\wp$, donc libre), et on applique [4], théorème I.2.9.

Exercice 2.9 Soit A un anneau de Dedekind de corps des fractions K. Soit L/K une extension finie séparable. Soit B un sous-anneau de L contenant A. On suppose que B est un A-module de type fini et qu'il vérifie l'hypothèse :

(*) Il existe une K-base $\mathcal{B} = (e_1, ..., e_n)$ de L, constituée d'élements de B, tel que pour tout idéal premier non nul $\wp$ de A on ait $v_\wp(\Delta_{L/K}(\mathcal{B})) \leq 1$.

Soit C la fermeture intégrale de B dans L. On se propose de montrer que $B = C$, c'est-à-dire que B est la fermeture intégrale de A dans L.

a) Soit $M = \bigoplus_{i=1}^n Ae_i$. Montrer que $M \subset B \subset C$.

b) Soit $\wp$ un idéal premier non nul de A. Montrer que les localisés $M_\wp$ et $C_\wp$ sont des $A_\wp$-modules libres de même rang.

c) Soit $\mathcal{B}' = (f_1, ..., f_n)$ une base du $A_\wp$-module $C_\wp$. Soit P la matrice de passage de $\mathcal{B}'$ à $\mathcal{B}$. Montrer que $P \in M_n(A_\wp)$, puis que $v_\wp(\det P) = 0$.

d) En déduire que $M_\wp = C_\wp$ et conclure.

Définition 2.10 Un *corps de nombres* K est une extension finie du corps $\mathbf{Q}$. L'*anneau des entiers* de K (noté $\mathcal{O}_K$) est la fermeture intégrale de $\mathbf{Z}$ dans K.

D'après le théorème 2.6, l'anneau $\mathcal{O}_K$ est de Dedekind et c'est aussi un $\mathbf{Z}$-module de type fini. Comme il est sans torsion sur l'anneau principal $\mathbf{Z}$, c'est un $\mathbf{Z}$-module libre (de rang $n := [K : \mathbf{Q}]$ car $\mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Q} \simeq K$, vu que la localisation commute avec le produit tensoriel).

Proposition 2.11 *Soit K un corps de nombres d'anneau des entiers $\mathcal{O}_K$. Soit I un idéal non nul de $\mathcal{O}_K$. Alors $\mathcal{O}_K/I$ est fini, son cardinal est appelé norme (absolue) de I.*

Démonstration : On sait que $I \cap \mathbf{Z}$ contient un élément non nul d (lemme 2.7). Alors I contient $d\mathcal{O}_K$, qui est un $\mathcal{O}_K$-module libre de rang 1, donc un $\mathbf{Z}$-module libre de rang n, ce qui implique (comme $\mathcal{O}_K$ est aussi libre de rang n sur $\mathbf{Z}$) que $\mathcal{O}_K/d\mathcal{O}_K$ est fini via le théorème de la base adaptée pour les modules sur l'anneau principal $\mathbf{Z}$. A fortiori, $\mathcal{O}_K/I$ est fini.

□

Définition 2.12 Soit K un corps de nombres. Le *discriminant* (absolu) de K est le déterminant Δ_K de la matrice de la forme bilinéaire $b_{K/\mathbf{Q}}$ dans une base du $\mathbf{Z}$-module libre $\mathcal{O}_K$.

Noter que ce déterminant ne dépend pas de la base choisie, car la matrice de passage d'une base à une autre est inversible dans $\mathbf{Z}$, donc de déterminant ± 1, donc le carré de son déterminant est 1. Les notions de norme et de discriminant seront généralisées au paragraphe 3.1.

Remarque 2.13 Soit $(b_1, ..., b_n)$ une base du $\mathbf{Z}$-module libre $\mathcal{O}_K$. Notons $\sigma_1, ..., \sigma_n$ les plongements de K dans $\mathbf{C}$ (il y en a bien n via le théorème de l'élément primitif). Alors, la matrice de la forme trace $b_{K/\mathbf{Q}}$ dans cette base est $B^t B$, où B est la matrice $(\sigma_i(b_j))$. Du coup, le discriminant Δ_K est le carré du déterminant de B. Si on suppose de plus qu'il existe $b \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbf{Z}[b]$, alors on peut choisir la base $(1, b, ..., b^{n-1})$, et B est juste la matrice de Van der Monde des racines $\alpha_1, ..., \alpha_n$ du polynôme minimal P de b. On a donc dans ce cas :

$$\Delta_K = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2,$$

c'est-à-dire que c'est le discriminant du polynôme P au sens usuel.

Exercice 2.14 Soit $K = \mathbf{Q}(\sqrt{d})$, où $d \neq 0, 1$ est un entier sans facteur carré. Montrer que $\mathcal{O}_K = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ si d est congru à 1 modulo 4, et $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$ si d est congru à 2 ou 3 modulo 4. Calculer le discriminant de K dans les deux cas.

Exercice 2.15 a) On considère $K = \mathbf{Q}(x)$, où x est une racine du polynôme $X^3 - X + 1$. Utiliser l'exercice 2.9 pour montrer que $\mathcal{O}_K = \mathbf{Z}[x]$.

b) Soit $K = \mathbf{Q}(\sqrt[3]{2})$. Utiliser l'exercice 2.9 pour montrer que $\mathbf{Z}[\sqrt[3]{2}]_{(p)} = (\mathcal{O}_K)_{(p)}$ si p est un nombre premier distinct de 2 et 3, puis vérifier que cela vaut aussi si $p = 2$ ou 3 (cf. exercice 1.15). En déduire que $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$.

2.3. Décomposition des idéaux dans une extension, ramification

On se place dans ce paragraphe sous les hypothèses du théorème 2.6, c'est-à-dire que A est un anneau de Dedekind de corps des fractions K, L est une extension finie de degré n de K, et B est la fermeture intégrale de A dans L, qui est un anneau de Dedekind et un A-module de type fini.

Définition 2.16 Soit $\mathfrak{q}$ un idéal premier non nul de B. On dit que $\mathfrak{q}$ *divise* l'idéal premier $\wp$ de A (ou *est au dessus* de $\wp$) si $\mathfrak{q} \cap A = \wp$. On note alors $\mathfrak{q} | \wp$.

Autrement dit, $\mathfrak{q}$ divise $\wp$ si et seulement s'il contient l'idéal $\wp B$ engendré par $\wp$ dans B.

Définition 2.17 Pour tout $\wp$ de A, écrivons la décomposition

$$\wp B = \prod_{\mathfrak{q}|\wp} \mathfrak{q}^{e_\mathfrak{q}}.$$

L'entier strictement positif $e_\mathfrak{q}$ (qu'on notera aussi $e_{\mathfrak{q}/\wp}$ s'il y a ambiguité) s'appelle *l'indice de ramification* de $\mathfrak{q}$ dans l'extension L/K. Le degré (fini vu que B est un A-module de type fini) $f_\mathfrak{q} := [B/\mathfrak{q} : A/\wp]$, où $\wp = \mathfrak{q} \cap A$, s'appelle le *degré résiduel* de $\mathfrak{q}$. On dit que l'extension L/K est *totalement ramifiée* en $\wp$ s'il y a un seul idéal premier $\mathfrak{q}$ au-dessus de $\wp$ avec de plus $f_\mathfrak{q} = 1$. Elle est dite *non ramifiée* en $\mathfrak{q}$ si $e_\mathfrak{q} = 1$ avec de plus $B/\mathfrak{q}$ extension séparable de $A/\wp$, et non ramifiée en $\wp$ (ou au-dessus de $\wp$) si elle est non ramifiée en tous les $\mathfrak{q}$ qui divisent $\wp$.

On va voir qu'il y a des relations entre les entiers $e_\mathfrak{q}$ et $f_\mathfrak{q}$. On démontre d'abord deux résultats utiles en eux-mêmes, sorte de généralisation du théorème des restes chinois :

Lemme 2.18 *a) Soit A un anneau. Soient I et J deux idéaux de A tels que $I + J = A$. Alors, l'application naturelle*

$$A/IJ \to A/I \times A/J$$

est un isomorphisme d'anneaux.

b) Soient $\wp_1$, $\wp_2$, $\wp_r$ des idéaux maximaux deux à deux distincts de A. Soient $n_1, ..., n_r \in \mathbf{N}^*$. Alors

$$\wp_i^{n_i} + \prod_{j \neq i} \wp_j^{n_j} = A \tag{1}$$

et l'application naturelle

$$A/\prod_{i=1}^{k} \wp_i^{n_i} \to \prod_{i=1}^{k} A/\wp_i^{n_i} \tag{2}$$

est un isomorphisme.

Démonstration : a) On observe que $IJ = I \cap J$ ($IJ \subset I \cap J$ est évident, et si on écrit $1 = i + j$ avec $i \in I$ et $j \in j$, alors tout élément x de $I \cap J$ s'écrit $x = xi + xj$ avec xi et xj dans IJ), d'où l'injectivité de l'application. Si maintenant x_1 et x_2 sont dans A, alors $x_1 j + x_2 i$ est un élément de A qui est congru à x_1 modulo I et à x_2 modulo J, d'où la surjctivité.

b) Si on n'avait pas (1), alors par le théorème de Krull il existerait un idéal maximal $\mathcal{M}$ de A contenant l'idéal $\wp_i^{n_i} + \prod_{j\neq i} \wp_j^{n_j}$. Comme $\mathcal{M}$ est premier, il contiendrait $\wp_i$ et l'un des $\wp_j$ pour $j \neq I$, donc il contiendrait $\wp_i + \wp_j = A$ (rappelons que $\wp_i$ et $\wp_j$ sont des idéaux maximaux distincts de A), ce qui est impossible. L'isomorphisme (2) en résulte par récurrence sur k grâce à a).

□

Theorème 2.19 ("Lemme d'approximation") *Soit A un anneau de Dedekind. Soient $\wp_1, \wp_2, ..., \wp_k$ des idéaux premiers non nuls de A deux à deux distincts. On se donne des entiers $n_1, ..., n_k$. Il existe alors $x \in K$ vérifiant : $v_{\wp_i}(x - x_i) \geq n_i$ pour tout $i \in \{1, ..., k\}$ et $v_\wp(x) \geq 0$ pour $\wp$ idéal premier non nul de A distinct des $\wp_i$.*

Démonstration : On peut supposer les $n_i > 0$. Comme A est de Dedekind, les $\wp_i$ sont des idéaux maximaux de A. Supposons d'abord que les x_i sont dans A. Alors l'isomorphisme (2) fournit $x \in A$ congru à x_i modulo $\wp_i^{n_i}$ pour tout i, ce qui donne $v_{\wp_i}(x - x_i) \geq n_i$ (et $v_\wp(x) \geq 0$ pour les $\wp$ autre que l'un des $\wp_i$).

Dans le cas général, écrivons $x_i = a_i/s$ avec $a_i \in A$ et s non nul dans A. On cherche alors x sous la forme $x = a/s$ avec a dans A vérifiant

$$v_{\wp_i}(a - a_i) \geq n_i + v_{\wp_i}(s),\ 1 \leq i \leq k;\ v_\wp(a) \geq v_\wp(s), \wp \neq \wp_1, ..., \wp_k,$$

ce qui est possible d'après ce qui précède (en ajoutant aux $\wp_i$ si nécessaire des $\wp$ tels que $v_\wp(s) > 0$, lesquels sont en nombre fini).

□

Theorème 2.20 *Soit $\wp$ un idéal premier non nul de A. Alors $B/\wp B$ est une $A/\wp$-algèbre de degré $n = [L : K]$, isomorphe à $\prod_{\mathfrak{q}|\wp} B/\mathfrak{q}^{e_\mathfrak{q}}$. On a :*

$$n = \sum_{\mathfrak{q}|\wp} e_\mathfrak{q} f_\mathfrak{q}.$$

Démonstration : Pour calculer le rang de $B/\wp B$, on localise par rapport à $S = A - \wp$, en posant $A' = S^{-1}A$ et $B' = S^{-1}B$. On sait que A' est un a.v.d. dont B' est la fermeture intégrale dans L. On a $A'/\wp A' = A/\wp$ et $B'/\wp B' = B/\wp B$. Comme B est un A-module de type fini, B' est un A'-module de type fini, et comme il est sans torsion (avec A' principal), il est libre de rang $n = [L : K]$, d'où le premier point.

Le lemme 2.18 donne un isomorphisme

$$B/\wp B \simeq \prod_{\mathfrak{q}|\wp} B/\mathfrak{q}^{e_\mathfrak{q}},$$

d'où le deuxième point. En prenant les degrés sur $A/\wp$, on obtient $n = \sum_{\mathfrak{q}|\wp} n_{\mathfrak{q}}$, avec $n_{\mathfrak{q}} = [B/\mathfrak{q}^{e_{\mathfrak{q}}} : A/\wp]$. Maintenant, on a une filtration de $A/\wp$-espaces vectoriels

$$B/\mathfrak{q}^{e_{\mathfrak{q}}} \supset \mathfrak{q}/\mathfrak{q}^{e_{\mathfrak{q}}} \supset ... \supset \mathfrak{q}^{e_{\mathfrak{q}}-1}/\mathfrak{q}^{e_{\mathfrak{q}}} \supset \{0\}$$

dont tous les quotients successifs (au nombre de $e_{\mathfrak{q}}$) sont isomorphes à $B/\mathfrak{q}$ via le lemme 1.27. Finalement :

$$n_{\mathfrak{q}} = e_{\mathfrak{q}}[B/\mathfrak{q} : A/\wp] = e_{\mathfrak{q}} f_{\mathfrak{q}},$$

ce qui achève la preuve.

□

Le lemme suivant précise un peu la structure "locale" de $B/\wp B$:

Lemme 2.21 *Soit $\mathfrak{q}$ un idéal premier non nul de B, posons $\wp = A \cap \mathfrak{q}$ et notons $k(\wp) = A/\wp$ le corps résiduel de A en $\wp$. Alors le localisé $(B/\wp)_{\mathfrak{q}}$ est une $k(\wp)$-algèbre de dimension finie, isomorphe à $B/\mathfrak{q}^{v_{\mathfrak{q}}(\wp B)}$.*

Démonstration : On écrit la décomposition

$$\wp B = \prod_{\tau|\wp} \tau^{v_\tau(\wp B)},$$

ce qui avec le lemme 2.18 donne

$$B/\wp \simeq \prod_{\tau|\wp} B/\tau^{v_\tau(\wp B)},$$

puis $(B/\wp)_{\mathfrak{q}} \simeq B/\mathfrak{q}^{v_{\mathfrak{q}}(\wp B)}$ vu que chaque $B/\tau^{v_\tau(\wp B)}$ est un anneau local d'idéal maximal τ (dont le localisé en $\mathfrak{q}$ est donc nul si $\tau \neq \mathfrak{q}$, et est lui-même si $\tau = \mathfrak{q}$). C'est une $k(\wp)$-algèbre de dimension finie puisque B est un A-module de type fini.

□

Exercice 2.22 Soit A un anneau de Dedekind de corps des fractions K. Soit L une extension finie de K, on suppose que la fermeture intégrale de A dans L est de la forme $B = A[x]$. Soit P le polynôme minimal de x sur K.

a) Montrer que $P \in A[X]$.

Soit $\wp$ un idéal maximal de A, on note $\overline{P}$ la réduction de P dans $k(\wp)[X]$, où $k(\wp) = A/\wp$ est le corps résiduel en $\wp$. On écrit

$$\overline{P} = \prod_{i=1}^{r} P_i^{e_i}$$

la factorisation de $\overline{P}$ en produit de polynômes irréductibles deux à deux distincts, et pour chaque i on relève P_i en un $\widetilde{P}_i \in A[X]$.

b) Soit $\mathfrak{q}_i$ l'idéal $\wp B + (\widetilde{P}_i(x))$ de B. Montrer que les idéaux maximaux de B divisant $\wp$ sont les $\mathfrak{q}_i$ (on pourra calculer $B/\wp B$).

c) Montrer plus précisément que la décomposition de l'idéal $\wp B$ est

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

(on pourra utiliser le lemme 2.18).

d) Utiliser ce qui précède pour donner la décomposition de l'idéal (11) dans $\mathcal{O}_K$, où $K = \mathbf{Q}(\sqrt{5})$.

e) Soit $K = \mathbf{Q}(\sqrt{17})$. Montrer que les idéaux de norme 2 de $\mathcal{O}_K$ sont principaux (on écrira d'abord la décomposition de l'idéal (2) dans $\mathcal{O}_K$). On peut en déduire que $\mathcal{O}_K$ est principal si on connaît une version précise de la finitude de $\mathrm{Cl}(\mathcal{O}_K)$.

2.4. Cas d'une extension galoisienne

On garde les hypothèses et notations du paragraphe précédent, mais on suppose de plus que l'extension L/K est galoisienne de groupe G. On va voir que dans ce cas, les formules se simplifient.

Proposition 2.23 *Soit $\wp$ un idéal premier non nul de A. Le groupe G opère transitivement sur l'ensemble des idéaux premiers $\mathfrak{q}$ qui divisent $\wp$.*

Démonstration : Choisissons $\mathfrak{q}$ au-dessus de $\wp$, et montrons par l'absurde qu'un $\mathfrak{q}'$ au-dessus de $\wp$ ne peut pas être distinct de tous les $g(\mathfrak{q}), g \in G$. Si c'était le cas, le lemme d'approximation donnerait un élément $a \in \mathfrak{q}'$ avec $a \notin g(\mathfrak{q})$ pour tout $g \in G$. Alors l'élément $x = N_{L/K}(a)$ est dans A, mais $x = \prod_{g\in G} g(a)$ serait dans $\mathfrak{q}'$ et pas dans $\mathfrak{q}$, ce qui contredit $\wp = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. □

Corollaire 2.24 *Soit $\wp$ idéal premier non nul de A. Pour $\mathfrak{q}$ divisant $\wp$, les entiers $e_\mathfrak{q}$ et $f_\mathfrak{q}$ ne dépendent que de $\wp$. En les notant $e_\wp$ et $f_\wp$, on a*

$$[L : K] = e_\wp f_\wp g_\wp,$$

où $g_\wp$ est le nombre d'idéaux premiers de B au-dessus de $\wp$.

En effet, si $\wp B = \prod_{\mathfrak{q}|\wp} \mathfrak{q}^{e_\mathfrak{q}}$, on a pour tout $g \in G$:

$$g(\wp B) = \wp B = \prod_{\mathfrak{q}|\wp} g(\mathfrak{q})^{e_\mathfrak{q}}.$$

Il suffit alors d'appliquer la proposition 2.23 et l'unicité de la décomposition.

Définition 2.25 Soient $\mathfrak{q}$ un idéal premier non nul de B et $\wp := \mathfrak{q} \cap A$. Le *groupe de décomposition* $D_\mathfrak{q}$ de $\mathfrak{q}$ est le sous-groupe de G constitué des g tels que $g(\mathfrak{q}) = \mathfrak{q}$.

Remarque 2.26 Si $\mathfrak{q}$ et $\mathfrak{q}'$ sont au-dessus du même $\wp$, alors la proposition 2.23 dit qu'il existe $g \in G$ tel que $g(\mathfrak{q}) = \mathfrak{q}'$, d'où $D_{\mathfrak{q}'} = gD_\mathfrak{q}g^{-1}$. En particulier, si le groupe de Galois G est abélien, le groupe de décomposition de $\mathfrak{q}$ ne dépend que de $\wp$.

Posons $k(\wp) = A/\wp$ et $k(\mathfrak{q}) = B/\mathfrak{q}$ (ce sont aussi les corps résiduels respectifs des a.v.d. $A_\wp$ et $B_\mathfrak{q}$). Pour $g \in D_\mathfrak{q}$, on note $\bar{g}$ le $k(\wp)$-automorphisme de $k(\mathfrak{q})$ induit par g.

Theorème 2.27 *On suppose de plus que l'extension $k(\mathfrak{q})/k(\wp)$ est séparable. Alors elle est galoisienne et l'application $u : g \mapsto \bar{g}$ induit un morphisme surjectif du groupe $D_\mathfrak{q}$ sur* $\mathrm{Gal}\,(k(\mathfrak{q})/k(\wp))$.

Démonstration : Soit $x \in k(\mathfrak{q})$, qu'on relève en un $\tilde{x} \in B$. Le polynôme $P = \prod_{g\in G}(X - g(\tilde{x}))$ est dans $A[X]$ car ses coefficients sont dans K (vu que $\sigma.P = P$ pour tout $\sigma \in G$) et dans B (donc entiers sur A, avec A normal). Ce polynôme est donc scindé dans L, avec ses racines dans B. La réduction modulo $\wp$ de P est un polynôme de $k(\wp)[X]$, scindé sur $k(\mathfrak{q})$ et qui annule x, ce qui prouve que le polynôme minimal de x sur $k(\wp)$ (qui divise cette réduction) est scindé sur $k(\mathfrak{q})$. Ceci montre que l'extension $k(\mathfrak{q})/k(\wp)$ est normale, et donc galoisienne puisqu'elle est supposée séparable. On a en fait montré que tout conjugué de x sur $k(\wp)$ est la réduction modulo $\mathfrak{q}$ d'un conjugué de $\tilde{x}$ sur K.

Montrons maintenant que u est surjective. On peut choisir $y \in k(\mathfrak{q})$ tel que $k(\mathfrak{q}) = k(\wp)[y]$ via le théorème de l'élément primitif, puis relever y en un $\tilde{y} \in B$. Soit $E = G - D_\mathfrak{q}$. Comme l'idéal premier $\mathfrak{q}$ est distinct des $g(\mathfrak{q})$ pour $g \in E$, on a

$$B = \mathfrak{q} + \prod_{g\in E} g(\mathfrak{q})$$

via le lemme 2.18. On peut donc écrire $\tilde{y} = y_1 + y_2$ avec $y_1 \in \mathfrak{q}$ et $y_2 \in \prod_{g\in E} g(\mathfrak{q})$. Ainsi y_2 est un relevé de y dans B qui vérifie $y_2 \in g(\mathfrak{q})$ si $g(\mathfrak{q}) \neq \mathfrak{q}$.

Soit alors $\tau \in \mathrm{Gal}\,(k(\mathfrak{q})/k(\wp))$. Alors $\tau(y)$ est conjugué de y sur $k(\wp)$, donc (comme observé ci-dessus) il admet un relevé dans B de la forme $\sigma(y_2)$ avec $\sigma \in G$. En particulier $\sigma(y_2) \notin \mathfrak{q}$, soit $y_2 \notin \sigma^{-1}(\mathfrak{q})$, d'où $\sigma \in D_\mathfrak{q}$. De plus $\bar{\sigma}$ et τ coïncident sur y par construction, donc sont égaux puisque $k(\mathfrak{q}) = k(\wp)[y]$.

□

Définition 2.28 Sous les hypothèses du théorème 2.27, le noyau $I_\mathfrak{q}$ du morphisme u s'appelle le *sous-groupe d'inertie* en $\mathfrak{q}$.

Proposition 2.29 *Le cardinal de $D_\mathfrak{q}$ est $e_\wp f_\wp$, et celui de $I_\mathfrak{q}$ est $e_\wp$.*

Démonstration : Le groupe G est de cardinal $e_\wp f_\wp g_\wp$, et opère transitivement sur l'ensemble des idéaux premiers au-dessus de $\wp$, qui est de cardinal $g_\wp$, ce qui fait que le stabilisateur $D_\mathfrak{q}$ de $\mathfrak{q}$ est de cardinal $e_\wp f_\wp$. La deuxième assertion résulte de la surjectivité de u, vu que le degré de l'extension résiduelle $k(\mathfrak{q})/k(\wp)$ est $f_\wp$.

□

Définition 2.30 On dit que l'extension L/K est *complètement décomposée* en $\wp$ si $e_\wp = f_\wp = 1$. Cela correspond au fait que $\wp B$ se décompose en le produit de $[L : K]$ idéaux premiers deux à deux distincts. Elle est dite *inerte* en $\wp$ si $e_\wp = g_\wp = 1$, ce qui correspond au fait que $\wp B$ reste un idéal premier. Ceci signifie que $\mathrm{Gal}\,(L/K)$ est isomorphe au groupe de Galois de l'extension résiduelle $k(\mathfrak{q})/k(\wp)$, il est en particulier cyclique si K est un corps de nombres vu que $k(\wp)$ est alors fini.

3. Extensions d'anneaux de Dedekind : compléments

3.1. Discriminant et différente

Dans ce paragraphe, A est un anneau de Dedekind de corps des fractions K, L est une extension finie séparable de K, et B est la fermeture intégrale de A dans L. En paticulier, B est un anneau de Dedekind et un A-module de type fini et le théorème 2.20 s'applique. Rappelons (remarque 2.1.) qu'en posant

$$M^\vee := \{x \in L, \mathrm{Tr}_{L/K}(xM) \subset A\}$$

pour tout A-module M, alors $B^\vee$ est un sous B-module de L contenant B, qui est de type fini comme A-module. Il s'agit donc d'un idéal fractionnaire non nul de B.

Définition 3.1 On appelle *différente* $\mathcal{D}_{B/A}$ de l'extension B/A l'inverse de $B^\vee$, qui est un idéal de B (en effet $B \subset B^\vee$, donc en prenant les inverses $\mathcal{D}_{B/A} \subset B$. De façon équivalente, $\mathcal{D}_{B/A}$ est l'idéal annulateur du B-module $B^\vee/B$).

Définition 3.2 Si $\mathfrak{q}$ est un idéal premier non nul de B au-dessus de l'idéal premier $\wp$ de A, on pose $N_{L/K}(\mathfrak{q}) = \wp^{f_\mathfrak{q}}$, où $f_\mathfrak{q}$ est le degré résiduel en $\mathfrak{q}$. On étend $N_{L/K}$ en un morphisme (appelé *norme*) $I(B) \to I(A)$ entre les groupes d'idéaux fractionnaires non nuls, en notant qu'$I(B)$ est le groupe abélien libre engendré par les idéaux premiers non nuls de B. On définit de même le morphisme d'*injection* $i_{L/K} : I(A) \to I(B)$ en posant $i_{L/K}(\wp) = \wp B$ pour tout idéal premier non nul $\wp$ de A.

Remarque 3.3 a) Dans le cas où $A = \mathbf{Z}$ et $B = \mathcal{O}_L$, on retrouve la définition de la norme absolue d'un idéal de $\mathcal{O}_L$, vu que pour tout idéal premier non nul $\mathfrak{q}$ de B, $B/\mathfrak{q}$ est de degré $f_\mathfrak{q}$ sur $\mathbf{Z}/p$, lequel est de cardinal p.

b) Soit I un idéal fractionnaire de B. Si L/K est galoisienne de groupe G, alors

$$i_{L/K}((N_{L/K}(I)) = \prod_{g \in G} g(I).$$

(il suffit de le vérifier quand $I = \mathfrak{q}$ est un idéal premier non nul de B, ce qui est facile via les propositions 2.29 et 2.23).

Définition 3.4 Avec les notations ci-dessus, l'*idéal discriminant* de l'extension B/A est $\Delta_{B/A} = N_{L/K}(\mathcal{D}_{B/A})$. C'est un idéal non nul de A.

Si A est un anneau principal et $M \subset N$ sont des A-réseaux (=A-modules libres de type fini) de même rang, alors on peut (via le théorème de la base adaptée) écrire la décomposition

$$N/M \simeq \prod_{i=1}^{n} A/(d_i),\ d_1|d_2|...|d_n$$

et on note alors $\mathcal{I}(N, M)$ l'idéal de A engendré par $\prod_{i=1}^n d_i$ (bien défini car les d_i sont uniques à inversible près dans $A - \{0\}$).

Lemme 3.5 *Soient $M \subset N \subset P$ trois A-réseaux de même rang. Alors*

$$\mathcal{I}(P, M) = \mathcal{I}(P, N).\mathcal{I}(N, M). \tag{3}$$

Démonstration : Cela résulte de ce que $\mathcal{I}(N, M)$ est aussi l'idéal engendré par le déterminant d'une matrice de passage d'une base de N à une base de M.

□

Proposition 3.6 *Si $I = (b)$ est un idéal fractionnaire principal non nul de B, alors sa norme est l'idéal fractionnaire principal $N(b)A$.*

Démonstration : Il suffit de vérifier le résultat après localisation en tout idéal premier non nul $\wp$ de A, et on peut donc supposer que A est principal. Par multiplicativité de la norme, on peut aussi supposer que $b \in B$. On écrit alors la décomposition

$$(b) = \prod_{i=1}^{r} \mathfrak{q}_i$$

de l'idéal (b) en produit d'idéaux premiers (pas forcément deux à deux distincts) de B. Si $\mathfrak{q}$ est un idéal premier non nul de B au-dessus de l'idéal $\wp$ de A, alors $B/\mathfrak{q}$ est un $A/\wp$-espace vectoriel de dimension $f_{\mathfrak{q}}$, d'où

$$\mathcal{I}(B, \mathfrak{q}) = \wp^{f_{\mathfrak{q}}} = N_{L/K}(\mathfrak{q}).$$

Par ailleurs, on a une chaîne de A-réseaux :

$$B \supset \mathfrak{q}_1 \supset \mathfrak{q}_1\mathfrak{q}_2 \supset ... \supset (b) = \prod_{i=1}^{r} \mathfrak{q}_i,$$

ce qui avec (3) donne finalement

$$\mathcal{I}(B, (b)) = \prod_{i=1}^{n} N_{L/K}(\mathfrak{q}_i) = N_{L/K}((b)),$$

vu que $B/\mathfrak{q}$ et $J/J\mathfrak{q}$ sont des B-modules isomorphes pour tout idéal J de B (lemme 1.27).

Maintenant, le théorème des diviseurs élémentaires dit que $\mathcal{I}(B, (b))$ est engendré par le déterminant de l'application A-linéaire m_b de B dans B, d'où finalement $\mathcal{I}(B, (b)) = N_{L/K}((b)) = N_{L/K}(b)A$ comme on voulait.

□

Lemme 3.7 *Soit S une partie multiplicative de A. Alors*

$$\mathcal{D}_{B/A}B_S = \mathcal{D}_{B_S/A_S};\ \Delta_{B/A}A_S = \Delta_{B_S/A_S}.$$

Démonstration : Par K-linéarité de $\mathrm{Tr}_{L/K}$, on a $(B_S)^\vee = (B^\vee)_S$, d'où la première assertion. La seconde en découle immédiatement, vu que

$$N_{L/K}(I)_S = N_{L/K}(I_S)$$

pour tout idéal I de B.

□

Proposition 3.8 *L'idéal discriminant $\Delta_{B/A}$ est engendré par les $\Delta(\mathcal{B})$, où $\mathcal{B}$ varie parmi les K-bases de L dont les éléments sont contenus dans B.*

Remarque 3.9 Supposons que le A-module projectif de type fini B admette une base $\mathcal{B}_0$ (ce qui est le cas par exemple si A est un anneau principal). Alors, l'idéal engendré par les $\Delta(\mathcal{B})$ pour $\mathcal{B}$ base de L sur K est simplement l'idéal principal engendré par $\Delta(\mathcal{B}_0)$ via la formule de changement de base pour les formes bilinéaires. En effet, la matrice de passage de $\mathcal{B}_0$ à $\mathcal{B}$ est à coefficients dans A. Quand $A = \mathbf{Z}$, on retrouve donc la définition du discriminant absolu d'un corps de nombres K comme générateur de l'idéal $\Delta_{\mathcal{O}_K/\mathbf{Z}}$.

Preuve de la proposition 3.8 : Soit I l'idéal de A engendré par les $\Delta(\mathcal{B})$ pour $\mathcal{B}$ décrivant les K-bases de L dont les éléments sont dans B. Il suffit de montrer que pour tout idéal premier non nul $\wp$ de A, les localisés $I_\wp$ et $(\Delta_{B/A})_\wp$ coïncident. Or, $(\Delta_{B/A})_\wp = \Delta_{B_\wp/A_\wp}$ (lemme 3.7) et $I_\wp$ est l'idéal engendré par $\Delta(\mathcal{B}_0)$, où $\mathcal{B}_0$ est une base du $A_\wp$-module $B_\wp$ (remarque 3.9). On se ramène donc à prouver la proposition quand A est un anneau de valuation discrète, d'idéal premier $\wp = (\pi)$.

Comme A est principal, on peut trouver une base $(e_1, ..., e_n)$ du A-module $B^\vee$ et des éléments non nuls $d_1|...|d_n$ de A tels que $(d_1e_1, ..., d_ne_n)$ soit une base du A-module B. Soit $\mathcal{B}^* = (e_1^*, ...e_n^*)$ la base duale de $(e_1, ..., e_n)$ (relativement à $b_{L/K}$), c'est aussi une base du A-module B. On sait (remarque 3.9) que I est engendré par le déterminant de $b_{L/K}$ dans la base $\mathcal{B}^*$, mais comme la matrice de passage de $\mathcal{B}^*$ à $(d_1e_1, ..., d_ne_n)$ est dans $\mathrm{GL}_n(A)$, c'est aussi le déterminant de la matrice $(b_{L/K}(e_i^*, d_je_j))$. Ainsi

$$I = (\prod_{j=1}^{n} d_j)A.$$

Écrivons maintenant la décomposition

$$\mathcal{D}_{B/A} = \mathfrak{q}_1...\mathfrak{q}_r$$

en produit d'idéaux premiers (pas forcément distincts) de B. Comme $B = B^\vee \mathcal{D}_{B/A}$, le B-module $B^\vee/B$ possède une filtration

$$B^\vee/B \supset B^\vee\mathfrak{q}_1/B \supset B^\vee\mathfrak{q}_1\mathfrak{q}_2/B \supset ... \supset B^\vee\mathcal{D}_{B/A}/B = \{0\}$$

dont les quotients successifs sont isomorphes à $B/\mathfrak{q}_i$ via le lemme 1.27. Comme les diviseurs élémentaires de $B/\mathfrak{q}_i$ sont $(\pi, ..., \pi)$ (où π apparaît $f_{\mathfrak{q}_i}$ fois), le produit des diviseurs élémentaires du A-module $B^\vee/B$ est $\pi^{\sum_{i=1}^r f_{\mathfrak{q}_i}}$, qui engendre l'idéal $N_{L/K}(\mathcal{D}_{B/A})$. Comme ce produit est aussi $\prod_{j=1}^n d_j$ par définition des d_j, on obtient finalement

$$\Delta_{B/A} = N_{L/K}(\mathcal{D}_{B/A}) = (\prod_{j=1}^{n} d_j) = I.$$

□

Lemme 3.10 *Soit $\mathfrak{q}$ un idéal premier non nul de B, posons $\wp = A \cap \mathfrak{q}$ et notons $k(\wp) = A/\wp$ le corps résiduel de A en $\wp$. Notons $B/\wp := B/\wp B$. Soit u le morphisme induit par la trace de $(B/\wp)_\mathfrak{q}$ dans son dual (en tant que $k(\wp)$-espace vectoriel) $(B/\wp)_\mathfrak{q}^D$. Alors $\mathcal{D}_{B/A} \subset \mathfrak{q}$ si et seulement si u n'est pas bijectif, et c'est aussi équivalent à u non surjectif.*

Démonstration : Via le lemme 2.21, on sait que $(B/\wp)_\mathfrak{q}$ est de dimension finie sur $k(\wp)$, d'où le fait que u est bijective si et seulement si elle est surjective (ou injective). Comme $\mathcal{D}_{B/A}$ est l'annulateur du A-module $B^\vee/B$, on a $\mathcal{D}_{B/A} \subset \mathfrak{q}$ si et seulement si $(B^\vee/B)_\mathfrak{q} \neq 0$. Via le lemme de Nakayama appliqué au $A_\wp$-module de type fini $(B^\vee/B)_\mathfrak{q}$, ceci est équivalent à $(B^\vee/\wp B^\vee)_\mathfrak{q} \neq 0$. La suite exacte

$$0 \to B \to B^\vee \to B^\vee/B \to 0$$

induit une suite exacte

$$(B/\wp)_\mathfrak{q} \xrightarrow{h_\mathfrak{q}} (B^\vee/\wp)_\mathfrak{q} \to (B^\vee/\wp B^\vee)_\mathfrak{q} \to 0,$$

par exactitude du foncteur de localisation et exactitude à droite du produit tensoriel $\otimes_B(B/\wp)$. Ainsi, la condition $\mathcal{D}_{B/A} \subset \mathfrak{q}$ équivaut à ce que le conoyau de $h_\mathfrak{q}$ soit non nul.

Comme $b_{L/K}$ est non dégénérée, on a par définition de $B^\vee$ un isomorphisme de B-modules $f : B^\vee \to \mathrm{Hom}_A(B, A)$ donné par $f(x) = \mathrm{Tr}_{L/K}(x, -)$. Comme B est un A-module projectif (remarque 2.8) de type fini, ceci induit un isomorphisme

$$\bar{f} : B^\vee/\wp \to \mathrm{Hom}_{k(\wp)}(B/\wp, k(\wp)).$$

En composant l'inclusion $h : B/\wp \to B^\vee/\wp$ avec $\bar{f}$, on obtient la flèche $g : x \mapsto \mathrm{Tr}_{(B/\wp)/k(\wp)}(x, -)$. Le conoyau de $h_\mathfrak{q}$ est donc isomorphe à celui de la flèche $g_\mathfrak{q}$ obtenue en localisant g en $\mathfrak{q}$, qui n'est autre que u (noter que $(B/\wp)_\mathfrak{q}$ est un facteur direct de la $k(\wp)$-algèbre de dimension finie $B/\wp$ via le lemme 2.21, donc la localisation en $\mathfrak{q}$ est juste la projection sur l'un des facteurs).

□

Theorème 3.11 *Soit $\mathfrak{q}$ un idéal premier non nul de B. Alors $\mathfrak{q}$ est ramifié dans l'extension L/K si et seulement si $\mathfrak{q}$ divise la différente $\mathcal{D}_{B/A}$.*

Démonstration : D'après le lemme 3.10, $\mathfrak{q}$ divise $\mathcal{D}_{B/A}$ si et seulement si u n'est pas bijectif, autrement dit (cf. proposition 2.3) ssi la trace est dégénérée sur la $k(\wp)$-algèbre $(B/\wp)_\mathfrak{q} \simeq B/\mathfrak{q}^{v_\mathfrak{q}(\wp B)}$. D'après la proposition 2.3, ceci se produit précisément quand l'une des deux conditions suivantes est réalisée : l'extension $k(\mathfrak{q}) = B/\mathfrak{q}$ n'est pas séparable sur $k(\wp)$, ou $v_\mathfrak{q}(\wp B) > 1$, c'est-à-dire finalement quand $\mathfrak{q}$ est ramifié dans l'extension L/K.

□

Remarque 3.12 Une autre preuve de ce résultat, reposant sur une approche locale basée sur les complétions, est donnée dans l'exercice 5.5.

Corollaire 3.13 *Si $\wp$ est un idéal premier non nul de A, alors L/K est ramifiée en $\wp$ si et seulement si $\wp$ divise le discriminant $\Delta_{B/A}$. En particulier, le nombre d'idéaux premiers de A ramifiés dans L/K est fini.*

Exercice 3.14 Soit A un anneau de Dedekind de corps des fractions K. Soient $K \subset L \subset M$ des extensions finies séparables, on note B et C les fermetures intégrales respectives de A dans L et M. Montrer les formules

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

pour tout idéal non nul I de C.

$$\mathcal{D}_{C/A} = \mathcal{D}_{C/B}\mathcal{D}_{B/A}.$$
$$\Delta_{C/A} = N_{B/A}(\Delta_{C/B}).\Delta_{B/A}^{[M:L]}.$$

3.2. Substitution de Frobenius

Soit A un anneau de Dedekind de corps des fractions K. Soient L une extension finie galoisienne de K et B la fermeture intégrale de A dans L. Soient $\mathfrak{q}$ un idéal premier non nul de B et $\wp = \mathfrak{q} \cap A$. On fait l'hypothèse supplémentaire que le corps résiduel $k(\wp)$ est fini (en particulier il est parfait), c'est alors aussi le cas de $k(\mathfrak{q})$, qui est une extension finie galoisisienne de $k(\wp)$. On sait que $\mathrm{Gal}\,(k(\mathfrak{q})/k(\wp))$ est cyclique, engendré par $F : x \mapsto x^q$, où q est le cardinal de $k(\wp)$.

Définition 3.15 Supposons $\mathfrak{q}$ (ou $\wp$, cela revient au même) non ramifié dans l'extension L/K. On appelle *élément de Frobenius* en $\mathfrak{q}$ l'unique élément du groupe de décomposition $D_\mathfrak{q}$ dont l'image dans $\mathrm{Gal}\,(k(\mathfrak{q})/k(\wp))$ est F. On le note $(\mathfrak{q}, L/K)$.

Rappelons que comme $\mathfrak{q}$ est non ramifié, la flèche naturelle

$$D_\mathfrak{q} \mapsto \mathrm{Gal}\,(k(\mathfrak{q})/k(\wp))$$

est un isomorphisme, ce qui justifie la définition ci-dessus. On peut caractériser $(\mathfrak{q}, L/K)$ comme l'unique σ de $\mathrm{Gal}\,(L/K)$ tel que $\sigma(\mathfrak{q}) = \mathfrak{q}$ et $\sigma(b) = b^q$ modulo $\mathfrak{q}$ pour tout $b \in B$. L'ordre de $(\mathfrak{q}, L/K)$ est le degré résiduel $f_\wp$.

Remarque 3.16 a) La construction de $(\mathfrak{q}, L/K)$ commute à la localisation : si S est une partie multiplicative de A disjointe de $\wp$, alors $(\mathfrak{q}_S, L/K) = (\mathfrak{q}, L/K)$.

b) Si on remplace $\mathfrak{q}$ par un autre idéal premier au-dessus de $\wp$, celui-ci est de la forme $\sigma(\mathfrak{q})$ (proposition 2.23 et $(\sigma(\mathfrak{q}), L/K) = \sigma(\mathfrak{q}, L/K)\sigma^{-1}$. Ainsi, si l'extension L/K est abélienne, l'élément de Frobenius ne dépend que de $\wp$ et peut être noté $(\wp, L/K)$.

On a des compatibilités diverses de l'élément de Frobenius :

Proposition 3.17 *Soit A un anneau de Dedekind de corps des fractions K. Soient M une extension finie galoisienne de K et $L \subset M$ une sous-extension. Soient B et C les fermetures intégrales respectives de A dans L et M. Soit $\mathfrak{q}$ un idéal premier non nul de C, on pose $\wp = \mathfrak{q} \cap A$ et $\tau = \mathfrak{q} \cap B$. On note $D_\mathfrak{q} \subset \mathrm{Gal}\,(M/K)$ et $D'_\mathfrak{q} \subset \mathrm{Gal}\,(M/L)$ ses groupes de décomposition, respectivement par rapport aux extensions M/K et M/L. On suppose $k(\wp)$ fini de cardinal q et $\mathfrak{q}$ non ramifié dans M/K. Alors :*

a) L'idéal $\mathfrak{q}$ est non ramifié dans M/L. De plus $D'_\mathfrak{q} = D_\mathfrak{q} \cap \mathrm{Gal}\,(M/L)$ et $(\mathfrak{q}, M/L) = (\mathfrak{q}, M/K)^{f_\wp}$, où $\wp = \mathfrak{q} \cap A$ et $f_\wp = f_{\tau/\wp}$ est le degré résiduel en $\wp$ pour l'extension L/K.

b) Supposons de plus L/K galoisienne. Alors l'image de $(\mathfrak{q}, M/K)$ dans $\mathrm{Gal}\,(L/K)$ est $(\tau, L/K)$.

Démonstration : a) Comme $1 = e_{\mathfrak{q}/\wp} = e_{\mathfrak{q}/\tau} e_{\tau/\wp}$, on a aussi $\mathfrak{q}$ non ramifié dans M/L. Par définition du sous-groupe de décomposition, on a $D'_{\mathfrak{q}} = D_{\mathfrak{q}} \cap \mathrm{Gal}\,(M/L)$. Soit H le noyau de la restriction $D_{\mathfrak{q}} \simeq \mathrm{Gal}\,(k(\mathfrak{q})/k(\wp)) \to \mathrm{Gal}\,(k(\tau)/k(\wp))$. On a clairement $D'_{\mathfrak{q}} \subset H$ et ils ont même cardinal $f_{\mathfrak{q}/\tau}$, d'où $H = D'_{\mathfrak{q}}$. En particulier $(\mathfrak{q}, M/K)^{f_\wp}$ est dans $D'_{\mathfrak{q}}$, et modulo $\mathfrak{q}$ il coïncide avec $x \mapsto x^{q^{f_\wp}}$, où $q^{f_\wp}$ est le cardinal de $k(\tau)$, d'où le résultat.

b) Posons $\sigma = (\mathfrak{q}, M/K)$. Alors $\sigma(\mathfrak{q}) = \mathfrak{q}$, donc l'image $\bar{\sigma}$ de σ dans $\mathrm{Gal}\,(L/K)$ fixe $\tau = \mathfrak{q} \cap B$. Par ailleurs si $x \in B$, alors $x \in C$ donc $\sigma(x) = x^q$ modulo $\mathfrak{q}$, mais alors $(\sigma(x) - x^q) \in (\mathfrak{q} \cap B) = \tau$, donc $\sigma(x) = x^q$ modulo τ, ce qui montre finalement que $\bar{\sigma}$ est l'élément de Frobenius $(\tau, L/K)$.

□

3.3. Extensions cyclotomiques

Soit $n \geq 2$ un entier, fixons une racine primitive n-ième de l'unité ζ et posons $K = \mathbf{Q}(\zeta)$. On rappelle que le polynôme minimal de ζ sur $\mathbf{Q}$ est le polynôme cyclotomique Φ_n, et que l'anneau des entiers de $\mathcal{O}_K$ est $\mathbf{Z}[\zeta]$ (voir TD). Ainsi le discriminant absolu de K est le discriminant de Φ_n. Rappelons aussi que l'extension K/Q est galoisienne de groupe de Galois G isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$, via l'application c qui envoie tout $\sigma \in G$ sur l'élément $c(\sigma)$ défini par $\sigma(\zeta) = \zeta^{c(\sigma)}$.

Proposition 3.18 *Soit p un nombre premier ne divisant pas n. Alors p est non ramifié dans l'extension $K/\mathbf{Q}$.*

Démonstration : Comme Φ_n divise $X^n - 1$ et $X^n - 1$ est séparable dans $\mathbf{F}_p[X]$ (car p ne divise pas n), la réduction $\overline{\Phi}_n$ de Φ_n modulo p est séparable, ce qui fait que son discriminant est un élement non nul de $\mathbf{F}_p$. Cela signifie que p ne divise pas le discriminant $\Delta_{\mathcal{O}_K/\mathbf{Z}}$, et donc est non ramifié dans l'extension $K/\mathbf{Q}$ d'après le corollaire 3.13.

□

Remarque 3.19 En fait, si p divise n, l'extension $\mathbf{Q}(\zeta)/\mathbf{Q}$ est effectivement ramifiée en p (voir TD).

Proposition 3.20 *Soit p un nombre premier ne divisant pas n. Alors l'élément de Frobenius de p (bien défini car G est abélien et p est non ramifié dans $K/\mathbf{Q}$) vérifie :*

$$c((p, K/\mathbf{Q})) = \bar{p} \in (\mathbf{Z}/n\mathbf{Z})^*.$$

Démonstration : Posons $c = c((p, K/\mathbf{Q}))$. Par définition de l'élément de Frobenius, on a $\bar{\zeta}_n^c = \bar{\zeta}_n^p$ dans $k(\mathfrak{q})$, où $\mathfrak{q}$ est un idéal premier au-dessus de $\wp$. Cette égalité est vraie de même pour tous les ζ^i avec $0 \leq i \leq n-1$, qui sont les racines distinctes du polynôme $(X^n - 1) \in \mathbf{F}_p[X]$, ce qui montre que c est congru à p modulo n.

□

Exercice 3.21 Avec les hypothèses et notations ci-dessus, montrer que le degré résiduel f_p en p est l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$. En particulier, p est congru à 1 modulo n si et seulement si l'extension $\mathbf{Q}(\zeta)/\mathbf{Q}$ est complètement décomposée en p.

4. Corps complets pour une valuation discrète

Dans ce chapitre on va voir que les résultats sur les anneaux de valuatuon discrètes peuvent être considérablement précisés quand on travaille avec des corps complets. Cela va nous amener à introduire les complétions du corps des fractions d'un anneau de Dedekind pour ses diverses valuations discrètes, ce qui s'avèrera particulièrement utile pour étudier les corps de nombres.

4.1. Valuations ultramétriques

Définition 4.1 Une *valeur absolue* d'un corps K est une application $|.| : K \to \mathbf{R}_+$ vérifiant :

i) $|x| = 0$ si et seulement si $x = 0$.
ii) $|xy| = |x||y|$ pour tous x, y de K.
iii) $|x + y| \leq |x| + |y|$ pour tous x, y de K.

Un *corps valué*[1] est un corps muni d'une valeur absolue. La valeur absolue $|.|$ est dite *ultramétrique* si on a la propriété plus forte $|x + y| \leq \max(|x|, |y|)$ pour tous x, y de K.

Remarque 4.2 Noter que si la valeur absolue est ultramétrique, on a $|x + y| = \max(|x|, |y|)$ dès que $|x| \neq |y|$ via l'égalité $x = (x + y) - y$ qu'on peut appliquer si par exemple $|x| \geq |y|$.

Exemple 4.3 a) La *valeur absolue triviale* est définie par $|x| = 1$ pour tout $x \neq 0$.

1. Attention, en anglais "valued field" réfère à un corps muni d'une valeur absolue ultramétrique, ou encore d'une valuation.

b) Sur $\mathbf{R}$ ou sur $\mathbf{Q}$, la valeur absolue usuelle (ou réelle) n'est pas ultramétrique. De même, on a sur $\mathbf{C}$ la valeur absolue définie par $z \mapsto |z|$, qui n'est pas ultramétrique.

c) Si p est un nombre premier, on peut définit une valeur absolue ultramétrique sur $\mathbf{Q}$ par $|x|_p := p^{-v_p(x)}$, où $v_p(x)$ est la valuation p-adique de x (en convenant que $|0| = 0$). Ceci s'étend à tout $K = \operatorname{Frac} A$, où A est un anneau de Dedekind, en posant $|x| = a^{-v_\wp(x)}$ pour tout idéal premier non nul $\wp$ de A, où a est un réel quelconque vérifiant $a > 1$.

On vérifie immédiatement que muni de la distance $(x, y) \mapsto |x-y|$ associée à une valeur absolue, un corps valué est un corps topologique.

Définition 4.4 On dit que deux valeurs absolues $|.|_1$ et $|.|_2$ sur un corps K sont *équivalentes* s'il existe un réel $\alpha > 0$ tel que $|x|_2 = |x|_1^\alpha$ pour tout x de K. Une *place* est une classe d'équivalence de valeurs absolues non triviales sur K.

Remarque 4.5 Si $|.|$ est une valeur absolue ultramétrique, alors toute puissance $|.|^\alpha$ avec $\alpha > 0$ en est encore une ; mais sans l'hypothèse ultramétrique, l'application $|.|^\alpha$ n'est en général pas une valeur absolue au sens strict si $\alpha > 1$ (elle ne vérifie pas forcément l'inégalité triangulaire).

Exercice 4.6 Vérifier que deux valeurs absolues sont équivalentes si et seulement si elles définissent la même topologie (on commencera par observer que pour toute valeur absolue $|.|$, les sous-ensembles de K définis par $|x| < 1$ et $|x| > 1$ ne dépendent que de la topologie associée à cette valeur absolue).

Exercice 4.7 a) Montrer qu'une valeur absolue non triviale $|.|$ sur un corps K est ultramétrique si et seulement si $|n| \leq 1$ pour tout $n \in \mathbf{Z}$. On pourra montrer d'abord que si cette hypothèse est vérifiée et si x et y sont deux éléments de K de valeur absolue au plus 1, alors $|x + y| \leq 1$ (développer $(x + y)^n$ et faire tendre n vers $+\infty$).

b) Vérifier que si K est de caractéristique non nulle, toute valeur absolue est ultramétrique.

On suppose maintenant que $|.|$ est une valeur absolue non ultramétrique sur un corps K, et donc qu'il existe un entier $a \geq 2$ tel que $|a| > 1$.

c) Montrer que la valeur absolue est archimédienne, à savoir : pour tout x non nul dans K et tout $M > 0$, il existe $n \in \mathbf{N}^*$ tel que $|nx| \geq M$.

d) Montrer que pour tout entier $b \geq 2$, on a $|b| > 1$ (raisonner par l'absurde en écrivant le développement de a^m en base b pour tout entier $m > 0$, afin d'obtenir une majoration du type $|a|^m \leq \frac{Cm \ln a}{\ln b}$, avec C constante indépendante de m, puis aboutir à une contradiction en faisant tendre m vers $+\infty$).

(Les résultats de cet exercice seront raffinés au paragraphe 4.6.).

Proposition 4.8 *Soit K un corps valué ultramétrique.*

a) L'ensemble $\mathcal{O} = \{x \in K, |x| \leq 1$ est un sous-anneau de K, qui est local d'idéal maximal $\mathcal{M} := \{x \in K, |x| < 1\}$. On l'appelle anneau de valuation associé à $|.|$, ou encore anneau des entiers de K.

b) L'idéal $\mathcal{M}$ est principal si et seulement si la valeur absolue est discrète, i.e. si l'image de K^* par $|.|$ est un sous-groupe discret de $\mathbf{R}_+^*$.

c) La valeur absolue est discrète et non triviale si et seulement si $\mathcal{O}$ est un anneau de valuation discrète ; la valeur absolue est alors de la forme $|x| = a^{v(x)}$, où $v : K^* \to \mathbf{Z}$ est la valuation et $a \in]0, 1[$.

Démonstration : a) Les propriétés d'une valeur absolue ultramétrique impliquent immédiatement que $\mathcal{O}$ est un sous anneau de A dont les inversibles sont les éléments x vérifiant $|x| = 1$, et dont $\mathcal{M}$ est un idéal. Ainsi l'ensemble des non-inversibles de $\mathcal{O}$ est un idéal et $\mathcal{O}$ est bien un anneau local.

b) Soit Γ l'ensemble des $|x|$ pour x dans K^*, c'est un sous-groupe de $\mathbf{R}_+^*$, qu'on peut supposer non trivial (sinon $\mathcal{O} = K$ est un corps et $\mathcal{M}$ est l'idéal nul, donc principal). Si $\mathcal{M}$ est principal engendré par π, alors l'intersection de Γ avec l'intervalle ouvert $]|\pi|, |\pi|^{-1}[$ se réduit à $\{1\}$ (en effet, tout élément x de K^* vérifie $x \in \mathcal{O}$ ou $x^{-1} \in \mathcal{O}$, donc s'écrit $x = u\pi^m$ avec $|u| = 1$ et $m \in \mathbf{Z}$), ce qui montre que le groupe Γ est discret. Si réciproquement Γ est discret (et non réduit à $\{1\}$), alors $\Gamma = a^{\mathbf{Z}}$, où a est un réel dont on peut supposer qu'il vérifie $0 < a < 1$. Posons alors $v(x) = \frac{\ln |x|}{\ln a}$ pour tout x de K^*, on vérifie immédiatement que v vérifie les conditions de la proposition 1.5, ce qui prouve b). c) en découle également.

□

Remarque 4.9 Dans le cas où K est un corps valué ultramétrique dont la valeur absolue n'est pas discrète, cette valeur absolue s'écrit encore sous la forme $|x| = a^{v(x)}$ avec $a \in]0, 1[$, mais v n'est plus à valeurs dans $\mathbf{Z}$, c'est une valuation dont l'image est un sous-groupe dense de $\mathbf{R}_+^*$.

4.2. Corps valués complets

Définition 4.10 Soit K un corps valué. On dit que K est *complet* si c'est un espace métrique complet pour la distance $d(x, y) := |x - y|$ associée à la valeur absolue. Pour tout corps valué K, on note $\widehat{K}$ son complété pour cette distance.

Comme toute application qui est uniformément continue, la valeur absolue s'étend de manière unique à $\widehat{K}$, qui est alors ipso facto un corps valué complet lorsqu'il est muni de ce prolongement (on vérifie facilement que les propriétés de la valeur absolue passent bien à la limite). Quand la valeur absolue provient d'une valuation (i.e. est ultramétrique), on pourra parler de complété pour ladite valuation.

Exemple 4.11 a) Le complété de $\mathbf{Q}$ pour la valeur absolue usuelle est $\mathbf{R}$.

b) Le complété de $\mathbf{Q}(i) = \mathbf{Q}(\sqrt{-1})$ pour $z \mapsto |z|$ est $\mathbf{C}$.

c) Soit p un nombre premier. Le complété de $\mathbf{Q}$ pour la valeur absolue $|x|_p := p^{-v_p(x)}$ (où v_p est la valeur absolue p-adique) s'appelle le *corps des nombres p-adiques*, qu'on note $\mathbf{Q}_p$. Comme la valeur absolue est ultramétrique (et discrète), on dispose de son anneau des entiers $\mathbf{Z}_p$ (qu'on peut aussi définir comme la limite projective des $\mathbf{Z}/p^n\mathbf{Z}$, voir proposition 4.13 plus bas).

d) Soient k un corps et $K = k(t)$. Considérons la valuation t-adique, définie par $v(P/Q) = v(P) - v(Q)$ où P et Q sont des polynômes non nuls et la valuation d'un polynôme est définie comme le plus petit degré des monômes apparaissant dans son écriture. C'est une valuation discrète, et le complété de K pour cette valuation est le corps des séries de Laurent $k((t))$. L'anneau des entiers de ce complété est l'anneau des séries formelles $k[[t]]$.

Pour tout corps valué ultramétrique K, notons $\mathcal{O}_K$ son anneau des entiers et $\mathcal{M}_K$ l'idéal maximal de $\mathcal{O}_K$.

Proposition 4.12 *Soit K un corps valué ultramétrique. Alors :*

a) On a $|K^*| = |\widehat{K}^*|$

b) L'anneau $\mathcal{O}_{\widehat{K}}$ est l'adhérence de $\mathcal{O}_K$ dans $\widehat{K}$.

c) L'application naturelle (induite par l'inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_{\widehat{K}}$)

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

entre corps résiduels est un isomorphisme.

Démonstration : a) Soit $r = |a|$ avec $a \in \widehat{K}^*$. Comme K est par définition dense dans $\widehat{K}^*$, on peut trouver b dans K avec $|a - b| < |a|$, ce qui implique $|b| = |a| = r$ puisque la valeur absolue est ultramétrique, soit finalement $r \in |K^*|$.

b) Soit x non nul dans $\mathcal{O}_{\widehat{K}}$, il est limite d'une suite (x_n) d'éléments de K. Pour n assez grand, on a $|x_n - x| < |x|$, ce qui implique $|x_n| = |x|$ et en particulier $x_n \in \mathcal{O}_K$, donc x est bien limite d'une suite d'éléments de $\mathcal{O}_K$.

c) L'idéal maximal $\mathcal{M}_{\widehat{K}}$ est un ouvert de $\mathcal{O}_{\widehat{K}}$ (c'est le sous-ensemble des éléments de valeur absolue différente de 1), ce qui avec b) implique que $\mathcal{O}_{\widehat{K}} = \mathcal{O}_K + \mathcal{M}_{\widehat{K}}$, ce qui donne le résultat en remarquant de plus qu'on a $\mathcal{M}_{\widehat{K}} \cap \mathcal{O}_K = \mathcal{M}_K$.

□

Proposition 4.13 *On garde les hypothèses de la proposition 4.12 et on suppose de plus que la valeur absolue est discrète. Soit π une uniformisante de l'a.v.d. $\mathcal{O}_K$. Alors :*

a) Le complété $\widehat{\mathcal{O}}_K$ s'identifie à $\varprojlim(\mathcal{O}_K/\pi^n\mathcal{O}_K)$.

b) Le corps K est localement compact si et seulement s'il est complet et son corps résiduel $\kappa := \mathcal{O}_K/\pi\mathcal{O}_K$ est fini. Dans ce cas $\mathcal{O}_K$ est compact.

Démonstration : a) Les idéaux $\pi^n\mathcal{O}_K$ forment une base de voisinages de 0 dans K (ou dans $\mathcal{O}_K$, qui est un ouvert de K car il consiste en les éléments de valuation > -1). Du coup, la topologie sur $\mathcal{O}_K$ est sa topologie d'anneau local noethérien, d'où le résultat (cf. [3], chapitre 9, paragraphe (23.H)).

b) Supposons K localement compact. Il est connu ([2], §3, corollaire 1 à la proposition 4) qu'alors, comme c'est un groupe topologique métrisable, il est complet. Comme de plus $\{0\}$ admet un voisinage compact V, l'un des $\pi^n\mathcal{O}_K$ est compact (en tant que fermé de V), donc par homothétie $\mathcal{O}_K$ est compact et le quotient $\mathcal{O}_K/\pi\mathcal{O}_K$ est alors compact et discret (vu que $\pi\mathcal{O}_K$ est un ouvert de $\mathcal{O}_K$), donc fini. Réciproquement, si K est complet avec κ fini, alors $\mathcal{O}_K$ est compact comme limite projective des groupes finis $\mathcal{O}_K/\pi^n\mathcal{O}_K$, et K est localement compact vu que 0 admet les $\pi^n\mathcal{O}_K$ comme base de voisinages compacts.

□

Noter que dans le cas b), le groupe $\mathcal{O}_K$ est *profini* (limite projective de groupes finis), ce qui est équivalent à dire qu'il est compact et totalement discontinu.

Exercice 4.14 Soit K un corps complet pour une valuation discrète de corps résiduel k. Soient π une uniformisante de K et Σ un système de représentants de k dans $\mathcal{O}_K$. Montrer que tout élément a de $\mathcal{O}_K$ s'écrit de façon unique :

$$a = \sum_{n=0}^{+\infty} a_n \pi^n$$

avec $a_n \in \Sigma$. Tout élément b de K s'écrit de même

$$b = \sum_{n=-N}^{+\infty} a_n \pi^n$$

avec $N \in \mathbf{N}$ et $b_n \in \Sigma$. Appliquer ces résultats à $K = \mathbf{Q}_p$, muni de l'uniformisante p, et en déduire que $\mathbf{Z}_p$ et $\mathbf{Q}_p$ ne sont pas dénombrables.

Exercice 4.15 Soit K un corps valué ultramétrique de clôture algébrique $\overline{K}$. Soient α, β deux éléments de $\overline{K}$ tels que α soit séparable sur K. On considère les conjugués $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ de α sur K et on suppose que

$$|\alpha - \beta| < |\alpha - \alpha_i|, 2 \leq i \leq n.$$

a) Soit $L = K(\beta)(\alpha_1, ..., \alpha_n)$. Montrer que $L/K(\beta)$ est galoisienne et que pour tout $\sigma \in G := \mathrm{Gal}\,(L/K(\beta))$, on a

$$|\beta - \sigma(\alpha)| < |\alpha - \alpha_i|, 2 \leq i \leq n.$$

b) En déduire que

$$|\alpha - \sigma(\alpha)| < |\alpha - \alpha_i|$$

pour $2 \leq i \leq n$.

c) Conclure que $\alpha \in K(\beta)$ (lemme de Krasner).

Dans toute la suite de l'exercice, on considère un polyôme $P \in K[X]$, irréductible et séparable de degré d. On fixe une norme $||$ sur le K-espace vectoriel $K_d[X]$ des polynômes de degré inférieur à d. On se propose de montrer qu'il existe $\delta > 0$ tel que pour tout polynôme Q de $K_d[X]$ vérifiant $||Q - P|| \leq \delta$, alors Q est irréductible, séparable, de corps de rupture $K[X]/(Q)$ isomorphe à celui de P.

d) Montrer qu'on peut supposer P unitaire, on écrit alors

$$P = \prod_{i=1}^{d} (X - \alpha_i),$$

avec les α_i deux à deux distincts dans $\overline{K}$.

e) Soit $\varepsilon > 0$. Montrer qu'il existe $\delta > 0$ tel que pour Q dans $K_d[X]$ de coefficient dominant b_d et vérifiant $||Q - P|| \leq \delta$, on a $Q(\alpha_1) < \varepsilon^d/2$ et $|b_d - 1| < 1/2$.

f) On écrit $Q = \prod_{i=1}^{d} (X - \beta_i)$, avec les β_i dans $\overline{K}$. Montrer qu'il existe $i \in \{1, ..., d\}$ tel que $|\beta_i - \alpha_1| < \varepsilon$.

g) Conclure en choisissant bien ε et en appliquant le lemme de Krasner.

Définition 4.16 Un *corps local* est un corps complet pour une valuation discrète, dont le corps résiduel est fini [2]

2. Certains auteurs étendent cette définition à tout corps valué localement compact dont la valeur absolue est non triviale, ce qui rajoute juste $\mathbf{R}$ et $\mathbf{C}$, voir la remarque 4.35.

Définition 4.17 Soit K un corps local dont on note $v : K^* \to \mathbf{Z}$ la valuation. La *valeur absolue normalisée* sur K est la valeur absolue définie par $|x| := q^{-v(x)}$, où q est le cardinal du corps résiduel de K.

Exercice 4.18 Soit K un corps local dont le corps résiduel κ est de cardinal q. Soit μ une mesure de Haar sur le groupe localement compact $(K, +)$ (c'est-à-dire une mesure invariante par translation). On note π une uniformisante de K.

a) Montrer que $\mu(a+\pi^n\mathcal{O}_K) = q^{-n}\mu(\mathcal{O}_K)$ pour tout $a \in K$ et tout $n \in \mathbf{Z}$.

b) Montrer que pour toute partie mesurable A de K et tout $a \in A$, on a $\mu(aA) = |a|\mu(A)$, où $|a|$ désigne la valeur absolue normalisée de a.

c) Montrer que si $K = \mathbf{R}$ ou $K = \mathbf{C}$, on a la même formule qu'en b), en remplaçant $|a|$ par la valeur absolue usuelle si $K = \mathbf{R}$, mais par le *carré* du module usuel si $K = \mathbf{C}$.

Remarque 4.19 La notion de valeur absolue normalisée s'étend à $\mathbf{R}$ et à $\mathbf{C}$, à condition dans le cas de $\mathbf{C}$ de remplacer le module par son carré, qui n'est plus une valeur absolue au sens strict. Cette convention est néanmoins nécessaire pour avoir la formule du produit sur un corps de nombres, comme on le verra un peu plus loin, cf. aussi le c) de l'exercice 4.18. Le point est qu'on aura besoin, pour une extension finie L/K, d'avoir que la valeur absolue normalisée de $a \in L$ est aussi la valeur absolue normalisée de $N_{L/K}(a)$ dans K.

4.3. Extensions d'un corps complet

On va voir dans ce paragraphe que les résultats du paragraphe 2.2. deviennent nettement plus précis quand on travaille avec un corps de base complet pour une valuation discrète. Si L est une extension d'un corps K, on dira qu'une valuation w de L est *au-dessus*[3] d'une valuation v de K si la valuation induite par w sur K est équivalente à v.

Theorème 4.20 *Soit K un corps complet pour une valuation discrète v dont on note A l'anneau des entiers. Soit L une extension finie de degré n de K. Soit B la fermeture intégrale de A dans L. Alors B est un anneau de valuation discrète, c'est un A-module libre de rang n et L est complet pour la topologie définie par B.*

3. Certains auteurs disent plutôt que w prolonge v, mais cela risque d'entraîner une confusion avec la propriété plus forte que la restriction de la valuation w à K est exactement v, ce qui dans le théorème ci-dessous implique en plus que l'indice de ramification soit 1.

Démonstration : Supposons d'abord que l'extension L/K est séparable (ce qui est automatique si K est parfait, par exemple de caractéristique zéro). On peut alors appliquer les théorèmes 2.20 et 2.6, qui nous disent que B est un anneau de Dedekind, et aussi un A-module de type fini ; comme ici A est principal, B est même libre de rang n (il est sans torsion de corps des fractions L). Considérons les idéaux premiers $\wp_1, ..., \wp_r$ de B (qui sont au-dessus de l'unique idéal premier de A). Ils induisent des valuations $w_1, ..., w_r$ et des normes sur L (pour la structure de K-espace vectoriel de L). Comme L est de dimension finie sur K et K est complet, toutes les normes sont équivalentes, ce qui implique que les w_i induisent la même topologie, et donc sont égales car l'anneau de valuation associé à w_i est l'ensemble des x de K tels que x^{-n} ne tend pas vers zéro pour la topologie associée à w_i. Ainsi, B n'a qu'un seul idéal premier et c'est donc un a.v.d. On sait par ailleurs que L (qui est isomorphe à K^n comme espace vectoriel normé muni de la norme sup, ou encore de la topologie produit) est complet vu que K est complet.

Passons au cas général. Il suffit maintenant par dévissage de traiter le cas où l'extension L/K est radicielle, c'est-à-dire du type $L = K(\sqrt[q]{a})$, où q est une puissance de la caractéristique p et $a \in K$, en particulier tout x de L vérifie $x^q \in K$. Posons alors $v'(x) = v(x^q)$ pour $x \in L$, l'image de v' est de la forme $m\mathbf{Z}$ avec $m \in \mathbf{N}^*$, d'où une valuation $w = \frac{1}{m}v$ sur L, dont l'anneau de valuation est B : en effet un élément x de L est entier sur K si est seulement si son polynôme minimal, qui est de la forme $X^{p^r} - a$, est dans $\mathcal{O}_K$, ce qui correspond à $v(a) \geq 0$ ou encore à $w(x) \geq 0$. La topologie définie par w coïncide avec celle de K-espace vectoriel normé de dimension finie de L, et elle fait donc de L un corps complet. Le même argument que précédemment donne alors qu'il n'y a qu'une seule valuation de L au-dessus de v, et il reste juste à montrer que B est un A-module de type fini pour conclure.

Soit π une uniformisante de A, posons $\widetilde{B} = B/\pi B$, c'est un κ-espace vectoriel de dimension finie, où $\kappa = A/\pi A$. Soient $b_1, ..., b_r$ des éléments de B dont les images dans $\widetilde{B}$ en forment une base. Alors la famille $(b_1, ..., b_r)$ est libre, car si on avait une relation $\sum a_i b_i = 0$, on pourrait supposer que l'un des a_i n'est pas divisible par π, d'où une contradiction en réduisant modulo π. Ainsi $r \leq n$. Maintenant, soit E le sous A-module de B engendré par les b_i. Tout x de B s'écrit alors $x = x_0 + \pi x_1$ avec $x_0 \in E$ et $x_1 \in B$. En appliquant ceci à x_1 et en itérant, on voit que x est la limite dans B d'une suite d'éléments de E, donc $x \in E$ vu que E est isomorphe à B^r, qui est complet. Finalement B est le A-module libre engendré par $b_1, ..., b_r$, et on a forcément $r = n$ puisque $\operatorname{Frac} B = L$.

□

En particulier, l'hypothèse que K est complet pour v implique qu'il n'y

a qu'un idéal premier de B au-dessus de l'idéal premier de A. On peut donc parler sans ambiguité de l'indice de ramification e et du degré résiduel f de l'extension L/K. Noter que B (défini a priori comme fermeture intégrale) est aussi l'anneau des entiers de L au sens de la proposition 4.8, ce qui justifie a posteriori la terminologie employée.

Corollaire 4.21 *Il n'y a qu'une valuation w de L au-dessus de v, et elle vérifie $w(\pi) = e$, où π est une uniformisante de A. Plus généralement, si $x \in K^*$, on a $w(x) = ev(x)$.*

Démonstration : La première assertion est juste une reformulation du théorème 4.20. Si maintenant $x \in K^*$, on l'écrit $x = u\pi^m$ avec $m \in \mathbf{Z}$ et u inversible dans A (donc aussi dans B), d'où $w(x) = w(\pi^m) = em = ev(x)$.

□

Corollaire 4.22 *On a $ef = n$.*

Démonstration : C'est le théorème 2.20 appliqué à notre situation, vu qu'il n'y a qu'un idéal premier au-dessus de l'idéal premier de A.

□

Corollaire 4.23 *a) Si x et y sont deux éléments de L conjugués sur K, alors $w(x) = w(y)$.*

b) Pour tout x de L, on a

$$w(x) = \frac{1}{f} v(N_{L/K}(x)),$$

où f est le degré résiduel.

c) La topologie de L peut être définie par la valeur absolue

$$|x|_L := |N_{L/K}(x)|_K.$$

Dans le cas où le corps résiduel de A est fini, la valeur absolue $|.|_L$ est normalisée si $|.|_K$ l'est.

Démonstration : a) Quitte à augmenter l'extension L, on peut la supposer normale sur K. Soit alors σ un élément de $G := \mathtt{Aut}_K(L)$. Alors la valuation $\sigma(w)$ est au-dessus de v, donc elle coïncide avec w. Le résultat en découle puisque les conjugués de x ne sont autre que les $\sigma(w)$ pour $\sigma \in G$.

b) On peut là encore supposer que L/K est normale, et il suffit de traiter les deux cas L/K séparable et radicielle. Dans le cas séparable, on a

$$v(N_{L/K}(x)) = \frac{1}{e} w(\prod_{\sigma \in G} \sigma(x)) = \frac{1}{e} \sum_{\sigma \in G} w(\sigma(x)),$$

qui via le a) et le corollaire 4.22 vaut aussi

$$\frac{1}{e} n w(x) = f w(x).$$

Dans le cas radiciel, on a $N_{L/K}(x) = x^q$ (où q est une puissance de la caractéristique), d'où

$$v(N_{L/K}(x)) = \frac{1}{e} w(x^q) = f w(x)$$

comme on voulait.

c) D'après b), la topologie de L (qui est induite par la valuation w) peut être définie par $|.|_L$. Supposons de plus le corps résiduel κ de A fini de cardinal q et $|.|_K$ normalisée. Alors, si π est une uniformisante de A et π_L une uniformisante de B, on a $|\pi|_K = q^{-1}$ d'où $|\pi|_L = q^{-n}$, soit $|\pi_L|_L = q^{-n/e} = q^{-f}$ vu que π_L^e et π ont même valuation. Or q^f est bien le cardinal du corps résiduel de B.

□

4.4. Lemme de Hensel

Le résultat suivant permet souvent de montrer que des équations à coefficients dans l'anneau des entiers d'un corps valué ont des solutions dans ce corps.

Theorème 4.24 (Lemme de Hensel) *Soit K un corps complet ultramétrique d'anneau des entiers $\mathcal{O}_K$ et de corps résiduel k. Soit $f \in \mathcal{O}_K[X]$ dont on note $\bar{f} \in k[X]$ la réduction modulo l'idéal maximal $\mathcal{M}_K$ de $\mathcal{O}_K$. Alors, toute racine simple $\bar{x} \in k$ de $\bar{f}$ se relève en une unique racine $y \in \mathcal{O}_K$ de f.*

On va en fait montrer l'énoncé plus général suivant (parfois appelé lui-même lemme de Hensel) :

Proposition 4.25 *Sous les hypothèses et notations du théorème 4.24, on suppose qu'il existe $\alpha \in \mathcal{O}_K$ tel que*

$$\frac{|f(\alpha)|}{|f'(\alpha)|^2} < 1.$$

Alors il existe un unique $y \in \mathcal{O}_K$ tel que $f(y) = 0$ et $|y - \alpha| \leq \frac{|f(\alpha)|}{|f'(\alpha)|}|$.

Le théorème 4.24 se déduit aisément de la proposition 4.25. En effet, si α est un relevé dans $\mathcal{O}_K$ de $\bar{x}$, on a $|f(\alpha)| < 1$ et $|f'(\alpha)| = 1$, donc α vérifie les hypothèses de cette proposition. On a donc un $y \in \mathcal{O}_K$ tel que $f(y) = 0$ et

$$|y - \alpha| \leq |f(\alpha)| < 1,$$

ce qui montre que y relève $\bar{x}$. Par ailleurs, tout x de $\mathcal{O}_K$ relevant $\bar{x}$ et racine de f vérifie :

$$0 = f(x) = f(\alpha) + (x - \alpha)f'(\alpha) + (x - \alpha)^2 R$$

avec $R \in \mathcal{O}_K$, via la formule de Taylor. On en déduit $|x-\alpha| = |f(\alpha)| = \frac{|f(\alpha)|}{|f'(\alpha)|}$, d'où l'unicité via la proposition 4.25.

Preuve de la proposition 4.25 : Existence. On construit par récurrence une suite (α_n) d'éléments de $\mathcal{O}_K$ en posant

$$\alpha_0 = \alpha,\ \alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}.$$

Montrons un lemme :

Lemme 4.26 *Soit $\varepsilon_0 := |\alpha_1 - \alpha_0|$ et $\eta_0 = |f'(\alpha_0)|$. Alors $|f(\alpha_1)| \leq \varepsilon_0^2$ et $|f'(\alpha_1)| = \eta_0$. De plus*

$$\frac{|f(\alpha_1)|}{|f'(\alpha_1)|^2} < 1.$$

Démonstration : On a déjà $\alpha_1 \in \mathcal{O}_K$ vu que $|\frac{f(\alpha_0)}{f'(\alpha_0)}| \leq |f'(\alpha_0)| \leq 1$. Posons $h = -\frac{f(\alpha_0)}{f'(\alpha_0)}$, la formule de Taylor donne

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

avec $R \in \mathcal{O}_K$, ce qui implique

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

En appliquant de même la formule de Taylor à f', on trouve maintenant $(f'(\alpha_1) - f'(\alpha_0)) \in h\mathcal{O}_K$, d'où

$$|f'(\alpha_1) - f'(\alpha_0)| \leq |h| = \varepsilon_0 < \eta_0,$$

via l'hypothèse sur α_0, ce qui avec la remarque 4.2 donne $|f'(\alpha_1)| = |f'(\alpha_0)| = \eta_0$. Enfin

$$\frac{|f(\alpha_1)|}{|f'(\alpha_1)|} \leq \varepsilon_0^2/\eta_0 < \eta_0 = |f'(\alpha_1)|,$$

d'où la dernière assertion du lemme.

□

En posant $\varepsilon_n = |\alpha_{n+1} - \alpha_n|$, le lemme donne

$$|f(\alpha_{n+1})| \leq \varepsilon_n^2;\ |f'(\alpha_n)| = \eta_0;\ \varepsilon_n < \eta_0.$$

Du coup,

$$\varepsilon_{n+1} = |\frac{f(\alpha_{n+1})}{f'(\alpha_{n+1})}| \leq \varepsilon_n^2/\eta_0 < \varepsilon_n,$$

ce qui donne par récurrence

$$\varepsilon_n \leq \eta_0(\frac{\varepsilon_0}{\eta_0})^{2^n}.$$

Ceci montre que la suite (α_n) converge (car la série de terme général $(\alpha_{n+1} - \alpha_n)$ est absolument convergente, donc convergente puisque K est complet) vers un $y \in \mathcal{O}_K$, qui vérifie $f(y) = 0$ (en passant à la limite). De plus, la suite (ε_n) est strictement décroissante, ce qui implique

$$|\alpha_{n+1} - \alpha_0| = |\sum_{k=0}^{n}(\alpha_{k+1} - \alpha_k)| \leq \varepsilon_0,$$

d'où à la limite $|y - \alpha| \leq \varepsilon_0 = |\frac{f(\alpha)}{f'(\alpha)}|$ comme on voulait vu que $\alpha_0 = \alpha$.

Unicité. Soient y_1, y_2 vérifiant les conditions requises. En appliquant la formule de Taylor à f', on obtient

$$|f'(y_i) - f'(\alpha)| \leq |y - \alpha| \leq |\frac{f(\alpha)}{f'(\alpha)}| < |f'(\alpha)|,$$

ce qui montre (via la remarque 4.2) que $|f'(y_i)| = |f'(\alpha)|$ pour $i = 1, 2$. Si on avait $y_1 \neq y_2$, la formule de Taylor appliquée à f entre y_1 et y_2 donnerait

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

avec $R \in \mathcal{O}_K$, d'où $f'(y_1) \in (y_2 - y_1)\mathcal{O}_K$, ce qui impliquerait

$$|f'(\alpha)| = |f'(y_1)| \leq |y_2 - y_1| \leq |\frac{f(\alpha)}{f'(\alpha)}|,$$

vu que $(y_1 - \alpha)$ et $(y_2 - \alpha)$ sont tous deux de valeur absolue $\leq |\frac{f(\alpha)}{f'(\alpha)}|$. Ceci contredit l'hypothèse faite sur α.

□

Exemple 4.27 Soit K un corps local dont le corps résiduel κ est de cardinal q. Tout élément ζ de κ^* est racine simple du polynôme $X^{q-1}-1$, donc se relève en une unique racine $[\zeta]$ de ce polynôme dans $\mathcal{O}_K$. On dit que $[\zeta]$ est le *relèvement de Teichmüller* de ζ, par unicité il vérifie $[\zeta\zeta'] = [\zeta][\zeta']$ pour tous ζ, ζ' de κ.

Exercice 4.28 Soit K un corps local de corps résiduel κ et d'uniformisante π. On pose $U_K^1 := 1 + \pi\mathcal{O}_K$ et on note p la caractéristique de κ.

a) Montrer que U_K^1 est un sous-groupe multiplicatif de $\mathcal{O}_K^*$, et qu'on a un isomorphisme

$$K^* \simeq \mathbf{Z} \times \kappa^* \times U_K^1.$$

b) Montrer que U_K^1 possède une filtration par les sous-groupes $U_K^i := (1+\pi^i\mathcal{O}_K)$ $(i \in \mathbf{N}^*)$, dont l'intersection est réduite à $\{1\}$ et dont les quotients successifs sont des p-groupes.

4.5. Extensions non ramifiées

Dans ce paragraphe, on suppose que K est un corps complet pour une valuation discrète, de corps résiduel κ. On fixe une clôture séparable K^{sep} de K. Soit L une extension finie de K, le théorème 4.20 dit qu'il n'y a qu'une valuation de L au-dessus de celle de K, ce qui permet de parler sans ambiguité de l'extension résiduelle (resp. de l'indice de ramification, du degré résiduel etc.) de l'extension.

Theorème 4.29 *a) Soit L une extension finie de K dont l'extension résiduelle κ_L/κ est séparable et de degré f. Il existe une unique sous-extension non ramifiée K'/K de degré résiduel f, et c'est la plus grande sous-extension de L/K qui est non ramifiée sur K.*

b) Soit κ_1/κ une extension finie galoisienne. Alors il existe une unique extension finie non ramifiée $K_1 \subset K^{\text{sep}}$ de K dont l'extension résiduelle est isomorphe à κ_1/κ. De plus, K_1 est galoisienne avec $\text{Gal}\,(K_1/K) \simeq \text{Gal}\,(\kappa_1/\kappa)$.

Noter qu'en particulier, si κ_L/κ est supposée galoisienne dans a), c'est aussi le cas de K'/K et son groupe de Galois est isomorphe à $\text{Gal}\,(\kappa_L/\kappa)$ (plonger L dans K^{sep} et appliquer b).

Démonstration : Montrons d'abord l'existence dans a). Par le théorème de l'élément primitif, on peut écrire $\kappa_L = \kappa[X]/(P)$ avec P irréductible unitaire dans $\kappa[X]$. On relève P en un $\widetilde{P} \in \mathcal{O}_K[X]$ unitaire. Soit α une racine de P dans κ_L, c'est une racine simple et le lemme de Hensel dit alors qu'elle

se relève en une unique racine $\widetilde{\alpha} \in \mathcal{O}_L$ de $\widetilde{P}$ dont la réduction (modulo une uniformisante π_L de L) est α. Posons alors $K' = K(\tilde{\alpha})$, alors K' est de degré $f = \deg P = \deg \widetilde{P}$ sur K (il est en effet immédiat que P reste irréductible sur K) et la réduction modulo π_L induit une flèche $\mathcal{O}_{K'} \hookrightarrow \mathcal{O}_L \to \kappa_L$ dont l'image est κ_L (puisque $\mathcal{O}_{K'}$ contient $\tilde{\alpha}$), ce qui montre que le corps résiduel de K' est κ_L. Ainsi K'/K est non ramifiée puisque son degré f coïncide avec celui de l'extension de corps résiduels associée.

Montrons b). Écrivons $\kappa_1 = \kappa[X]/(Q)$, où Q est un polynôme unitaire irréductible de degre d sur κ, qui est donc scindé à racines simples sur κ_1. Soit $\widetilde{Q} \in \mathcal{O}_K[X]$ un polynôme unitaire relevant Q, il est encore irréductible. Posons alors $K_1 = K[X]/(\widetilde{Q})$, et plongeons le corps K_1 dans K^{sep}. C'est une extension finie de K de corps résiduel κ_1 et de degré $d = \deg Q = [\kappa_1 : \kappa]$, elle est donc non ramifiée. De plus $\widetilde{Q}$ est scindé à racines simples sur K_1 par le lemme de Hensel, donc K_1 est galoisienne sur K. L'isomorphisme entre les groupes de Galois résulte alors du théorème 2.27. Si maintenant F est une autre sous-extension de K^{sep} qui est non ramifiée sur K et dont l'extension résiduelle est isomorphe à κ_1/κ, on a comme ci-dessus $F = K(\tilde{\beta})$, où $\tilde{\beta}$ est une racine de Q, donc $F = K_1$ vu que K_1 est le corps de décomposition (inclus dans K^{sep}) de Q sur K, qui est aussi un corps de rupture pour Q.

Montrons enfin que dans a), K' est la plus grande sous-extension non ramifiée de K incluse dans L (elle est donc unique). Soit F une telle sous-extension, son corps résiduel κ_F est une sous-extension de κ_L, qu'on peut écrire $\kappa_F = \kappa[X]/(R)$ avec R unitaire irréductible sur κ. Avec des notations comme ci-dessus, on a alors $F = K(\tilde{\gamma})$, où $\tilde{\gamma} \in \mathcal{O}_F$ est une racine de $\widetilde{R}$ qui relève une racine γ de R dans κ_F. Mais par le lemme de Hensel, $\widetilde{R}$ possède également une unique racine dans K' qui relève γ, c'est donc forcément $\tilde{\gamma}$ et $F \subset K'$.

□

Corollaire 4.30 *La réunion (dans K^{sep}) de toutes les extensions finies non ramifiées de K est galoisienne, de groupe de Galois isomorphe au groupe de Galois absolu de κ. On dit que c'est l'extension maximale non ramifiée de K.*

Cela résulte du théorème 4.29 b) par passage à la limite sur toutes les extensions finies galoisiennes de κ incluses dans une clôture séparable fixée de κ.

Remarque 4.31 La valuation de K se prolonge en une valuation sur K^{nr}, une uniformisante de K restant une uniformisante de K^{nr}. Attention, K^{nr} ne reste en général pas complet [4] pour cette valuation discrète.

4. Il reste par contre *hensélien*.

Corollaire 4.32 *Si K est un corps local et $d \in \mathbf{N}^*$, alors il existe un unique sous-corps de K^{sep} qui est non ramifié et de degré d sur K. Le groupe $\mathrm{Gal}\,(K^{\mathrm{nr}}/K)$ est isomorphe à $\widehat{\mathbf{Z}} := \varprojlim_{d\in\mathbf{N}^*}(\mathbf{Z}/d\mathbf{Z}) \simeq \prod_{p\in\mathcal{P}} \mathbf{Z}_p$ (où $\mathcal{P}$ désigne l'ensemble des nombres premiers).*

Démonstration : Comme le corps résiduel κ est fini, on sait qu'il admet une unique extension de degré d, dont le groupe de Galois sur κ est isomorphe à $\mathbf{Z}/d\mathbf{Z}$, d'où le résultat avec le théorème 4.29 b) et le corollaire 4.30.

□

4.6. Classification des corps locaux

On commence par le classique résultat suivant, qui décrit les valeurs absolues sur $\mathbf{Q}$:

Theorème 4.33 (Ostrowski) *Les places de $\mathbf{Q}$ sont associées soit à la valeur absolue usuelle $|.|_\infty$, soit à la valeur absolue p-adique $x \mapsto |x|_p := p^{-v_p(x)}$ pour un certain nombre premier p. De plus, ces places sont distinctes deux à deux.*

Démonstration : Soit $|.|$ une valeur absolue ultramétrique sur $\mathbf{Q}$. Soit $\mathcal{O}$ son anneau de valuation et $\wp$ son idéal maximal. Alors $\wp \cap \mathbf{Z}$ est un idéal premier de $\mathbf{Z}$, qui ne peut pas être nul (sinon la valeur absolue serait triviale). Il existe donc un nombre premier p tel que $\wp \cap \mathbf{Z} = p\mathbf{Z}$. Si m est un entier premier à p, on a alors $|m| = 1$, ce qui montre que pour tout entiers r, s premiers à p, on a

$$|p^\alpha . \frac{r}{s}| = |p^\alpha| = |p|^\alpha$$

pour tout entier α, d'où on déduit que $|.|$ est équivalente à la valeur absolue p-adique. Si p et q sont deux nombres premiers distincts, les valeurs absolues correspondantes n'ont pas le même anneau de valuation, donc ne sont pas équivalentes.

Supposons maintenant que $|.|$ n'est pas ultramétrique. D'après l'exercice 4.7, on a alors $|a| > 1$ pour tout entier $a \geq 2$. Soient $a, b \geq 2$ deux entiers. On écrit b en base a, soit

$$b = \sum_{j=0}^{k} b_j a^j,\ 0 \leq b_j < a, \quad b_k \geq 1,$$

ce qui donne en particulier $k \leq \frac{\ln b}{\ln a}$ et

$$|b| \leq C \sum_{j=0}^{k} |a|^j,$$

où $C = \max(|1|, |2|, ..., |a-1|)$ est une constante indépendante de b. On obtient

$$|b| \leq C \frac{|a|^{k+1} - 1}{|a| - 1} \leq C' |a|^{\frac{\ln b}{\ln a}} = C' b^{\frac{\ln(|a|)}{\ln a}},$$

où C' est une autre constante. Posons $s = \frac{\ln(|a|)}{\ln a}$, on a $0 < s \leq 1$ et $|b| \leq C' b^s$. En appliquant ceci à b^m pour m entier et en faisant tendre m vers $+\infty$, on voit qu'en fait $|b| \leq b^{\frac{\ln(|a|)}{\ln a}} = b^s$. En échangeant les rôles de a et b, on obtient $|a| \leq a^{\frac{\ln(|b|)}{\ln b}}$, soit $\frac{\ln(|b|)}{\ln b} \geq \frac{\ln(|a|)}{\ln a} = s$, ou encore $|b| \geq b^s$. Finalement, on a $|b| = b^s = |b|_\infty^s$ pour tout entier $b \geq 2$, et on étend immédiatement la formule à tout rationnel par multiplicativité de la valeur absolue.

□

Theorème 4.34 *Soit K un corps local de caractéristique zéro. Alors K est isomorphe à une extension finie de $\mathbf{Q}_p$ pour un certain nombre premier p.*

Démonstration : Le corps K contient $\mathbf{Q}$ (comme son sous-corps premier) et la restriction de la valeur absolue à $\mathbf{Q}$ est non triviale, sinon $\mathbf{Q}$ s'injecterait dans le corps résiduel de K, lequel est fini. D'après le théorème 4.33, cette restriction est équivalente à la valeur absolue $|.|_p$ pour un certain nombre premier p. L'adhérence $\widehat{\mathbf{Q}}$ de $\mathbf{Q}$ dans K est alors un sous-groupe localement compact (car fermé dans un groupe localement compact), donc complet et $\widehat{\mathbf{Q}}$ s'identifie au complété de $\mathbf{Q}$ pour $|.|_p$, c'est-à-dire à $\mathbf{Q}_p$. Par ailleurs, le théorème de Riesz implique que K est de dimension finie sur $\widehat{\mathbf{Q}}$, d'où le résultat.

□

Remarque 4.35 Il est classique (théorème de Gelfand-Mazur) que tout corps valué complet non ultramétrique est isomorphe à $\mathbf{R}$ ou $\mathbf{C}$. Du coup, on voit (en le plongeant dans son complété) que tout corps valué K non ultramétrique a une valeur absolue donnée par $x \mapsto |j(x)|$, où j est un plongement de K dans $\mathbf{C}$ et $|.|$ est le module usuel.

On a un également un résultat en caractéristique p :

Theorème 4.36 *Soit K un corps local de caractéristique $p > 0$. Alors K est isomorphe à $k((T))$, où k est son corps résiduel.*

Démonstration : Soit q le cardinal du corps résiduel k. Considérons le relevé de Teichmüller $x \mapsto [x]$ de k^* dans K^*, qu'on étend à k en posant $[0] = 0$. On a déjà vu que ce relevé était multiplicatif. En caractéristique p, on a également $[x+y] = [x] + [y]$ pour tous x, y de k : c'est immédiat si x, y, ou $x+y$ est nul, et sinon cela résulte de la formule

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

laquelle montre que $([x]+[y])$ est bien le relevé de Teichmüller de $x+y$. Ainsi $[.]$ est un morphisme de corps de k dans K, on l'étend alors en un morphisme de corps $k((T)) \to K$ en envoyant $\sum_{n \geq -N} a_n T^n$ sur $\sum_{n \geq -N} [a_n] \pi^n$, où on a fixé une uniformisante π de K. Il est facile de voir (cf. exercice 4.14) qu'il s'agit d'un isomorphisme de corps valués.

□

5. Corps globaux

5.1. Extensions des valeurs absolues

On commence par un énoncé qui relie extensions et complétions pour un anneau de valuation discrète.

Theorème 5.1 *Soit L/K une extension de corps de degré n. Soit v une valuation discrète sur K, dont on note A_v l'anneau. Soit B_v la fermeture intégrale de A_v dans L, dont on suppose que c'est un A_v-module de type fini (ex. L/K séparable). Soient $w_1, ..., w_r$ les différentes valuations de L correspondant aux idéaux premiers non nuls de B_v, on note e_i l'indice de ramification de w_i et f_i son degré résiduel. Soit $\widehat{K}$ le complété de K pour v et $\widehat{L}_i$ le complété de L pour w_i.*

a) On a $[\widehat{L}_i : \widehat{K}] = n_i := e_i f_i$.

b) La valuation w_i est l'unique valuation de $\widehat{L}_i$ au-dessus de v ; son indice de ramification et son degré résiduel dans l'extension $\widehat{L}_i/\widehat{K}$ sont respectivement e_i et f_i.

c) Le morphisme canonique

$$\varphi : L \otimes_K \widehat{K} \to \prod_{i=1}^{r} \widehat{L}_i$$

est un isomorphisme.

Démonstration : Le point b) résulte immédiatement du théorème 4.20. On en déduit le point a) via le corollaire 4.22. Montrons c). Les deux termes sont des $\widehat{K}$-espaces vectoriels normés de dimension n via la formule

$$n = \sum_{i=1}^{r} e_i f_i$$

(théorème 2.20). L'image de φ est dense par le lemme d'approximation (théorème 2.19), ce qui implique la surjectivité de φ vu qu'en dimension finie, un $\widehat{K}$-sous-espace vectoriel est fermé (car complet) vu que $\widehat{K}$ est complet. Par égalité des dimensions, φ est bijective.

□

Corollaire 5.2 *Si l'extension L/K est séparable, c'est aussi le cas des $\widehat{L}_i/\widehat{K}$. Si L/K est galoisienne de groupe de Galois G, l'extension $\widehat{L}_i/\widehat{K}$ est galoisienne de groupe de Galois D_i, où D_i est le groupe de décomposition de w_i dans G.*

Démonstration : Supposons L/K séparable, alors d'après le théorème 5.1 c), la $\widehat{K}$-algèbre de dimension finie $\prod_{i=1}^{r} \widehat{L}_i$ est une algèbre étale, donc chaque $\widehat{L}_i$ est une extension séparable de $\widehat{K}$. Si de plus L/K est galoisienne, tout élément de D_i se prolonge par continuité en un $\widehat{K}$-automorphisme de $\widehat{L}_i$, d'où un plongement $D_i \hookrightarrow \mathtt{Aut}_{\widehat{K}}(\widehat{L}_i)$. Comme le cardinal de D_i est $n_i = e_i f_i == [\widehat{L}_i : \widehat{K}]$ par la proposition 2.29, on en déduit que $\widehat{L}_i/\widehat{K}$ est galoisienne de groupe D_i (vu qu'elle a au moins n_i automorphismes, ceux induits par les éléments de D_i).

□

Exercice 5.3 Soit B_i l'anneau de la valuation w_i. Montrer qu'on a un isomorphisme

$$B_v \otimes_{A_v} \widehat{A} \simeq \prod_{i=1}^{r} \widehat{B}_i$$

(on pourra d'abord montrer que les deux termes sont des $\widehat{A}_v$-modules libres de type fini, puis considérer la réduction de chaque terme modulo l'idéal maximal de $\widehat{A}_v$).

Remarque 5.4 On peut appliquer le théorème 5.1 à la situation plus globale suivante. Soient A un anneau de Dedekind de corps des fractions K, L une extension finie séparable de K, et B la fermeture intégrale de A dans L. Pour tout idéal premier $\wp$ de A correspondant à une valuation v, on est dans

la situation du théorème en posant $A_v = S^{-1}A$ et $B_v = S^{-1}B$, où S est la partie multiplicative $A - \wp$. L'anneau B_v est semi-local, ses idéaux maximaux étant les $\mathfrak{q}_i B_v$, où les $\mathfrak{q}_i$ sont les idéaux premiers de B au-dessus de $\wp$. Les valuations $w_1, ..., w_r$ du théorème 5.1 sont donc les valuations sur L induites par les a.v.d. $B_{\mathfrak{q}_i} = (B_v)\wp_i$.

Exercice 5.5 On se place dans la situation de la remarque 5.4. Soit $\wp$ un idéal maximal de A et $\mathfrak{q}$ un idéal maximal de B au-dessus de $\wp$. On note $K_\wp$ le complété de L pour la place définie par $\wp$ et $L_\mathfrak{q}$ le complété de L pour la place définie par $\mathfrak{q}$, puis $\mathcal{O}_\wp$ et $\mathcal{O}_\mathfrak{q}$ leurs anneaux de valuation respectifs.

a) En utilisant l'exercice 5.3, montrer que la flèche naturelle

$$B \otimes_A \mathcal{O}_\wp \to \prod_{\mathfrak{q}|\wp} \mathcal{O}_\mathfrak{q}$$

est un isomorphisme de $\mathcal{O}_\wp$-modules.

b) Montrer que sous cet isomorphisme, l'application $\mathrm{Tr}_{L/K} \otimes \mathrm{Id}$ s'identifie à $\prod_{\mathfrak{q}|\wp} \mathrm{Tr}_{L_\mathfrak{q}/K_\wp}$.

c) Montrer que

$$\mathcal{D}_{B/A}^{-1} \otimes_A \mathcal{O}_\wp \simeq \prod_{\mathfrak{q}|\wp} \mathcal{D}_{\mathcal{O}_\mathfrak{q}/\mathcal{O}_\wp}^{-1}.$$

d) Montrer que la différente locale $\mathcal{D}_{\mathcal{O}_\mathfrak{q}/\mathcal{O}_\wp}$ est l'idéal de $\mathcal{O}_\mathfrak{q}$ engendré par $\mathcal{D}_{B/A}$ et que les discriminants locaux sont liés par la formule

$$\Delta_{B/A} = \prod_{\mathfrak{q}|\wp} \Delta_{\mathcal{O}_\mathfrak{q}/\mathcal{O}_\wp}.$$

e) Retrouver que $\mathfrak{q}$ est non ramifié dans l'extension B/A si et seulement s'il ne divise pas la différente (on se ramènera au cas où A et B sont des a.v.d. complets via d) ; puis prendre une base de B sur A et son image comme base de $B/\wp B$ sur $A/\wp$; et enfin traduire le fait que $B/\wp$ soit un corps extension séparable de $A/\wp$ en termes de la non nullité du déterminant de la forme bilinéaire trace dans cette base).

5.2. Places d'un corps de nombres et d'un corps de fonctions

Définition 5.6 Un *corps global* est un corps de nombres ou une extension finie (qu'on peut supposer séparable) de $\mathbf{F}_q(t)$, où $\mathbf{F}_q$ est un corps fini.

Les deux types de corps globaux partagent de nombreuses propriétés. En particulier ce sont les corps de fractions d'anneaux de Dedekind (via le théorème 2.6, vu que $\mathbf{Z}$ et $\mathbf{F}_q[T]$ sont des anneaux de Dedekind. De plus, le complété d'un corps global pour une valuation discrète est un corps local puisque les corps résiduels correspondant aux idéaux premiers de $\mathbf{Z}$ et de $\mathbf{F}_q[T]$ sont finis.

On va maintenant décrire les places d'un corps global, en commençant par le cas d'un corps de nombres K d'anneau des entiers $\mathcal{O}_K$, fermeture intégrale de $\mathbf{Z}$ dans K. Pour tout idéal premier non nul $\wp$ de $\mathcal{O}_K$, on dispose de la valeur absolue normalisée

$$x \mapsto |x|_\wp := N(\wp)^{-v_\wp(x)},$$

où $N(\wp)$ est la norme de $\wp$, c'est-à-dire le cardinal du corps résiduel $\mathcal{O}_K/\wp$.

Theorème 5.7 *Soit K un corps de nombres. L'application $u : \wp \mapsto |.|_\wp$ induit une bijection des idéaux premiers non nuls de $\mathcal{O}_K$ sur les places ultramétriques de K.*

Démonstration : Une valeur absolue ultramétrique $|.|_K$ sur K induit une valeur absolue ultramétrique sur $\mathbf{Q}$. On sait (théorème 4.33) que cette valeur absolue est alors associée à la valuation discrète v_p pour un unique nombre premier p, ce qui fait que $|.|_K$ correspond à une valuation discrète w, dont la boule unité ouverte est un idéal premier $\wp$ non nul de $\mathcal{O}_K$ au-dessus de $p\mathbf{Z}$. Il suffit de montrer que w et $v_\wp$ induisent des valeurs absolues équivalentes pour conclure (on aura construit une bijection réciproque à u en envoyant toute place ultramétrique de K sur sa boule ouverte unité). Soit $\mathcal{O}_w$ l'anneau de la valuation w, on a $\mathcal{O}_K \subset \mathcal{O}_w$, et aussi $(\mathcal{O}_K)_\wp \subset \mathcal{O}_w$ vu que les éléments de $\mathcal{O}_K - \wp$ sont inversibles dans $\mathcal{O}_w$. Les a.v.d. $(\mathcal{O}_K)_\wp$ et $\mathcal{O}_w$ sont en fait égaux, car si un élément x de K^* n'est pas dans $(\mathcal{O}_K)_\wp$, alors x^{-1} est dans l'idéal maximal $\wp(\mathcal{O}_K)_\wp$ de $(\mathcal{O}_K)_\wp$, donc aussi dans celui de $\mathcal{O}_w$, d'où $x \notin \mathcal{O}_w$. Ainsi, les boules unités pour w et $v_\wp$ sont les mêmes, ce qui implique que les valeurs absolues associées sont équivalentes.

□

Remarque 5.8 Le même argument montre que dans le théorème 5.1, les places de L au-dessus de la place v sont exactement celles associées aux w_i. Si K est un corps de nombres et L une extension finie de K, on peut appliquer ce théorème à toute place ultramétrique v de K (qui correspond à un idéal premier $\wp$ de $\mathcal{O}_K$), cf. remarque 5.4.

Proposition 5.9 *Les places non ultramétriques d'un corps de nombres K avec $[K : \mathbf{Q}] = d$ sont données par $x \mapsto |j_r(x)|$ avec $1 \leq r \leq d$, où $j_1, ..., j_d$ sont les différents plongements de K dans $\mathbf{C}$ et $|.|$ est le module usuel. On a $d = r_1 + 2r_2$, où r_1 est le nombre de ces plongements qui sont réels, et $2r_2$ le nombre de ces plongements qui ne le sont pas.*

Démonstration : Cela résulte par exemple de la remarque 4.35, combinée au fait que si j est un plongement non réel de K dans $\mathbf{C}$, alors son conjugué $\bar{j}$ en est un autre.

□

Passons aux corps de fonctions. On sait que dans ce cas toutes les places sont ultramétriques. On peut les décrire précisément pour le corps $\mathbf{F}_q(t)$ via la construction suivante : pour tout polynôme irréductible unitaire P de $\mathbf{F}_q[T]$, on définit une valuation sur l'anneau principal $\mathbf{F}_q[T]$ en posant $v_P(F) = m$, où m est la plus grande puissance de P qui divise F, valuation qu'on étend au corps des fractions $\mathbf{F}_q(t)$. On peut également poser $v_\infty(R/S) = \deg R - \deg S$ pour tous R, S de $\mathbf{F}_q[T] - \{0\}$. On a alors :

Theorème 5.10 *Les places de $\mathbf{F}_q(t)$ sont données par les valuations v_P pour P irréductible et v_∞.*

Démonstration : Soit $|.|$ une valeur absolue non triviale sur $\mathbf{F}_q(t)$. Supposons d'abord que tout élément de $\mathbf{F}_q[T]$ soit dans la boule unité fermée. La boule unité ouverte est alors un idéal premier non nul de $\mathbf{F}_q[T]$, il existe donc un unique polynôme irréductible unitaire P qui l'engendre. Tout F de $\mathbf{F}_q(t)$ s'ecrit alors $F = P^{v_P(F)}(R/S)$ avec R et S polynômes non divisibles par P (donc de valeur absolue 1), d'où $|F| = |P|^{v_P(F)}$, ce qui montre que $|.|$ est équivalente à une valeur absolue induite par v_P.

Si maintenant on a un $Q \in \mathbf{F}_q[T]$ avec $|Q| > 1$, alors $|T| > 1$ vu que la valeur absolue d'un polynôme constant non nul est 1. Ceci implique que $\mathbf{F}_q[T^{-1}]$ est inclus dans la boule unité fermé avec T^{-1} dans la boule unité ouverte. On prouve alors comme ci-dessus (en remplaçant $\mathbf{F}_q[T]$ par $\mathbf{F}_q[T^{-1}]$) que $|.|$ est équivalente à v_∞.

Les places ainsi construites sont bien deux à deux distinctes, car leurs boules unité ouvertes sont deux à deux distinctes.

□

Remarque 5.11 Pour une extension finie séparable K de $\mathbf{F}_q(t)$, on a un énoncé analogue (qui se ramène facilement au précédent) en considérant une courbe projective lisse C sur $\mathbf{F}_q$ dont le corps des fonctions est K. Les places

sont alors données par les valuations aux divers points fermés de C. Le cas $K = \mathbf{F}_q(t)$ correspond à $C = \mathbf{P}^1_{\mathbf{F}_q}$, les points fermés étant ceux de la droite affine $\mathbf{P}^1_{\mathbf{F}_q}$ (qui correspondent aux polynômes irréductibles unitaires de $\mathbf{F}_q[T]$), plus le point à l'infini qui donne la valuation v_∞.

5.3. Formule du produit

Soit K un corps global. Pour toute place v de K, on note $|.|$ la valeur absolue normalisée induite par v, avec la convention de la remarque 4.19 que pour une place complexe non réelle d'un corps de nombres, $|.|_v$ désigne le *carré* du module complexe usuel. On note K_v le complété de K en la place v.

Theorème 5.12 *Soit K un corps global dont on note Ω_K l'ensemble de toutes les places. Alors, pour tout $x \in K^*$, on a $|x|_v = 1$ pour presque toute place v et*

$$\prod_{v \in \Omega_k} |x|_v = 1.$$

On montre d'abord un lemme :

Lemme 5.13 *a) Soit $x \in K$. Alors $|x|_v \leq 1$ pour presque toute place v.*

b) Soit L/K une extension finie de corps globaux. Alors pour tout x de L et toute place v de K, on a :

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

Démonstration : a) Supposons d'abord que K est un corps de nombres. Soit x dans K, on peut trouver $m \in \mathbf{N}^*$ tel que $mx \in \mathcal{O}_K$. Si v est ultramétrique, elle est au-dessus d'un certain nombre premier p. Comme $|y|_p \leq 1$ pour tout y de $\mathbf{Z}$, on a $|z|_v \leq 1$ pour tout z de $\mathcal{O}_K$ vu que $\mathcal{O}_K$ est entier sur $\mathbf{Z}$. Ainsi, $|mx|_v \leq 1$, mais comme $|m|_p = 1$ pour presque tout p, on a $|m|_v = 1$ pour presque toute v, et donc $|x|_v \leq 1$ pour presque toute v (il n'y a qu'un nombre fini de places non ultramétriques). Le cas du corps de fonctions est analogue en remplaçant $\mathbf{Z}$ par $\mathbf{F}_q[T]$ et $\mathbf{Q}$ par $\mathbf{F}_q(T)$, en notant que seul un nombre fini de places (celles au-dessus de v_∞) ne vérifient pas $|y|_v \leq 1$ pour tout y de $\mathbf{F}_q[T]$.

b) On sait que $N_{L/K}(x)$ est le déterminant de la multiplication de x dans K, ou encore celui de la multiplication par $(x \otimes 1)$ dans $L \otimes_K K_v$. Le

théorème 5.1 c) donne alors

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

la dernière égalité résultant du corollaire 4.23 c) (qui s'étend bien au cas où v est une place réelle ou complexe via la convention de normalisation adoptée). □

Preuve du théorème 5.12 : La première assertion résulte immédiatement du lemme 5.13 a) appliqué à x et x^{-1}. Pour montrer la formule, le lemme 5.13 b) permet de se ramener aux cas $K = \mathbf{Q}$ et $K = \mathbf{F}_q(t)$, qu'on traite facilement par un calcul direct via la description des places de $\mathbf{Q}$ (théorème 4.7) et de $\mathbf{F}_q(t)$ (théorème 5.10).

6. Adèles et idèles

L'utilisation des adèles et des idèles permet de donner une présentation plus moderne de résultats classiques tels que la finitude du groupe des classes d'idéaux d'un corps de nombres ou le théorème des unités de Dirichlet. Elle est aussi très commode dans la théorie du corps de classes, pour laquelle la présentation classique en termes d'idéaux est moins commode.

Dans toute la suite, on désigne par K un corps global et par Ω_K (resp. Ω_f, Ω_∞) l'ensemble de toutes ses places (resp. de ses places ultramétriques, de ses places archimédiennes si K est un corps de nombres). On note K_v le complété du corps K en la place v et $\mathcal{O}_v \subset K_v$ l'anneau de valuation de v dans K_v si v est ultramétrique, en convenant que $\mathcal{O}_v = K_v$ si v est archimédienne.

6.1. Adèles

Définition 6.1 On définit un sous-anneau $\mathbf{A}_K$ du produit $\prod_{v\in\Omega_K} K_v$ comme le produit restreint des K_v par rapport aux $\mathcal{O}_v$. On l'appelle anneau des *adèles* de K.

Explicitement, $\mathbf{A}_K$ est donc l'ensemble des familles (x_v) dans $\prod_{v\in\Omega_K} K_v$ telles que $x_v \in \mathcal{O}_v$ pour presque toute place v. On le munit de sa topologie de produit restreint, c'est-à-dire de la structure de groupe additif topologique pour laquelle les voisinages ouverts de 0 sont les parties de la forme $\prod_{v\in\Omega_K} U_v$, avec U_v ouvert de K_v et $U_v = \mathcal{O}_v$ pour presque toute v.

Proposition 6.2 *Le groupe topologique $\mathbf{A}_K$ est localement compact. Son sous-groupe*

$$U := \prod_{v\in\Omega_f} \mathcal{O}_v \times \prod_{v\in\Omega_\infty} \{0\}$$

est compact, et c'est un ouvert de $\mathbf{A}_K$ si K est un corps de fonctions.

Démonstration : On sait que $\mathcal{O}_v$ est compact et ouvert dans K_v si v est ultramétrique. Si on choisit un voisinage compact U_v de 0 pour chaque place archimédienne v, alors $\prod_{v\in\Omega_f} \mathcal{O}_v \times \prod_{v\in\Omega_\infty} U_v$ est un voisinage compact (comme produit de compacts) de 0, donc $\mathbf{A}_K$ (qui est séparé comme sous-espace d'un espace séparé) est localement compact. De même, U est compact comme produits de compact, et dans le cas du corps de fonctions c'est un ouvert par définition de la topologie de produit restreint.

□

Remarque 6.3 On a même que $\mathbf{A}_K$ est un anneau topologique (on vérifie immédiatement que la multiplication dans $\mathbf{A}_K$ est continue). Attention, la topologie sur $\mathbf{A}_K$ est plus fine que celle induite par $\prod_{v\in\Omega_K} K_v$.

On a un plongement diagonal $K \to \mathbf{A}_K$ via le lemme 5.13 a) ; on notera souvent encore K l'image de K dans $\mathbf{A}_K$.

Theorème 6.4 *Le sous-groupe K de $\mathbf{A}_K$ est discret pour la topologie induite, et $\mathbf{A}_K/K$ est compact pour la topologie quotient.*

Démonstration : Fixons une place v_0 de K et un $r \in]0,1[$. Le voisinage de zéro dans $\mathbf{A}_K$ défini par

$$V := \{(x_v) \in \mathbf{A}_K,\ |x_{v_0}| < r, |x_v|_v \leq 1 \text{ si } v \neq v_0\}$$

vérifie $V \cap K = \{0\}$ via la formule du produit. Ainsi K est discret dans $\mathbf{A}_K$. Pour montrer la compacité de $\mathbf{A}_K/K$, on va traiter le cas du corps de nombres (le cas d'un corps de fonctions est analogue en remplaçant $\mathbf{Z}$ par $\mathbf{F}_q[T]$ et la place archimédienne de $\mathbf{Z}$ par v_∞, cf. théorème 5.10). Posons $K_\infty = K \otimes_{\mathbf{Q}} \mathbf{R} = \prod_{v|\infty} K_v$.

Lemme 6.5 *On a*

$$\mathbf{A}_K = K + (K_\infty \times \prod_{v\not|\infty} \mathcal{O}_v)$$

et

$$K \cap (K_\infty \times \prod_{v\not|\infty} \mathcal{O}_v) = \mathcal{O}_K.$$

Démonstration : Soit $(x_v) \in \mathbf{A}_K$, alors il n'existe qu'un nombre fini S de places ultramétriques de K telles que $|x_v|_v > 1$. D'après le lemme d'approximation (théorème 2.19), il existe $y \in K$ tel que $|x_v - y|_v \leq 1$ pour $v \in S$ et $|y|_v \leq 1$ pour toute place v de K non dans S et non au-dessus de ∞. Alors

$$(x_v - y) \in (K_\infty \times \prod_{v|\not\infty} \mathcal{O}_v),$$

d'où le premier point. Le deuxième résulte de ce qu'un élément de K qui est dans $(\mathcal{O}_K)_\wp$ pour tout idéal maximal de $\mathcal{O}_K$ est dans $\mathcal{O}_K$.

□

Reprenons la preuve du théorème 6.4. Le lemme 6.5 donne un isomorphisme de groupe topologiques

$$\mathbf{A}_K/K \simeq (K_\infty \times \prod_{v|\not\infty} \mathcal{O}_v)/\mathcal{O}_K.$$

Fixons une base $(e_1, ..., e_d)$ de $\mathcal{O}_K$ sur $\mathbf{Z}$, c'est aussi une base de K sur $\mathbf{Q}$, et $(e_1 \otimes_1, ..., e_d \otimes 1)$ est une base du $\mathbf{R}$-espace vectoriel K_∞. Posons alors

$$Q := \{\sum_{i=1}^{d} t_i(e_i \otimes 1),\ -1/2 \leq t_i \leq 1/2\},$$

c'est un compact de K_∞ (car fermé et borné) et on a une surjection continue $Q \to K_\infty/\mathcal{O}_K$, d'où une surjection continue

$$Q \times \prod_{v|\not\infty} \mathcal{O}_v \to \mathbf{A}_K/K.$$

Le terme de gauche est compact comme produit de compacts, donc celui de droite (qui est séparé car K est discret, donc fermé dans K) est compact.

□

Remarque 6.6 La preuve donne une surjection $Q \times \prod_{v|\not\infty} \mathcal{O}_v \to \mathbf{A}_K/K$. Via l'équivalence des normes sur un $\mathbf{R}$-espace vectoriel de dimension finie, on obtient une surjection $W \to \mathbf{A}_K/K$, où W est un compact de $\mathbf{A}_K$ défini comme l'ensemble des (x_v) avec $|x_v| \leq M$ si v est archimédienne et $x_v \in \mathcal{O}_v$ si v est ultramétrique, où $M > 0$ est une constante. On a un énoncé analogue dans le cas d'un corps de fonctions en remplaçant l'ensemble des places archimédiennes par l'ensemble des places au-dessus de la place v_∞ de $\mathbf{F}_q(T)$.

Exercice 6.7 Soit L une extension finie séparable de K. Alors on a un isomorphisme d'anneaux topologiques

$$\mathbf{A}_K \otimes_K L \simeq \mathbf{A}_L,$$

dans lequel l'injection canonique $K \otimes_K L = L \hookrightarrow \mathbf{A}_L$ correspond au plongement diagonal de L dans $\mathbf{A}_L$ (prendre une base de L sur K et utiliser l'exercice 5.3.

6.2. Théorème d'approximation forte

Comme tout groupe localement compact, on dispose d'une *mesure de Haar* (:= invariante par translation) sur $\mathbf{A}_K$, bien définie à multiplication par une constante près. Plus précisément, on peut la définir de la manière suivante : si v est une place ultramétrique, on définit μ_v comme la mesure de Haar sur K_v telle que $\mu(\mathcal{O}_v) = 1$. Pour une place réelle v, on prend pour μ_v la mesure de Lebesgue sur K_v et si v est complexe on prend la mesure $\mu_v = 2dxdy = dzd\bar{z}$ sur $K_v \simeq \mathbf{C}$ (identifié à $\mathbf{R}^2$ avec coordonnées (x, y) dans la première écriture). On définit alors μ comme la mesure de Haar sur $\mathbf{A}_K$ pour laquelle une base d'ensemble mesurables est constituée des $\prod_{v\in\Omega_K} M_v$, où $\mu_v(M_v) < +\infty$ pour toute v et $M_v = \mathcal{O}_v$ pour presque toute v, avec la formule

$$\mu(\prod_{v\in\Omega_K} M_v) = \prod_{v\in\Omega_K} \mu_v(M_v).$$

(mesure "produit restreint").

Lemme 6.8 *Soit K un corps global. Alors, il existe une constante $C > 0$ telle que pour tout $\alpha = (\alpha_v)$ dans $\mathbf{A}_K$ vérifiant*

$$\prod_{v\in\Omega_K} |\alpha_v|_v > C, \tag{4}$$

il existe $\beta \in K^*$ tel que $|\beta|_v \leq |\alpha_v|_v$ pour toute place v de K.

Démonstration : Comme presque tous les α_v sont de valeur absolue au plus 1, la condition (4) impose que $|\alpha_v|_v = 1$ pour presque toute v. Soient c_0 la mesure du compact $\mathbf{A}_K/K$ et c_1 celle de l'ensemble des adèles (γ_v) vérifiant : $|\gamma_v| \leq 1/10$ si v est archimédienne et $|\gamma_v| \leq 1$ pour les autres v. On a $0 < c_1 < +\infty$ (car il n'y a qu'un nombre fini de places archimédiennes), posons $C = c_0/c_1$. Soit alors une adèle (α_v) vérifiant (4).

Calculons la mesure de l'ensemble T des adèles (γ_v) vérifiant

$$|\gamma_v| \leq \frac{1}{10}|\alpha_v|_v$$

si v est archimédienne et $|\gamma_v| \leq |\alpha_v|_v$ sinon. Par définition de la mesure de Haar, on a via la condition (4) :

$$\mu(T) = c_1 \prod_v |\alpha_v|_v > c_1 C = c_0.$$

Si on considère l'application de passage au quotient $\mathbf{A}_K \to \mathbf{A}_K/K$, il doit donc exister deux éléments distincts τ, τ' de T qui ont la même image dans $\mathbf{A}_K/K$. En posant $\beta = \tau - \tau'$, on obtient un élément de K qui possède les propriétés voulues, par inégalité triangulaire si v est archimédienne et inégalité ultramétrique pour les autres v.

□

Proposition 6.9 *Soit v_0 une place fixée de K. Pour toute $v \neq v_0$, soit $\delta_v \in \mathbf{R}_+^*$, avec la condition $\delta_v = 1$ pour presque toute v. Alors il existe $\beta \in K^*$ tel que $\beta_v \leq \delta_v$ pour toute place $v \neq v_0$.*

Démonstration : Pour $v \neq v_0$, choisissons α_v avec $0 < |\alpha_v|_v < \delta_v$ et $|\alpha_v|_v = 1$ si $\delta_v = 1$ (donc pour presque toute v). On peut alors trouver $\alpha_{v_0} \in K_{v_0}$ tel que $\prod_{v \in \Omega_K} |\alpha_v|_v > C$, ce qui permet d'appliquer le lemme 6.8 pour obtenir le résultat.

□

Theorème 6.10 (Approximation forte) *Soit K un corps global. Soit v_0 une place de K. Soit S un ensemble fini de places de K avec $v_0 \notin S$. Soit $\alpha_v \in K_v$ pour $v \in S$. Alors pour tout $\varepsilon > 0$, il existe $\beta \in K$ vérifiant : $|\beta - \alpha_v|_v \leq \varepsilon$ pour $v \in S$ et $\beta_v \in \mathcal{O}_v$ pour v non dans $S \cup \{v_0\}$.*

En d'autres termes, K est dense dans le produit restreint (relativement aux $\mathcal{O}_v$) des K_v pour $v \neq v_0$. On voit que la situation est complètement différente du cas où on n'enlève pas une place, auquel cas K est discret dans $\mathbf{A}_K$.

Démonstration : Soit $W \subset \mathbf{A}_K$ comme dans la remarque 6.6, c'est-à-dire que W est défini par des inégalités du type $|\alpha_v|_v \leq \delta_v$ pour toute place v, où (δ_v) est une famille de réels > 0 vérifiant $\delta_v = 1$ pour presque toute place v, et de plus $\mathbf{A}_K = W + K$. La proposition 6.9 donne un $\lambda \in K^*$ tel que

$|\lambda_v|_v \leq \delta_v^{-1}\varepsilon$ pour v dans S, et $|\lambda_v|_v \leq \delta_v^{-1}$ pour v non dans $S \cup \{v_0\}$. Soit alors $\alpha \in \mathbf{A}_K$, alors on peut écrire $\lambda^{-1}\alpha = w + \gamma$ avec $w \in W$ et $\gamma \in K$, d'où $\alpha = w' + \beta$ avec $w' \in \lambda W$ et $\beta \in K$. On obtient le résultat en prenant pour α l'adèle qui vaut α_v pour v dans S et 0 ailleurs.

□

6.3. Idèles

Définition 6.11 Soit K un corps global. Un *idèle* de K est une famille $(x_v)_{v\in\Omega_k}$ dans $\prod_{v\in\Omega_K} K_v^*$, vérifiant $|x_v|_v = 1$ pour presque toute place v de K (autrement dit : $x_v \in \mathcal{O}_v^*$ pour presque toute v). Le groupe multiplicatif des idèles est noté I_K, il est équipé de sa topologie de produit restreint.

Remarque 6.12 On peut dire que I_K est le groupe des inversibles de l'anneau $\mathbf{A}_K$, mais attention, la topologie sur I_K est plus fine que celle induite par celle de $\mathbf{A}_K$: une base de voisinages de 1 dans I_K est constituée des $\prod_{v\in\Omega_K} U_v$ avec U_v ouvert de K_v^* et $U_v = \mathcal{O}_v^*$ pour presque toute v. Tout comme $\mathbf{A}_K$, le groupe I_K est localement compact, et de plus totalement discontinu si K est un corps de fonctions.

On identifie K^* à son image dans I_K via le plongement diagonal. On pose $C_K = I_K/K^*$.

Proposition 6.13 *Le groupe K^* est discret (et donc fermé) dans I_K.*

Démonstration : Soit S un ensemble fini non vide de places de K, contenant l'ensemble des places archimédiennes si k est un corps de nombres. Soit U le voisinage ouvert de 1 dans I_K défini par $(\alpha_v) \in U$ si et seulement si $|\alpha_v - 1|_v < 1$ pour tout $v \in S$ et $|\alpha_v| = 1$ pour $v \notin S$. Alors si $x \in K^*$ n'est pas égal à 1, on a $\prod_{v\in\Omega_K} |x-1|_v = 1$ via la formule du produit, ce qui exclut $x \in U$ sinon on aurait $|x-1|_v < 1$ pour $v \in S$ et $|x-1|_v \leq \max(|x|_v, 1)$ pour $v \notin S$, ce qui impliquerait $\prod_{v\in\Omega_k} |x-1|_v < 1$. Ainsi 1 est un point isolé du sous-groupe image de K^* dans I_K, ce qui montre que ce sous-groupe est discret.

□

Considérons l'homomorphisme continu

$$|.| : I_K \to \mathbf{R}_+^*, \quad (\alpha_v) \mapsto \prod_{v\in\Omega_K} |\alpha_v|_v$$

et notons I_K^0 son noyau. Via la formule du produit, on a $K^* \subset I_K^0$, d'où un homomorphisme induit $|.| : C_K \to \mathbf{R}_+^*$, de noyau $C_K^0 := I_K^0/K^*$.

Theorème 6.14 *Le groupe C_K^0 est compact.*

La preuve du théorème 6.14 repose sur les deux lemmes suivants, qui comparent les deux topologies sur I_K^0.

Lemme 6.15 *Le sous-ensemble I_K^0 est fermé dans $\mathbf{A}_K$ pour la $\mathbf{A}_K$-topologie.*

Démonstration : Soit $\alpha = (\alpha_v)$ une adèle qui n'est pas dans I_K^0. Il s'agit de trouver un voisinage ouvert W de α dans $\mathbf{A}_K$ qui ne rencontre pas I_K^0. Notons déjà que comme presque tous les $|\alpha_v|_v$ sont ≤ 1, le produit infini $C = \prod_{v\in\Omega_K} |\alpha_v|$ a un sens dans $\mathbf{R}_+$, vu que la série de terme général $\log(|\alpha_v|_v)$ est à termes négatifs ou nuls à partir d'un certain rang. Distinguons deux cas :

a) Supposons $C < 1$. Comme α est une adèle, seul un nombre fini de places v de k vérifient $|\alpha_v|_v \geq 1$. La propriété $C < 1$ implique alors qu'on peut trouver un ensemble fini S de places de k tel que S contienne toutes les places v telles que $|\alpha_v|_v \geq 1$, avec de plus $\prod_{v\in S} |\alpha_v|_v < 1$. Il suffit alors de prendre W défini par $|\xi_v - \alpha_v|_v < \varepsilon$ pour $v \in S$ (pour ε assez petit) et $|\xi_v|_v \leq 1$ pour $v \notin S$.

b) Supposons $C \geq 1$. Montrons d'abord que α est forcément un idèle, et donc que $C > 1$ puisque par hypothèse $\alpha \notin I_K^0$. Pour v non archimédienne, la plus grande valeur absolue < 1 dans K_v est q^{-1}, où q est le cardinal du corps résiduel de $\mathcal{O}_v$. Il existe donc (en se ramenant au cas $K = \mathbf{Q}$ ou $K = \mathbf{F}_q(T)$) un ensemble fini S de places de K tel que pour v non dans S, on ait ou bien $|\alpha_v|_v = 1$, ou bien $|\alpha_v|_v \leq 1/2$ (comme α est une adèle, on peut dès le départ supposer que $|\alpha_v|_v \leq 1$ si $v \notin S$). Mais comme le produit infini $\prod |\alpha_v|_v$ converge vers un réel > 0, son terme général tend vers 1, ce qui implique que seuls un nombre fini de $|\alpha_v|_v$ sont $\leq 1/2$. Finalement, quitte à agrandir S, on peut supposer que $|\alpha_v|_v = 1$ pour v non dans S, et α est bien un idèle avec $C > 1$.

Quitte à agrandir S, on peut maintenant aussi supposer que pour toute v non dans S, la propriété $|\xi_v|_v < 1$ implique $|\xi_v|_v < (2C)^{-1}$. Enfin, par définition de C, on peut aussi imposer

$$1 < \prod_{v\in S} |\alpha_v| < 2C.$$

Maintenant, pour $\varepsilon > 0$ assez petit, la condition $|\xi_v - \alpha_v|_v < \varepsilon$ pour $v \in S$ implique

$$1 < \prod_{v\in S} |\xi_v|_v < 2C. \tag{5}$$

On peut alors prendre W défini par $|\xi_v - \alpha_v|_v < \varepsilon$ pour $v \in S$ et $|\xi_v|_v \leq 1$ pour $v \notin S$. En effet une adèle $\xi = (\xi_v)$ de W ne peut pas alors vérifier $|\xi| = 1$, vu l'inéquation (5) et le fait que pour $v \notin S$, $|\xi_v|$ est ou bien égal à 1 ou bien $< (2C)^{-1}$. Finalement I_K^0 est bien fermé dans $\mathbf{A}_K$.

□

Lemme 6.16 *Les topologies induites par $\mathbf{A}_K$ et I_K sur I_K^0 coïncident.*

Démonstration : Soit $\alpha = (\alpha_v) \in I_K^0$. Il est immédiat qu'un $\mathbf{A}_K$-voisinage de α contient un I_K-voisinage de α par définition des topologies de produit restreint vu que $\mathcal{O}_v^* \subset \mathcal{O}_v$ pour toute place ultramétrique v de K. Soit réciproquement H un I_K-voisinage de α, il contient un I_K-voisinage ouvert du type $|\xi_v - \alpha_v|_v < \varepsilon$ pour $v \in S$ et $|\xi_v|_v = 1$ pour $v \notin S$, où S contient les places archimédiennes (si K est un corps de nombres) et toutes les places v telles que $|\alpha_v|_v \neq 1$. En particulier $\prod_{v \in S} |\alpha_v| = 1$ car $\alpha \in I_k^0$. On peut aussi supposer (cf. preuve du lemme 6.15) que pour v non dans S, la condition $|\xi_v|_v < 1$ implique $|\xi_v|_v < 1/2$. Maintenant la propriété $\prod_{v \in S} |\alpha_v| = 1$ permet en plus de choisir ε tel que tout élément (ξ_v) de I_K^0 vérifiant $|\xi_v - \alpha_v|_v < \varepsilon$ pour $v \in S$ et $|\xi_v|_v \leq 1$ pour $v \notin S$ vérifie $\prod_{v \in S} |\xi_v|_v < 2$, donc vérifie en fait $|\xi_v|_v = 1$ pour $v \notin S$ (sinon on aurait une place $v \notin S$ avec $|\xi_v|_v < 1/2$, ce qui contredirait $(\xi_v) \in I_K^0$). Il en résulte que $H \cap I_K^0$ contient un $\mathbf{A}_k$-voisinage de α dans I_K^0 comme on voulait.

□

Preuve du théorème 6.14 : D'après les lemmes 6.15 et 6.16, il suffit de trouver un ensemble $\mathbf{A}_K$-compact $W \subset \mathbf{A}_K$ tel que le passage au quotient $W \cap I_K^0 \to I_K^0/K^*$ soit surjectif. Choisissons un idèle $\alpha = (\alpha_v)$ tel que $|\alpha| := \prod_v \alpha_v$ soit $> C$, où C est la constante donnée par le lemme 6.8. On choisit alors pour W le compact (comme produit de compacts) de $\mathbf{A}_k$ défini par $|\xi_v|_v \leq |\alpha_v|_v$ pour toute place v. Le lemme 6.8 dit alors que si $\beta = (\beta_v)$ est dans I_K^0, alors on a un $\eta \in K^*$ tel que $|\eta|_v \leq |\beta_v^{-1}\alpha_v|_v$ pour toute place v, i.e. $\eta\beta \in W$ comme on voulait.

□

6.4. Idèles et idéaux

Soit K un corps de nombres. Le groupe multiplicatif des idéaux fractonnaires $I(\mathcal{O}_K)$ est isomorphe au groupe $\mathcal{I}_K$ des sommes formelles presque nulles $\sum_{v \in \Omega_f} n_v v$ avec $n_v \in \mathbf{Z}$ (qui, dans le langage de la géométrie algébrique, est le groupe des *diviseurs* $\mathrm{Div}\,(\mathrm{Spec}\,\mathcal{O}_K)$). Les idéaux maximaux

de $\mathcal{O}_K$ (au sens usuel) correspondent aux sommes formelles presque nulles $\sum_v n_v.v$ avec $n_v \geq 0$ (les *diviseurs effectifs*).

Theorème 6.17 *Le groupe des classes d'idéaux* $\mathrm{Cl}(\mathcal{O}_K)$ *est fini.*

Démonstration : Le morphisme de groupes

$$I_K \to \mathcal{I}_K, \quad (\alpha_v) \mapsto \sum_{v \in \Omega_f} v(\alpha_v) v$$

est continue ($\mathcal{I}_K$ étant muni de la topologie discrète) par définition de la topologie de I_K. Par ailleurs l'image de K^* est par définition le groupe des idéaux principaux $\mathcal{P}_K$, et le quotient $\mathcal{I}_K/\mathcal{P}_K$ est isomorphe au groupe $\mathrm{Cl}(\mathcal{O}_K)$. On obtient une surjection (parce qu'il y a au moins une place archimédienne dans K) continue $I_K^0/K^* \to \mathrm{Cl}(\mathcal{O}_K)$. Comme un compact discret est fini, le théorème 6.14 donne alors le résultat.

□

Remarque 6.18 On a un résultat analogue (avec la même preuve) si K est un corps de fonctions, avec une légère modification. Soit X une courbe projective lisse sur un corps fini $\mathbf{F}_q$, de corps de fonctions K. C'est maintenant le groupe $\mathcal{I}_K^0/\mathcal{P}_K$ qui est fini, où $\mathcal{I}_K^0$ est le groupe des diviseurs de degré zéro sur X et $\mathcal{P}_K$ le groupe des diviseurs principaux. Ici le groupe des diviseurs $\mathcal{I}_K$ est composé des sommes formelles presque nulles $\sum_{v \in \Omega_K} n_v v$ avec $v \in \mathbf{Z}$, et le degré d'un tel diviseur est $\sum_v n_v d_v$, où d_v est le degré sur $\mathbf{F}_q$ du corps résiduel de X en v.

En particulier si on enlève un point fermé v_0 de X, l'anneau de Dedekind des fonctions régulières de la courbe affine $Y = X \setminus \{v_0\}$ a un groupe des classes d'idéaux fini (en effet si on note d le degré du point fermé v_0, les diviseurs de Y dont le degré est dans $d\mathbf{Z}$ forment un sous-groupe d'indice fini de $\mathrm{Div}\, Y$, et ce sous-groupe est isomorphe à $\mathrm{Div}^{\,0} X$)

6.5. Le théorème des unités de Dirichlet

Dans ce paragraphe, on va voir une autre conséquence classique du théorème 6.14. On considère un ensemble fini non vide S de places d'un corps global K, contenant toutes les places archimédiennes si K est un corps de nombres.

Définition 6.19 L'*anneau des S-entiers* $\mathcal{O}_{K,S}$ de K est le sous-anneau de K constitué des $x \in K$ vérifiant $|x|_v \leq 1$ (i.e. $x \in \mathcal{O}_v$) pour toute place $v \notin S$.

Le *groupe des S-unités* de K est le groupe des inversibles $E_{K,S} := \mathcal{O}_{K,S}^*$ de $\mathcal{O}_{K,S}$. Le *groupe des S-idèles* $I_{K,S}$ est le sous-groupe de I_K constitué des (x_v) tels que $|x_v|_v = 1$ pour toute place v non dans S.

Autrement dit, $E_{K,S}$ consiste en les $a \in K^*$ vérifiant $|a|_v = 1$ pour toute place v non dans S, et on a une définition analogue pour $I_{K,S}$.

Theorème 6.20 (Dirichlet) *Le groupe des S-unités $E_{K,S}$ est isomorphe au produit direct d'un groupe fini (les racines de l'unité de K^*) et de $\mathbf{Z}^{s-1}$, où s est le cardinal de S.*

Le théorème découle immédiatement du lemme suivant :

Lemme 6.21 *Soit V le $\mathbf{R}$-espace vectoriel des applications de S dans $\mathbf{R}$. Soit $\lambda : E_{K,S} \to V$ l'homomorphisme défini par $\lambda(a) = f_a$, où $f_a(v) = \log |a|_v$ pour toute $v \in S$. Alors λ a un noyau fini, et son image est un réseau engendrant le $\mathbf{R}$-espace vectoriel V^0 des $f \in V$ telles que $\sum_{v \in S} f(v) = 0$.*

Démonstration : On observe d'abord que si c et C sont des constantes avec $0 < c < C$, alors l'ensemble des S-unités η telles que

$$\forall v \in S, \quad c \leq |\eta|_v \leq C$$

est fini comme intersection d'un compact de I_K avec le sous-groupe discret (cf. proposition 6.13) K^*. En particulier les éléments x vérifiant $|x|_v = 1$ pour toute place v sont en nombre fini et forment un groupe multiplicatif, c'est donc exactement le groupe des racines de l'unité de K^*. Ceci montre que $\ker \lambda$ est fini.

Pour obtenir l'assertion sur son image, on observe qu'on peut définir λ par la formule analogue sur les S-idèles $I_{K,S}$, et l'image de $I_S^0 := I_{K,S} \cap I_K^0$ engendre [5] le $\mathbf{R}$-espace vectoriel V^0, qui est de dimension $s-1$. Le groupe $\lambda(E_{K,S})$ est discret : en effet il n'y a qu'un nombre fini de $\eta \in E_{K,S}$ avec $1/2 \leq |\eta|_v \leq 2$ pour toute place v de S, ce qui implique que 0 est un point isolé de $\lambda(E_{K,S})$. De plus, $\lambda(I_S^0)/\lambda(E_{k,S})$ est compact via la compacité de $I_S^0/E_{K,S}$ qui résulte du théorème 6.14 (noter que $I_S^0/E_{K,S}$ est un sous-groupe ouvert, donc fermé de I_K^0/K^*). Finalement $\lambda(E_{K,S})$ est un réseau qui engendre le $\mathbf{R}$-espace vectoriel V^0.

□

5. et même lui est égal si k est un corps de nombres et S est l'ensemble des places archimédiennes.

Références

[1] N. Bourbaki : *Algèbre*, chapitre V.

[2] N. Bourbaki : *Topologie générale*, chapitre III.

[3] H. Matsumura :*Commutative Algebra*.

[4] , J. S. Milne : *Étale cohomology*.

[5] J-P. Serre : *Corps locaux*.