Théorie du corps de classes local

encadré par Xavier Caruso

Tristan Vaccon

août-septembre 2011

Table des matières

Introduction

L'objectif de ce texte est la démonstration du théorème de classification des extensions abéliennes des corps locaux par la correspondance avec les corps de classes, et d'en déduire le théorème de Kronecker-Weber, qui énonce que toute extension abélienne finie de $\mathbb{Q}$ est contenue dans une extension cyclotomique. Cette démonstration prendra le chemin des théories du corps de classes générale et locale, tout en commençant à partir de la construction de $\mathbb{Q}_p$. On s'efforcera d'être le plus direct sur ce chemin, hormis quelques petits à-côtés : quelques mots sur les polygones de Newton, sur la structure des extensions d'un corps local, ou sur la théorie du corps de classes générale infinie. Certaines connaissances de base en théorie de Galois et en théorie algébrique des nombres seront supposées connues.

Dans notre texte, les deux premières parties sont essentiellement inspirées d'un cours de M2 de Pierre Colmez [4]. Néanmoins, certains éléments sont inspirés du livre de Neukirch [1] (en particulier sur les groupes profinis), et le paragraphe sur les polygones de Newton utilise aussi le livre de Robert [5], ainsi qu'un texte de la préparation à l'agrégation de l'université de Rennes 1 [9] (pour le côté effectif). Les trois parties suivantes sont, elles, très fortement inspirées du premier livre de Neukirch [1], avec parfois quelques incursions dans son second livre étudié ici [3], qui contient intégralement le premier, à quelques reformulations près. Pour les considérations sur les bases de la théories de Galois, on peut consulter les livres de Gozard [6] et, plus généralement, de Lang [7].

1 Présentation du contexte

Dans cette première partie, nous allons construire les objets de bases sur lesquels portent la théorie du corps de classes local : valuations, corps locaux, en particulier $\mathbb{Q}_p$ et certaines de ses extensions, avec un petit détour par les polygones de Newton.

1.1 Constructions de $\mathbb{Q}_p$, groupes profinis

Le premier objet qu'il convient de définir est $\mathbb{Q}_p$: nous en donnerons plusieurs construction au cours de ce texte, en particulier ici une en tant que complété de $\mathbb{Q}$, puis en tant que groupe profini.

1.1.1 Corps normés

Ici, nous allons étudier les corps muni d'une norme de corps, et notamment voir que l'on connaît toutes celles sur $\mathbb{Q}$, ce qui permettra de définir une première fois $\mathbb{Q}_p$.

Définition 1.1.1. Soit K un corps. On appelle norme sur K une application $|\cdot| : K \to \mathbb{R}_+, x \mapsto |x|$ telle que :

$$(i)\ |x| = 0 \Leftrightarrow x = 0;$$
$$(ii)\ |xy| = |x||y|;$$
$$(iii)\ |x + y| \leqslant |x| + |y|.$$

Elle est de plus dite *ultramétrique* si on a la condition (iii') plus restrictive que (iii) :

$$(iii')\ |x + y| \leqslant \sup(|x|, |y|).$$

Proposition 1.1.2. *Si K est un corps et $||$ une norme sur K, alors les conditions suivantes sont équivalentes :*

(i) $||$ est ultramétrique ;

(ii) $||$ est bornée sur $\phi(\mathbb{Z})$ (avec $\phi : \mathbb{Z} \to K$, $1 \mapsto 1$, pour limiter un peu les abus de notations) ;

(iii) $\forall x \in \mathbb{Z}$, $|\phi(x)| \leqslant 1$

Démonstration. Avec $|1| = 1$, on a directement $(i) \Rightarrow (iii) \Rightarrow (ii)$. Montrons $(ii) \Rightarrow (i)$. Soit $M \in \mathbb{R}_+^*$ tel que : $\forall x \in \mathbb{Z}$, $|\phi(x)| \leqslant M$. Soit $x, y \in K$, $n \in \mathbb{N}^*$, alors :

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

En passant à la racine n-ème, on obtient $|x+y| \leqslant (M(n+1))^{\frac{1}{n}} \sup(|x|, |y|)$, ce qui donne bien l'inégalité voulue en passant à la limite. □

Corollaire 1.1.3. *Toute norme sur un corps de caractéristique $p \neq 0$ est ultramétrique.*

On peut naturellement définir une distance sur un corps muni d'une norme $(d(x, y) = |x - y|)$, nous allons voir quelques rapides aspects topologiques dans le cas où la norme est ultramétrique.

Lemme 1.1.4. *Si $||$ est une norme ultramétrique sur le corps K, et $x, y \in K$ tels que $|x| \neq |y|$, alors $|x + y| = \sup(|x|, |y|)$.*

Démonstration. On peut supposer, quitte à permuter, que $|x| > |y|$. Alors,

$$|x + y| \leqslant \sup(|x|, |y|) = |x| = |(x + y) - y| \leqslant \sup(|x + y|, |y|).$$

Or on a $|y| < |x|$, et $|x + y| \leqslant |x| \leqslant \sup(|x + y|, |y|)$, donc nécessairement, $\sup(|y|, |x + y|) \leqslant |x| \leqslant \sup(|y|, |x + y|)$ et $|x| = \sup(|x + y|, |y|) = |x + y|$, soit finalement $|x| = |x + y|$. □

Proposition 1.1.5. *Si $|\ |$ est une norme ultramétrique sur K, alors :*

(i) Tout triangle est isocèle ;

(ii) Tout point d'une boule en est "le centre" (i.e. si $B = B(x_0, r)$ avec $x_0 \in K$, $r \in \mathbb{R}_+^*$, si $x \in B$, alors $B = B(x, r)$, ouverte ou fermée) ;

(iii) Deux boules sont soit disjointes, soit l'une est contenue dans l'autre ;

(iv) Les boules sont à la fois ouvertes et fermées ;

(v) La topologie est totalement discontinue, i.e. les composantes connexes de K sont les singletons.

Démonstration. Pour le (i), si $x, y, z \in K$, alors on a avec le lemme : si $|x - y| \neq |x - z|$, alors $|y - z| = \sup(|x - y|, |y - z|)$, ce qui permet de conclure.

Pour le deuxième point, si $x_1 \in B(x_0, r)$, $r \in \mathbb{R}_+^*$ (boule ouverte ou fermée), alors si $y \in B(x_1, r)$, on a $d(x_0, y) \leqslant \sup(d(x_0, x_1), d(x_1, y)) \leqslant r$ (ou $< r$ pour le cas de boules ouvertes), donc $B(x_1, r) \subset B(x_0, r)$. Comme, par définition, on a aussi $x_0 \in B(x_1, r)$, on en déduit l'égalité $B(x_1, r) = B(x_0, r)$, ce que l'on souhaitait démontrer.

Maintenant, si deux boules B_1 et B_2 ne sont pas disjointes, si $x \in B_1 \cap B_2$, alors $B_1 = B(x, r_1)$ et $B_2 = B(x, r_2)$ pour un certain r_1 et un certain r_2, d'après (ii), ce qui donne le résultat.

Si B est une boule ouverte de rayon $r \in \mathbb{R}_+^*$, alors avec (ii) et (iii), si $x \in B^c$ (notation pour le complémentaire de B), alors $B(x, r) \subset B^c$, et donc B^c est ouvert, donc B est fermée. Inversement, si B est une boule fermée de rayon $r \in \mathbb{R}_+^*$, le (ii) donne directement que B est un voisinage de chacun de ses points, ce qui donne bien le fait que B est ouverte.

Le dernier point se déduit du précédent : deux points distincts x et y ne peuvent pas être dans la même composante connexe C, puisqu'on peut les séparer par deux boules, $B = B(x, \frac{1}{2}|x-y|)$ et $B(x, \frac{1}{2}|x-y|)$, et alors B et B^c étant à la fois ouverts et fermés, $C \cap B$ et $C \cap B^c$ sont tout deux, disons, fermés, non triviaux, et C n'est pas connexe. □

Définition 1.1.6. Deux normes sur un corps K sont dites équivalentes si elles définissent la même topologie.

Il se trouve que l'on peut caractériser les normes qui sont équivalentes :

Proposition 1.1.7. *Deux normes $||_1$ et $||_2$ sur K sont équivalentes si et seulement si il existe $s \in \mathbb{R}_+^*$ tel que $|\ |_1 = |\ |_2^s$.*

Démonstration. Si $|\ |_1 = |\ |_2^s$, alors les deux normes définissent les même boules (les boules de l'une sont des boules de l'autre (pas de même rayon !)) donc la même topologie, et elles sont donc bien équivalentes. Réciproquement, on remarque que si $|\ |$ est une norme sur K, alors $|x| < 1$ si et seulement si la suite $(x^n)_{n\in\mathbb{N}}$ tend vers 0. Ainsi, si $||_1$ et $||_2$ sont équivalentes, par définition, la suite $(x^n)_{n\in\mathbb{N}}$ converge pour

l'une si et seulement si elle converge pour l'autre. On a donc $\{x \in K / |x|_1 < 1\} = \{x \in K / |x|_2 < 1\}$. Si cet ensemble est réduit à $\{0\}$, alors pour tout $x \in K^*$, on a $|x|_1 = |x|_2 = 1$ (comme $|x||x^{-1}| = 1$), et les deux normes sont bien équivalentes. Sinon, soit $x \in K^*$ tel que $|x|_1 < 1$. Si $y \in K^*$, $a \in \mathbb{Z}$ et $b \in \mathbb{N}$, alors :

$$|y^b x^{-a}|_1 < 1 \Leftrightarrow |y^b x^{-a}|_2 < 1.$$

Ainsi, en passant au log,

$$\left\{ r \in \mathbb{Q} / r < \frac{\log |y|_1}{\log |x|_1} \right\} = \left\{ r \in \mathbb{Q} / r < \frac{\log |y|_2}{\log |x|_2} \right\}$$

Ces deux ensembles étant égaux, leur sup dans $\mathbb{R}$ sont égaux, donc $\frac{\log |y|_1}{\log |x|_1} = \frac{\log |y|_2}{\log |x|_2}$, et enfin $\frac{\log |y|_1}{\log |y|_2} = \frac{\log |x|_1}{\log |x|_2}$, ce qui permet de conclure. □

Exemple. On peut munir tout corps de la norme triviale : $|x| = 1$ si $x \neq 0$. Correspondant à la topologie discrète sur K, elle est ultramétrique.

Exemple. La norme usuelle sur $\mathbb{C}$ est une norme de corps.

Exemple. Si L est un corps normé, et K un sous-corps de L, L est naturellement un corps normé pour la norme restriction de la norme sur L.

Nous allons voir qu'on connaît, à équivalence près, toutes les normes sur le corps $\mathbb{Q}$.

Définition 1.1.8. Si $n \in \mathbb{Z}$, on définit la valuation p-adique de n par $v_p(n) = \sup \left\{ k \in \mathbb{N} / p^k | n \right\}$ (on a $v_p(n) \in \mathbb{N} \cup \{+\infty\}$). Si $r = \frac{a}{b} \in \mathbb{Q}$, on définit la valuation p-adique de r par $v_p(r) = v_p(a) - v_p(b)$ (elle ne dépend pas du choix du numérateur et du dénominateur).

Proposition 1.1.9. $|\ |_p : \mathbb{Q} \to \mathbb{R}$, $x \mapsto p^{-v_p(x)}$ *définit une norme sur* $\mathbb{Q}$*, appelée norme p-adique. Cette norme est ultramétrique.*

Démonstration. Tout est conséquence directe de la décomposition en facteur premier des entiers. □

Théorème 1.1.10 (Ostrowski)**.** *Une norme sur* $\mathbb{Q}$ *est équivalente soit à la norme triviale, soit à la norme usuelle* $|\ |_\infty$*, soit à une norme p-adique pour un nombre premier p donné.*

Démonstration. Soit $|\ |$ une norme non triviale. Supposons qu'il existe $k \in \mathbb{N}$ tel que $|k| > 1$. Comme $|1| = 1$, on a, par inégalité triangulaire, $|k| \leqslant k$, et donc il existe $\alpha \in]0, 1]$ tel que $|k| = k^\alpha$. Soit $m \in \mathbb{N}$, m peut s'écrire en base k :

$m = \sum_{i=0}^{n} a_i k^i$, avec $a_i \in \{0, \dots, k-1\}$ et $a_n \neq 0$. On a en particulier $k^n \leqslant m$. Comme $|a_i| \leqslant a_i \leqslant k-1$ et $|k^i| = |k|^i$, on en déduit :

$$|m| \leqslant (k-1) \sum_{i=1}^{n} k^{i\alpha} = \frac{k-1}{k^\alpha - 1}(k^{(n+1)\alpha} - 1) \leqslant \frac{k^\alpha (k-1)}{k^\alpha - 1} k^{n\alpha} \leqslant C m^\alpha,$$

où $C = \frac{k^\alpha(k-1)}{k^\alpha - 1} > 0$ est une constante qui ne dépend pas de m.

Appliquons cette inégalité à m^l, on a $|m|^l \leqslant C m^{l\alpha}$. Si on prend la racine l-ème et qu'on passe à la limite $l \to +\infty$, on obtient $|m| \leqslant m^\alpha$. Au final, $\frac{\log|m|}{\log m} \leqslant \frac{\log|k|}{\log k}$. Si on suppose que $|m| > 1$, alors par symétrie, on obtient $\frac{\log|m|}{\log m} = \frac{\log|k|}{\log k}$. Sinon, il existe $l \in \mathbb{N}$ tel que $|k^l m| > 1$, et en appliquant ce qui précéde à $k^l m$, on obtient la même égalité pour tout $m \in \mathbb{N}$. Par multiplicativité de la norme, on $|-1| = 1$, et on peut en déduire directement que $|x| = |x|_\infty^\alpha$ pour tout $x \in \mathbb{Q}$. Ainsi, s'il existe $k \in \mathbb{N}$ tel que $|k| > 1$, $|\ |$ est équivalente à la norme usuelle.

Maintenant, si $\forall l \in \mathbb{N}, |l| \leqslant 1$, c'est en particulier vrai pour tout nombre premier p. Par décomposition en facteurs premier de tout entier, la norme étant supposée non triviale on en déduit que nécessairement, il existe p premier tel que $|p| < 1$. S'il existe un autre entier premier q tel que $|q| < 1$, alors par le théorème de Bézout, pour tout $n \in \mathbb{N}^*$, il existe $u_n, v_n \in \mathbb{Z}$ tel que $u_n p^n + v_n q^n = 1$. On a alors pour tout n :

$$1 = |1| = |u_n p^n + v_n q^n| \leqslant |u_n||p|^n + |v_n||q|^n \leqslant |p|^n + |q|^n,$$

ce qui est absurde avec $|p| < 1$ et $|q| < 1$. On a donc un seul nombre premier, p, tel que $|p| < 1$, et tout les autres sont de norme 1. On en déduit alors que si $x \in \mathbb{Q}$, $x = p^l \frac{a}{b}$ avec $l \in \mathbb{Z}$, $a \wedge p = b \wedge p = 1$, alors par multiplicativité de la norme, on a $|x| = |p|^l$, ce qui montre directement que $|\ |$ est équivalente à la norme p-adique, et clôt la démonstration. □

La formule suivante permet de comprendre pourquoi on a normalisé la norme p-adique avec $|p| = \frac{1}{p}$ (alors que $|p|$ valant n'importe réel de $]0, 1[$ définirait une norme équivalente).

Théorème 1.1.11 (Formule du produit)**.** *Soit $x \in \mathbb{Q}^*$, alors :*

$$|x|_\infty \times \prod_{p \text{ premier}} |x|_p = 1$$

Démonstration. Il suffit d'écrire la décomposition de $x \in \mathbb{Z}^*$ en facteurs premiers. On notera que le produit infini a presque tout ses termes égaux à un. □

1.1.2 Complétion

Définition 1.1.12. Si K est un corps normé, on notera (dans cette première partie seulement) $\tilde{K}$ l'ensemble des suites de Cauchy à valeurs dans K, soit l'ensemble :

$$\{(a_n)_{n\in\mathbb{N}} / \forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geqslant N, \forall p \in \mathbb{N}, |a_{n+p} - a_n| < \varepsilon\}.$$

On notera $I \subset \tilde{K}$ l'ensemble des suites à valeur dans K qui convergent vers 0.

Nous allons montrer que I est un idéal maximal de $\tilde{K}$, qui est un anneau, et que $\tilde{K}/I$ est le complété de K.

Lemme 1.1.13. *(i) Si $(a_n)_{n\in\mathbb{N}} \in \tilde{K}$, alors la suite $(|a_n|)_{n\in\mathbb{N}}$ converge dans $\mathbb{R}_+$;*
(ii) Si de plus, $|\ |$ est une norme ultramétrique et $(a_n)_{n\in\mathbb{N}} \notin I$, alors la suite $(|a_n|)_{n\in\mathbb{N}}$ est constante à partir d'un certain rang ;
(iii) Si $a = (a_n)_{n\in\mathbb{N}}$ et $b = (b_n)_{n\in\mathbb{N}}$ sont dans $\tilde{K}$ et différent d'un élément de I, alors $\lim_{n\to+\infty} |a_n| = \lim_{n\to+\infty} |b_n|$.

Démonstration. Pour le premier point, l'inégalité triangulaire donne $||a_{n+p}|-|a_n|| \leqslant |a_{n+p} - a_n|$ quels que soient n et p, ce qui montre directement le fait que $(|a_n|)$ est de Cauchy si (a_n) l'est, $\mathbb{R}_+$ étant complet.

Concernant le deuxième point, si $a = (a_n)_{n\in\mathbb{N}} \in \tilde{K} \setminus I$, alors il existe $\delta > 0$ et $N \in \mathbb{N}$ tels que si $n \geqslant N$ et $p \in \mathbb{N}$, on a $|a_n| > \frac{2}{3}\delta$ et $|a_{n+p} - a_n| < \frac{\delta}{2}$. On a alors $|a_{n+p} - a_n| < |a_n|$, et comme $|\ |$ est ultramétrique, alors $|a_{n+p}| = |a_n|$ (sinon, $|a_{n+p} - a_n| = \sup(|a_n|, |a_p|)$, ce qui est absurde), ce qu'on souhaitait démontrer.

Enfin, pour le dernier point, $||a_n| - |b_n||| \leqslant |a_n - b_n|$ et l'hypothèse énonce que $a_n - b_n$ tend vers 0, d'où le résultat. □

Lemme 1.1.14. *$\tilde{K}$ est un anneau et I en est un idéal maximal.*

Démonstration. Pour voir que $\tilde{K}$ est un anneau, la seule chose non immédiate est le fait que le produit de deux suites de Cauchy reste de Cauchy. On peut le montrer en écrivant $|a_{n+p}b_{n+p} - a_nb_n| = |a_{n+p}(b_{n+p} - b_n) + b_n(a_{n+p} - a_n)|$, puis en utilisant l'inégalité triangulaire et le fait qu'une suite de Cauchy est bornée. L'élément unité est bien sûr la suite constante égale à 1. Le fait que I soit un idéal est aussi immédiat, par les mêmes manipulations.

Si $a = (a_n)_{n\in\mathbb{N}} \in \tilde{K} \setminus I$, avec le lemme précédent, $(|a_n|)_n$ converge, mais pas vers 0 vu la définition de (a_n). Il existe alors $\delta > 0$ et $N \in \mathbb{N}$ tel que si $n \geqslant N$, $|a_n| > \delta > 0$. Mais alors, en posant $b_n = 0$ pour $n \leqslant N$ et $b_n = a_n^{-1}$ pour $n > N$, on obtient une suite de Cauchy. En effet, $a_{n+p}^{-1} - a_n^{-1} = \frac{1}{a_n a_{n+p}}(a_n - a_{n+p})$, donc $|a_{n+p}^{-1} - a_n^{-1}| \leqslant \frac{1}{\delta^2}|a_n - a_{n+p}|$. Ainsi, on a bien $(b_n) \in \tilde{K}$, et même $(a_nb_n - 1) \in I$, ce qui montre que $a \in \tilde{K} \setminus I$ est inversible dans $\tilde{K}/I$, et donc I est bien un idéal maximal. □

Ainsi, $\widehat{K} = \tilde{K}/I$ est un corps, et avec le (*iii*) du lemme 1.1.13 , $|\ |$ s'étend bien à $\widehat{K}$, en prenant pour $|a|$, avec $a = (a_n)_{n\in\mathbb{N}}$, la limite de $|a_n|$.

Proposition 1.1.15. *$|\ |$ est une norme sur $\widehat{K}$ (qui reste ultramétrique si elle l'est sur K) et $\widehat{K}$ est complet pour cette norme, et contient K (identifiés aux classes des suites constantes) comme sous-corps dense.*

Démonstration. La multiplicativité de la norme et l'inégalité triangulaire (et éventuellement ultramétrique) passent bien à la limite. D'autre part, $|a| = 0$ dans $\widehat{K}$ si et seulement si $a = (a_n)_{n\in\mathbb{N}}$ et $|a_n| \to 0$, soit si et seulement si $a \in I$, et $|\ |$ étendue à $\widehat{K}$ en fait bien un corps normé.

Pour ce qui est de la densité, si $a = (a_n)_{n\in\mathbb{N}} \in \tilde{K}$, alors (dans $\tilde{K}$) $|a - a_n| \leqslant \sup_{p\in\mathbb{N}^*} |a_{n+p} - a_n|$, et donc tend vers 0 comme (a_n) est de Cauchy. Alors, dans $\widehat{K}$, on a $a = \lim_{n\to+\infty} a_n$, et K est bien dense dans $\widehat{K}$.

Enfin, si $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy de $\widehat{K}$, alors comme on vient de voir que K est dense dans $\widehat{K}$, on peut trouver $b_n \in K$ tel que $|a_n - b_n| \leqslant 2^{-n}$, et alors b_n est de Cauchy dans K, donc converge dans $\widehat{K}$ par définition de $\tilde{K}$ et $\widehat{K}$. Sa limite est alors aussi celle de $(a_n)_{n\in\mathbb{N}}$ et on a bien le résultat sur la complétude. □

Définition 1.1.16. Le corps $\widehat{K}$, muni de la norme $|\ |$, est le *complété* de K pour la norme $|\ |$.

Exemple. $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour la norme $|\ |_\infty$ (mais la construction précédente ne founit pas une construction de $\mathbb{R}$, car elle utilise le fait que $\mathbb{R}$ soit complet, dans le premier lemme).

Exemple. Le complété de $K(X)$ pour la norme $|\ |_X$ (définie par val_X de même que les $|\ |_p$ pour $\mathbb{Q}$) est $K((X))$, corps des séries de Laurent à coefficient dans K.

Définition 1.1.17. On note $\mathbb{Q}_p$, corps des nombres p-adiques, le complété de $\mathbb{Q}$ pour la norme $|\ |_p$.

Remarque. D'une manière similaire, on peut compléter l'anneau $\mathbb{Z}$ muni $|\ |_p$ pour obtenir $\mathbb{Z}_p$, l'anneau des entiers p-adiques. On peut alors vérifier que $\mathbb{Q}_p = Frac(\mathbb{Z}_p)$. L'intérêt de ce point de vue se situe dans le fait que, de manière similaire à la construction des séries formelles par rapport aux polynômes, si on écrit les éléments de $\mathbb{Z}$ en base p, *i.e.* si $x \in \mathbb{Z}$, alors $x = \sum_{i=0}^{k_x} a_i p^i$ où $a_i \in \{0, \cdots, p-1\}$, on a une écriture pour les éléments de $\mathbb{Z}_p$, si $x \in \mathbb{Z}_p$, alors $x = \sum_{i=0}^{+\infty} a_i p^i$ où $a_i \in \{0, \cdots, p-1\}$. Ainsi, si $x \in \mathbb{Q}_p$, on peut écrire $x = \sum_{i=-k_x}^{+\infty} a_i p^i$ où $a_i \in \{0, \cdots, p-1\}$, et $k_x \in \mathbb{N}$.

1.1.3 Groupes profinis

Nous allons voir une deuxième construction, classique, de $\mathbb{Q}_p$ à partir de groupes profinis. Ces derniers réapparaitront un peu plus loin, et de manière cruciale, dans la définition du groupe de Galois $G(\overline{\mathbb{Q}}|\mathbb{Q})$.

Définition 1.1.18. Un *groupe profini* est un groupe topologique G qui est compact (et séparé) et a une base de voisinages ouverts de 1 constitués de sous-groupes distingués.

Nous allons voir que les groupes profinis sont exactement les limites projectives de groupes finis.

Définition 1.1.19. Un *ensemble dirigé* est un ensemble ordonné I tel que $\forall i, i' \in I, \exists i'' \in I, i, i' \leqslant i''$

Un *système projectif* d'ensembles (de groupes, anneaux...) sur un ensemble dirigé I est une famille

$$\{G_i, f_{i,j} \diagup i, j \in I, i \leqslant j\}$$

d'ensembles G_i et d'applications (de morphismes de groupes, d'anneaux...) $f_{i,j} : G_j \to G_i$ telles que, si $i \leqslant j \leqslant k$,

$$f_{i,k} = f_{i,j} \circ f_{j,k}.$$

On définit alors la *limite projective* $G = \lim_{\leftarrow} G_i$ de ce système projectif comme l'ensemble (groupe, anneau, ...) :

$$G = \left\{ \prod_{i \in I} \sigma_i \in \prod_{i \in I} G_i \diagup f_{i,j}(\sigma_j) = \sigma_i, \text{ si } i \leqslant j \right\}.$$

Si les G_i sont des espaces topologiques et que les $f_{i,j}$ sont des applications continues, alors G est un fermé de l'espace topologique produit $\prod_{i \in I} G_i$.

Proposition 1.1.20. *Si G est un groupe profini, et si N parcours les sous-groupes distingués ouverts de G, alors (comme ensemble et comme groupe topologique) :*

$$G \cong \lim_{\leftarrow} G/N.$$

Réciproquement, si $\{G_i, f_{i,j}\}$ est un système projectif de groupes finis G_i, alors

$$G = \lim_{\leftarrow} G_i$$

est un groupe profini.

Démonstration. Soit G un groupe profini, et soit $\{N_i,\ i \in I\}$ la famille des sous-groupes distingués ouverts de G. Comme G est compact, chaque N_i ne donne lieu qu'à un nombre fini de classe d'équivalence gN_i modulo N_i, comme l'ensemble des gN_i pour $g \in G$ forme un recouvrement ouvert de G. Ainsi, $G_i = G/N_i$ est un groupe fini. On écrira $i \leqslant j$ si $N_i \supset N_j$, et $f_{i,j} : G_j \to G_i$ pour les projections canoniques. Alors $\{G_i, f_{i,j}\}$ est un système projectif de groupes finis, et on va montrer que :

$$f : G \to \lim_{\leftarrow} G_i,\ \ \sigma \mapsto \prod_{i \in I} \sigma_i,\ \ \sigma_i = \sigma \mod N_i,$$

est un isomorphisme et un homéomorphisme.

f est injective car le noyau de f est l'intersection $\bigcap_{i \in I} N_i$ qui vaut $\{1\}$ car G est séparé. Les groupes $U_S = \prod_{i \notin S} G_i \times \prod_{i \in S} \{1_{G_i}\}$, avec S parcourant les sous-ensembles finis de I, forment une base de voisinages ouverts de 1 dans $\prod_{i \in I} G_i$. Comme $f^{-1}(U_S \cap \lim_{\leftarrow} G_i) = \cap_{i \in S} N_i$ qui est ouvert (S fini), f est continue. Comme G est compact, son image par f est fermée dans $\lim_{\leftarrow} G_i$. Par ailleurs, cette image est dense. En effet, si $\overline{\sigma} = \prod_{i \in I} \sigma_i \in \lim_{\leftarrow} G_i$ et $\overline{\sigma}(U_S \cap \lim_{\leftarrow} G_i)$ est une base de voisinages ouverts de $\overline{\sigma}$, alors on peut choisir $\sigma \in G$ tel que son image par $G \to G/N_k$, avec $N_k = \prod_{i \in S} N_i$ est envoyée sur σ_k, de telle manière que $\sigma \mod N_i = \sigma$ pour tout $i \in S$, c'est à dire $f(\sigma) \in \overline{\sigma}(U_S \cap \lim_{\leftarrow} G_i)$. Ainsi, $f(G)$ est dense dans $\lim_{\leftarrow} G_i$ et donc $f(G) = \lim_{\leftarrow} G_i$.

Comme G est compact, f est une application fermée, donc ouverte. Finalement f est un isomorphisme et un homéomorphisme.

Réciproquement, si $\{G_i, f_{i,j}\}$ est un système projectif de groupes finis, en considérant les G_i comme munis de la topologie discrète, il sont compacts. Alors $G = \lim_{\leftarrow} G_i$ est un sous-groupe fermé du groupe compact (par le théorème de Tychonov) $\prod_{i \in I} G_i$, donc est un groupe compact. Les sous-groupes distingués $U_S \cap G$ où $U_S = \prod_{i \notin S} G_i \times \prod_{i \in S} H_i$, avec S un sous-ensemble fini de I, H_i un sous-groupe distingué de G_i, forment une base de voisinages ouverts de 1, et ainsi, G est un groupe profini. □

Remarque. On a vu au passage que si N est un sous-groupe ouvert de G, alors il est d'indice fini. Réciproquement, si un sous-groupe N est d'indice fini, il est clairement le complémentaire d'une union finie de fermés (les classes autres que celle de 0 modulo N), donc ouvert.

Maintenant, voici deux exemples fondamentaux de groupes profinis :

Exemple. Si p est un nombre premier, alors les anneaux $\mathbb{Z}/p^n\mathbb{Z}$ forment un système projectif avec pour $f_{i,j}$ les projections canoniques $\mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$, $i \leqslant j$. La limite projective $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ est l'anneau des entiers p-adiques $\mathbb{Z}_p$. En effet, à partir de l'écriture en base p (si $x \in \mathbb{Z}_p$, $x = \sum_{i=0}^{+\infty} a_i p^i$, $a_i \in \{0, \cdots, p-1\}$), on peut aisément imaginer un isomorphisme $\mathbb{Z}_p \to \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$.

Exemple. Les anneaux $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$ forment un système projectif, avec pour ordre celui donné par la relation de divisibilité, et pour $f_{i,j}$ les projections canoniques $\mathbb{Z}/j\mathbb{Z} \to \mathbb{Z}/i\mathbb{Z}$, $i|j$. La limite projective $\widehat{\mathbb{Z}} = \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z}$ est appelée le groupe de Prüfer, ou simplement "Z chapeau"...

Remarque. On montre que les $n\widehat{\mathbb{Z}}$ sont exactement les sous-groupes ouverts de $\widehat{\mathbb{Z}}$, et on montre alors que $\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}$, et par le théorème chinois, si $n = \prod_p p^{v_p(n)}$, on a $\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z} = \prod_p \mathbb{Z}/p^{v_p(n)}\mathbb{Z}$. En passant à la limite projective, on obtient $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$

Nous allons étudier un peu plus finement les propriétés de $\widehat{\mathbb{Z}}$:

Définition 1.1.21. On appelle *groupe procyclique* un groupe profini G, qui est topologiquement engendré par un élément $\sigma \in G$, c'est-à-dire que G est l'adhérence de $\langle\sigma\rangle = \{k\sigma,\ k \in \mathbb{Z}\}$.

Exemple. Deux cas particuliers de groupes procycliques sont $\mathbb{Z}_p$ et $\widehat{\mathbb{Z}}$, tout deux engendrés par leur élément 1.

Proposition 1.1.22. *Les sous-groupes ouverts d'un groupe procyclique G sont les nG, avec $n \in \mathbb{N}^*$.*

Démonstration. nG est fermé car c'est l'image du compact G par le morphisme continu $G \to G$, $\gamma \mapsto n\gamma$. De plus, G/nG est fini. En effet, si σ engendre topologiquement G, alors G/nG admet le groupe fini $\{k\sigma \mod nG / 0 \leqslant k < n\}$ comme sous-groupe dense. Or G/nG est compact, comme image de G par la surjection canonique, donc fermé, et ainsi, il coïncide avec la clôture de ce groupe fini, soit lui-même. Ainsi G/nG est fini, de cardinal au plus n. Réciproquement, si H est un sous-groupe ouvert de G, d'indice n, alors $nG \subset H \subset G$ et $n = (G : H) \leqslant (G : nG) \leqslant n$, et ainsi $H = nG$. □

En fait, $\widehat{\mathbb{Z}}$ est le prototype des groupes procycliques.

Proposition 1.1.23. *Tout groupe procyclique G est un quotient de $\widehat{\mathbb{Z}}$.*

Démonstration. Pour tout n, on a un homomorphisme surjectif :

$$\mathbb{Z}/n\mathbb{Z} \to G/nG,\ 1 \mod n\mathbb{Z} \mapsto \sigma \mod nG,$$

ainsi, en passant à la limite projective, on obtient une surjection $\widehat{\mathbb{Z}} \to G$, ce qui donne le résultat. □

Remarque. D'un autre côté, tout morphisme continu surjectif $G \to \widehat{\mathbb{Z}}$ doit être un isomorphisme, puisque pour tout n, il induit un isomorphisme $G/nG \to \mathbb{Z}/n\mathbb{Z}$ (surjectif, puis pour raisons de cardinalité).

1.2 Corps valués

Après avoir vu quelques comportements de corps munis d'une norme, nous pouvons préciser notre étude aux corps munis d'une valuation :

1.2.1 Corps valués et corps ultramétriques

Définition 1.2.1. Si K est un corps, une valuation v sur K est une application $K \to \mathbb{R} \cup \{+\infty\}$, $x \mapsto v(x)$, telle que :
(i) $v(x) = +\infty \Leftrightarrow x = 0$;
(ii) $v(xy) = v(x) + v(y)$;
(iii) $v(x+y) \geqslant \inf(v(x), v(y))$.

Valuations et normes sont étroitement liées dans le cas des normes ultramétriques :

Remarque. (i) Si K est un corps muni d'une norme ultramétrique $||$ et si $\lambda < 0$, alors : $K \to \mathbb{R} \cup \{+\infty\}$ définie par $v(x) = \lambda \log |x|$ est une valuation sur K.
(ii) Réciproquement, si v est une valuation sur K et $0 < a < 1$, alors $|x| = a^{v(x)}$ défini une norme ultramétrique sur K.
(iii) On peut alors en déduire : si $v(x) \neq v(y)$, alors $v(x+y) = \inf(v(x), v(y))$.

Définition 1.2.2. On dit que la valuation est *discrète* si $v(K^*)$ est un sous-groupe discret de $\mathbb{R}$ (*i.e.* de la forme $a\mathbb{Z}$), et qu'elle est normalisée si $v(K^*) = \mathbb{Z}$.

On a vu qu'il est équivalent de raisonner en termes de normes ultramétriques et en termes de valuations. On utilisera les deux visions par la suite.

Exemple. – La valuation p-adique v_p défini une valuation sur $\mathbb{Q}$, puis sur $\mathbb{Q}_p$ (et donc le nom "valuation" est bien cohérent avec ce qui précéde).
– La valuation en X, v_X défini une valuation sur $K(X)$, puis sur $K((X))$.

Remarque. – Si K est muni d'une valuation v, on a vu lors de la construction de $\widehat{K}$ que si $(a_n) \in \tilde{K}$, alors $v(a_n)$ constante à partir d'un certain rang. On en déduit que $v(K^*) = v(\widehat{K}^*)$.
– Une suite est de Cauchy si et seulement si $v(u_{n+1} - u_n)$ tend vers $+\infty$. Ainsi, si K est complet, une suite converge si et seulement si $v(u_{n+1} - u_n) \to +\infty$, et en particulier, une série converge dans K si et seulement si son terme général tend vers 0 (ou la valuation de son terme général tend vers $+\infty$).

On peut définir le corps résiduel d'un corps valué :

Proposition 1.2.3. *Si K est un corps muni d'une valuation v, alors $O_K = \{x \in K / v(x) \geqslant 0\}$ est un anneau local d'idéal maximal $m_K = \{x \in K / v(x) > 0\}$*

Démonstration. La définition d'une valuation donne directement le fait que O_K est un anneau et m_K un idéal. Reste à voir pourquoi il est maximal. Si $x \in O_K \setminus m_K$, alors $v(x) = 0$, et donc $v(x^{-1}) = 0$ et $x^{-1} \in O_K \setminus m_K$ ce qui permet de conclure sur la maximalité. En fait, on a même $O_K \setminus m_K = U(O_K)$, le groupe des unités de O_K. □

Définition 1.2.4. O_K est *l'anneau des entiers* de K, et le corps $k_K = O_K/m_K$ est *le corps résiduel* de K.

Exemple. L'anneau des entiers de $K((X))$ est $K[[X]]$, et son corps résiduel est K.

Exemple. L'anneau des entiers de $\mathbb{Q}_p$ est $\mathbb{Z}_p$, son idéal maximal est $p\mathbb{Z}_p$ et son corps résiduel est $\mathbb{Z}/p\mathbb{Z}$.

Cette dernière affirmation découle du lemme suivant :

Lemme 1.2.5. *L'application naturelle $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ est un isomorphisme.*

Démonstration. Soit $x \in \mathbb{Z} \cap p^n\mathbb{Z}_p$, on a $v_p(x) \geqslant n$ donc $x \in p^n\mathbb{Z}$. Cela donne l'injectivité.

Soit $x \in \mathbb{Z}_p$ et $\overline{x}$ son image modulo p^n. Comme $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$, il existe $r \in \mathbb{Q}$ tel que $v_p(x - r) \geqslant n$. On a alors $v_p(r) \geqslant 0$ (sinon, $n \leqslant v_p(x - r) = \inf(v_p(x), v_p(r)) = v_p(r)$ ce qui est absurde). On écrit $r = \frac{a}{b}$. Comme $v_p(a) \geqslant v_p(b)$ et quitte à diviser numérateur et dénominateur par $p^{v_p(b)}$, on peut supposer $b \wedge p = 1$. Soit $c \in \mathbb{Z}$ tel que $bc = 1 \mod p^n$. Alors $v_p(r - ac) = v_p(a\frac{1-bc}{b}) = v_p(a) + v_p(1 - bc)$. On a $v_p(a) \geqslant n$ et $v_p(1 - bc) \geqslant n$, donc au final :

$$v_p(x - ac) \geqslant \inf(v_p(x - r), v_p(r - ac)) \geqslant n,$$

et ac a pour image $\overline{x}$ dans $\mathbb{Z}_p/p^n\mathbb{Z}_p$ ce qui permet de conclure. □

1.2.2 Le lemme de Hensel

Les corps valués complets possèdent un analogue de la méthode de Newton réelle, le lemme de Hensel, qui nous donnera un puissant outil de démonstration d'existence de racines. Nous ne le verrons pas, mais il sert aussi, de manière effective, à "remonter" des factorisations.

Théorème 1.2.6 (Lemme de Hensel)**.** *Soit K un corps valué complet. Soit $f \in O_K[X]$. Soit $x \in O_K$. Supposons que $|f(x)| < |f'(x)|^2$. Alors il existe $\xi \in O_K$ tel que ξ est une racine de f et $|\xi - x| = |\frac{f(x)}{f'(x)}| < |f'(x)|$. Cette racine est la seule dans la boule ouverte $B(x, |f'(x)|)$.*

Démonstration. On définit $(x_n)_{n\in\mathbb{N}} \in O_K^{\mathbb{N}}$ par $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ et $x_0 = x$. On va montrer que la suite est bien définie, et qu'elle converge vers une racine de f.

On pose $c = -|\frac{f(x)}{f'(x)^2}| < 1$. Montrons par récurrence forte sur n que x_n est bien définie, $|f'(x_n)| = |f'(x)|$, $|x_n - x_{n-1}| \leqslant c^{2^{n-1}}|f'(x_0)|$, et $|f(x_n)| \leqslant c^{2^n}|f'(x_0)|^2$.

L'hypothèse nous donne $|f'(x_0)| > 0$ et donc x_1 est bien défini. On a alors $x_1 - x_0 = -\frac{f(x)}{f'(x)} = -\frac{f(x)}{f'(x)^2}f'(x)$. Donc $|x_1 - x_0| = c|f'(x_0)|$ (qu'on souhaitait montrer). De plus, on a $(x_1 - x_0)^2 = \left(\frac{f(x)}{f'(x)}\right)^2 = cf(x)$ donc $|x_1 - x_0|^2 = c|f(x)|$. La formule de Taylor pour les polynômes, à l'ordre 1 et pour f', nous donne :

$$f'(x_1) = f'(x_0) + (x_1 - x_0)s,$$

avec $s \in O_K$, donc $|s| \leqslant 1$. Ainsi,

$$|f'(x_1) - f'(x_0)| \leqslant |x_1 - x_0| = c|f'(x_0)| \leqslant |f'(x_0)|.$$

On en déduit que (norme ultramétrique) $|f'(x_1)| = |f'(x_0) + (f'(x_1) - f'(x_0))| = |f'(x_0)|$.

La formule de Taylor pour les polynômes, à l'ordre 2 et pour f, nous donne :

$$f(x_1) = f(x_0) + (x_1 - x_0)f'(x_0) + (x_1 - x_0)^2 r,$$

où $r \in O_K$. Par définition, $f(x_0) + (x_1 - x_0)f'(x_0) = 0$, donc

$$|f(x_1)| \leqslant |x_1 - x_0|^2 = c|f(x_0)|,$$

ce qui termine l'initialisation de la récurrence.

Pour ce qui est de l'hérédité, on remarque que si la suite est définie jusqu'au rang $n - 1 \geqslant 0$, alors d'après les hypothèses :

$$|\frac{f(x_{n-1})}{f'(x_{n-1})^2}| \leqslant c^{2^{n-1}}\frac{f'(x_0)^2}{f'(x_{n-1})^2} = c^{2^{n-1}} < 1.$$

On peut donc appliquer les calculs qui précédent avec x_{n-1} à la place de x_0. On obtiendra alors exactement la démonstration de l'hypothèse de récurrence au rang n.

On peut donc conclure la récurrence. Maintenant, on a :

– $$|f(x_n)| \leqslant c^{2^n}|f'(x_0)|^2$$
donc $f(x_n) \to 0$;

– $$|x_n - x_{n-1}| \leqslant c^{2^{n-1}}|f'(x_0)|$$
donc la suite (x_n) est de Cauchy dans K complet, elle converge alors dans K. Comme de plus, O_K est, par définition, un fermé de K, (x_n) converge dans O_K vers $\xi \in O_K$.

– On voit facilement que les polynômes définissent des fonctions continues. Comme f est un polynôme, il est continu, donc $f(\xi) = 0$.
– De plus, on remarque que, f' étant continu et $|f'(x_n)| = |f'(x)|$, on a $|f'(\xi)| = |f'(x)|$.

Enfin, pour ce qui est de l'unicité, soit $\eta = \xi + h$ une autre racine de f, avec $|h| < |f'(x)| = |f'(\xi)|$. La formule de Taylor pour les polynômes, à l'ordre 2 pour f, en ξ, donne :

$$0 = f(\eta) = f(\xi) + hf'(\xi) + h^2 t,$$

avec $t \in O_K$, donc $|t| \leqslant 1$.

Ainsi ($f(\xi) = 0$),

$$0 = h(f'(\xi) + ht),$$

ce qui est absurde si $h \neq 0$ car $|ht| < |f'(\xi)|$

On a donc montré le résultat, ainsi, au passage, que la vitesse de convergence de la méthode (ordre 2). □

Corollaire 1.2.7. *Soit $f \in O_K[X]$ un polynôme unitaire et soit $\overline{f}$ la réduction de f modulo m_K. Si $\overline{\alpha}$ est une racine simple de $\overline{f}$ dans k, alors il existe $\tilde{\alpha} \in O_K$, unique, dont la réduction modulo m_K est $\overline{\alpha}$, et tel que $f(\tilde{\alpha}) = 0$.*

Démonstration. Soit $\alpha \in O_K$ dont la réduction modulo m_K est $\overline{\alpha}$. Supposer que $\overline{\alpha}$ est racine simple de $\overline{f}$ revient à dire que $v(f(\alpha)) > 0$ et $v(f'(\alpha)) = 0$, ce qui nous place exactement dans les conditions d'applications du lemme de Hensel, et permet de conclure. □

Maintenant, nous allons voir que le lemme de Hensel peut, sous une version un peu différente, permettre de relever, non seulement des racines, mais aussi des factorisations.

Définition 1.2.8. Si $g \in K_n[X]$ et $h \in K_m[X]$, on note $\theta_{g,h}$ l'application de $K_m[X] \oplus K_n[X]$ dans $K_{m+n}[X]$ qui à (u, v) associe $ug + vh$, et on note $R_{m,n}(g, h)$ le déterminant de la matrice de $\theta_{g,h}$ exprimée dans les bases $(e_i, e_j)_{i \leqslant m, j \leqslant n}$ et $(e_k)_{i \leqslant m+n}$. C'est le résultant de ces deux polynômes (modulo la considération de ces polynômes dans des espaces trop "gros").

Lemme 1.2.9. *$R_{m,n}(g, h) = 0$ si et seulement si $\deg g \leqslant n - 1$ et $\deg h \leqslant m - 1$ ou g et h ne sont pas premiers entre eux.*

Démonstration. Si $\deg g \leqslant n - 1$ et $\deg h \leqslant m - 1$, alors $\theta_{g,h}(K_m[X] \oplus K_n[X]) \subset K_{n+m+1}[X]$ et $\theta_{g,h}$ ne peut être bijective pour des considérations de dimension. Si g et h sont divisibles par w avec $\deg w \geqslant 1$, alors $\theta_{g,h}\left(\frac{h}{w}, -\frac{g}{w}\right) = 0$ et $\theta_{g,h}$ n'est pas injective. Ainsi, dans chacun de ces deux cas, $R_{m,n}(g, h) = 0$.

Réciproquement, si $g \wedge h = 1$, alors une solution de l'équation $gu + hv = 0$ doit vérifier $g|v$ et $h|u$, donc si $(u, v) \neq 0$, $\deg g \leqslant \deg v$ et $\deg h \leqslant \deg u$. Or, si $\deg g = n$ ou $\deg h = m$, comme on regarde $(u, v) \in K_m[X] \oplus K_n[X]$, c'est absurde. Ceci implique que $\theta_{g,h}$ est injective, donc bijective pour des considérations de dimension. Ainsi, on a bien $R_{m,n}(g, h) \neq 0$. □

Définition 1.2.10. Si $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, on définit $v_G(f)$, valuation de Gauss de f, par la formule $v_G(f) = \inf_{0 \leqslant i \leqslant n} v(a_i)$. On peut remarquer qu'elle correspond, sur $K_n[X]$, à la norme infinie de K^{n+1}.

Théorème 1.2.11 (Forme forte du lemme de Hensel)**.** *Soit $C > 0$ et soient $f, g, h \in O_K[X]$ tels que :*

(i) $\deg g \leqslant n$, $\deg h \leqslant m$ *et* $\deg f - gh \leqslant n + m - 1$ *;*

(ii) $v_G(f - gh) \geqslant C + 2v(R_{m,n}(g, h))$ *(en particulier, cela suppose que ce résultant est non nul),*

alors il existe des polynômes $\tilde{g}, \tilde{h} \in O_K[X]$ tels que l'on ait :

(i) $\deg(\tilde{g} - g) \leqslant n - 1$ *et* $\deg(\tilde{h} - h) \leqslant m - 1$ *;*

(ii) $v_G(\tilde{g} - g) \geqslant C + v(R_{m,n}(g, h))$ *et* $v_G(\tilde{h} - h) \geqslant C + v(R_{m,n}(g, h))$ *;*

(iii) $f = \tilde{g}\tilde{h}$.

Démonstration. L'essentiel de la preuve sera de se ramener au théorème de point fixe de Picard.

En effet, on cherche $(u, v) \in K_n[X] \oplus K_m[X]$ tel que :

$$f = (g + v)(h + u) \Leftrightarrow f - gh - uv = gu + hv \Leftrightarrow (u, v) = \theta_{g,h}^{-1}(f - gh - uv).$$

On remarque que l'hypothèse (ii) montre, avec le lemme précédent, que $\theta_{g,h}^{-1}$ est bien définie.

Soit $\phi(u, v) = \theta_{g,h}^{-1}(f - gh - uv)$, on est ramené à chercher un point fixe de ϕ. Soit $B = \{(u, v) \in K_n[X] \oplus K_m[X], \inf(v_G(u), v_G(v)) \geqslant C + v(R_{m,n}(g, h))\}$.

B est une boule fermée de $K_n[X] \oplus K_m[X]$, donc en particulier, B est complet.

Lemme 1.2.12. *ϕ est une application strictement contractante de B dans lui-même.*

Démonstration. Soit $(u, v) \in B$, alors

$$\begin{aligned} v_G(f - gh - uv) &\leqslant \inf(v_G(f - gh), v_G(uv)) \\ &\leqslant \inf(C + 2v(R_{m,n}(g, h)), 2C + 2v(R_{m,n}(g, h))) = C + 2v(R_{m,n}(g, h)) \end{aligned}$$

D'autre part, comme g et h sont à coefficient dans O_K, alors $\theta_{g,h}$ a tous ses coefficients dans O_K et la matrice de $\theta_{g,h}^{-1}$ est donc à coefficients dans $\frac{1}{R_{m,n}(g,h)} O_K$,

et $v_G(\theta_{g,h}^{-1}(x)) \geqslant v_G(x) - v(R_{m,n}(g,h))$. Ainsi, ϕ envoie B dans lui-même. De plus, si (u,v) et (u',v') sont dans B alors :

$$\begin{aligned} v_G(\phi(u,v) - \phi(u',v')) &= v_G(\theta_{g,h}^{-1}(uv - u'v')) \\ &\geqslant v_G(u(v-v') + v'(u-u')) - v(R_{m,n}(g,h)) \\ &\geqslant \inf(v_G(u) + v_G(v-v'), v_G(v') + v_G(u-u') - v(R_{m,n}(g,h)) \\ &\geqslant c + \inf(v_G(u-u'), v_G(v-v')), \end{aligned}$$

et ainsi, on a bien le fait que ϕ soit contractante. □

On peut donc appliquer le théorème du point fixe de Picard dans B, et on a montré le théorème. □

Corollaire 1.2.13. *Soient $f, g, h \in O_K[X]$ tels que : g est unitaire de degré n, $\deg h \leqslant m$ et $\deg(f - gh) \leqslant n + m - 1$, les réductions $\overline{g}$ et $\overline{h}$ et de g et h modulo m_K sont premières entre elles, et $v_G(f - gh) > 0$. Alors il existe $\tilde{g}$ et $\tilde{h} \in O_K[X]$, uniques, tels que $\deg(\tilde{g}-g) \leqslant n-1$, $\deg(\tilde{h}-h) \leqslant m-1$, $v_G(\tilde{g}-g) > 0$, $v_G(\tilde{h}-h) > 0$ et $\tilde{g}\tilde{h} = f$.*

Démonstration. Comme $\overline{g}$ et $\overline{h}$ sont premiers entre eux, on a $R_{m,n}(\overline{g}, \overline{h}) \neq 0$. Ceci implique $v(R_{m,n}(g,h)) = 0$. On peut alors appliquer le théorème précédent pour n'importe quel $C \in \mathbb{R}$ tel que $v_G(f - gh) \geqslant C > 0$, et il suffit alors de faire tendre C vers 0 pour obtenir le résultat.

□

Corollaire 1.2.14. *Soit $f \in K[X]$ un polynôme unitaire irréductible tel que $f(0) \in O_K$. Alors f a tout ses coefficients dans O_K.*

Démonstration. Soit i le plus grand indice tel que $v(a_i)$ soit minimal. On a $v_G(f) = v(a_i)$ et si on pose :

$$a_i^{-1} f(X) = b_n X^n + \cdots + b_{i+1} X^{i+1} + X^i + b_{i-1} X^{i-1} + \cdots + b_0,$$

alors les b_k sont dans O_K, et en particulier, $v(b_k) > 0$ si $i+1 \leqslant k \leqslant n$. Remarquons que si on pose $g(X) = X^i + b_{i-1}X^{i-1} + \cdots + b_0$ et $h = 1 + b_n X^{n-i}$, alors $a_i^{-1} f = gh$ modulo m_K. On est en fait exactement dans les conditions d'applications du corollaire précédent, qui nous donne $\tilde{g}$ et $\tilde{h}$ dans $O_K[X]$ tels que $f = a_i \tilde{g}\tilde{h}$, vu les définitions, ni $\tilde{g}$, ni $\tilde{h}$ ne soit constant, ce qui contredit l'hypothèse f irréductible, et donne le résultat. □

1.3 Clôture algébrique d'un corps valué complet, le corps $\mathbb{C}_p$

Muni de ces résultats, nous allons pouvoir étudier la clôture algébrique d'un corps valué complet, ainsi que le comportement par rapport à la complétion d'un corps algébriquement clos. Au passage, on montrera le théorème fondamental sur les extensions de valuations et on donnera quelques mots sur la théorie des polygones de Newton.

1.3.1 Espaces vectoriels de dimension finie sur un corps normé complet

Ici, nous allons voir que l'équivalence des normes en dimension fini ne concerne pas seulement les $\mathbb{R}$-espaces vectoriels, mais que seul le fait d'être un corps normé complet suffit.

Proposition 1.3.1. *Soit K un corps normé complet, et V un espace vectoriel de dimension finie sur K. Alors toutes les normes d'espace vectoriel sur V qui sont compatibles avec la norme sur K (i.e. que $\|\lambda x\| = |\lambda|\|x\|$ si $\lambda \in K$, $x \in V$) sont équivalentes et rendent V complet.*

Démonstration. Montrons qu'elles sont toutes équivalentes à la norme "infinie", par récurrence sur la dimension, et qu'elles rendent l'espace complet.

Si V est de dimension 1, on n'a rien à prouver.

Sinon, si on a le résultat pour tout K-espace vectoriel de dimension $n-1 \geqslant 1$, alors soit V un K-espace vectoriel de dimension n et $\| \ \|$ une norme sur V compatible avec la norme sur K.

Soit $(e_1, \dots, e_n)$ une base de V. On a :

$$\|x\| = \|x_1e_1 + \cdots + x_ne_n\| \leqslant (\|e_1\| + \cdots + \|e_n\|) \sup(|x_1|, \dots, |x_n|) = (\|e_1\| + \cdots + \|e_n\|)\|x\|_\infty,$$

ce qui montre la première inégalité pour l'équivalence des normes.

Montrons la seconde par l'absurde : supposons qu'il existe une suite $x^{(k)} = x_1^{(k)}e_1 + \cdots + x_n^{(k)}e_n$ qui tende vers 0 pour la norme $\| \ \|$ mais pas pour la norme infinie.

Alors, il existe $C > 0$, $i \in \{1, \dots, n\}$ et $\phi : \mathbb{N} \to \mathbb{N}$ strictement croissante, tels que pour tout $k \in \mathbb{N}$, on ait $|x_i^{\phi(k)}| \geqslant C$. Ainsi, la suite de terme général $v_k = \frac{x_1^{\phi(k)}}{x_i^{\phi(k)}}e_1 + \cdots + \frac{x_n^{\phi(k)}}{x_i^{\phi(k)}}e_n$ tend encore vers 0 pour la norme $\| \ \|$. Ainsi, e_i est dans l'adhérence de $Vect(e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n)$ qui est complet donc fermé par hypothèse de récurrence, ce qui implique $e_i \in Vect(e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n)$, ce qui est absurde.

Par ailleurs, la norme infinie rend bien V complet : être de Cauchy pour $\| \ \|_\infty$ implique l'être pour chaque coordonnées, et K est supposé complet. On a donc montré l'hérédité, et le résultat par récurrence. □

1.3.2 Extensions de valuations

Après avoir vu l'équivalence des normes en dimension finie, nous allons en déduire qu'il n'y a qu'une manière de prolonger une valuation sur un corps complet à une extension finie de celui-ci.

Définition 1.3.2. Soit L une extension finie d'un corps K, et $x \in L$. Alors on définit la norme de x de L sur K, $N_{L/K}(x)$ comme le déterminant de l'endomorphisme $y \mapsto xy$ du K-espace vectoriel L. Si $P = X^d + \cdots + a_0$ est le polynôme minimal unitaire de x sur K, alors $N_{L/K}(x) = ((-1)^d a_0)^{\frac{[L:K]}{d}}$.

Théorème 1.3.3. *Soit K un corps complet pour une valuation v, et soit L une extension finie de K. Alors il existe une unique manière de prolonger v en une valuation de L. De plus, si $x \in L$, alors :*

$$v(x) = \frac{1}{[L:K]} v(N_{L/K}(x)).$$

Démonstration. Considérons d'abord l'unicité : L peut être vu comme un K-espace vectoriel de dimension finie $[L:K]$. Si v_1 et v_2 sont deux valuations sur L prolongeant v sur K, alors par l'équivalence des normes en dimension finie et la caractérisation de cette équivalence en terme de valuations : il existe $s \in \mathbb{R}_+^*$ tel que $v_2(x) = sv_1(x)$. En prenant $x \in K$, on obtient $s = 1$, ce qu'on voulait démontrer.

Maintenant, pour l'existence, montrons que la formule donnée défini bien une valuation sur L. La seule chose, non immédiate, à vérifier est l'inégalité ultratriangulaire : $v(\alpha + \beta) \geqslant \inf(v(\alpha), v(\beta))$. En soustrayant $v(\alpha)$ ou $v(\beta)$ de chaque côté de l'égalité (et en supposant $\alpha, \beta \neq 0$, sans ça, il n'y a rien à montrer), on est ramené à $v(1 + x) \geqslant \inf(0, v(x))$ et $v(1 + \frac{1}{x}) \geqslant \inf(0, v(\frac{1}{x}))$ Ceci revient alors à montrer que si $v(x) \geqslant 0$, alors $v(1 + x) \geqslant 0$ (en effet, montrer cette implication couvre bien le second cas de $v(1 + x) \geqslant \inf(0, v(x))$, qui se ramène bien l'inégalité ultratriangulaire).

Soit $x \in L$, supposons que $v(N_{L/K}(x)) \geqslant 0$ et montrons que $v(N_{L/K}(1 + x)) \geqslant 0$. Soit $f(X) = X^d + \cdots + a_0$ le polynôme minimal de x sur K. On a alors (par multiplicativité des degrés) $d|[L:K]$ et $N_{L/K}(x) = ((-1)^d a_0)^{\frac{[L:K]}{d}}$. Ainsi, $v(N_{L/K}(x)) \geqslant 0$ implique $a_0 \in O_K$ et l'irréductibilité de f implique alors f à coefficients dans O_K, d'après le corollaire 1.2.14. De plus, le polynôme minimal de $1 + x$ est $f(X - 1)$ et donc $N_{L/K}(1 + x) = ((-1)^d f(-1))^{\frac{[L:K]}{d}} \in O_K$, ce qui conclut. □

Remarque. Le résultat est faux si K n'est pas complet. Par exemple, si $K = \mathbb{Q}$ muni de v_5, et si $L = \mathbb{Q}(i)$, alors on a dans L, $5 = (2 - i)(2 + i)$, décomposition en facteurs premiers, et donc on peut définir naturellement sur L les valuations v_{2-i} et v_{2+i}, qui prolongent toutes deux v_5 sur K.

Corollaire 1.3.4. *Si $\overline{K}$ est une clôture algébrique de K, il existe une unique manière de prolonger v à $\overline{K}$. De plus,* $\mathrm{Aut}(\overline{K}/K)$ *agit sur $\overline{K}$ par des isométries.*

Démonstration. L'unicité est directe par le résultat précédent, de même que l'existence, en considérant $x \in \overline{K}$ comme $x \in L = K(x)$. Enfin, si on remarque que si $x \in \overline{K}$, $\sigma \in \mathrm{Aut}(\overline{K}/K)$, alors $N_{K(x)/K}(x) = N_{K(\sigma(x))/K}(\sigma(x))$.

□

Corollaire 1.3.5. *Si $P \in K[X]$ est irréductible, alors toutes ses racines dans $\overline{K}$ ont la même valuation.*

Démonstration. $\mathrm{Aut}(\overline{K}/K)$ permute transitivement les racines d'un polynôme irréductible, ce qui permet de conclure. □

1.3.3 Polygone de Newton

Ces outils étant développés, nous pouvons maintenant considérer la théorie des polygones de Newton, outil puissant d'étude des polynômes. Elle nous permettra, par exemple, de donner une généralisation du crière d'Eisenstein.

Pour ce qui suit, on fixe une clôture algébrique de K et on va prendre les racines des polynômes de $K[X]$ dans cette clôture. Ce qui précède montre qu'on peut aussi considérer leurs valuations.

Définition 1.3.6. Soit $f(X) = a_0 + \cdots + a_n X^n \in K[x]$ un polynôme. Soit $P = \{(0, v(a_0)), \ldots, (n, v(a_n))\}$.

On définit *le polygone de Newton* de f comme l'ensemble des points d'abscisse dans $[0, n]$ qui sont au-dessus de l'enveloppe convexe "inférieure" de P, ainsi que cette enveloppe convexe. On entend par enveloppe convexe "inférieure" l'enveloppe convexe des points de P, à l'exception de ceux qui sont au-dessus du segment joignant $(0, (a_0))$ à $(n, v(a_n))$.

Cela correspond aussi au graphe de la plus grande fonction convexe sur $[0, n]$, f, qui soit "sous" les points de P, c'est-à-dire telle que f est convexe et vérifie pour tout i, $f(i) \leqslant v(a_i)$, et elle est le plus grande (au sens d'être plus grand en chaque point) à le vérifier.

Cette fonction convexe sera notée $Newt_f$.

Vue cette définition, une petite modification de l'algorithme décrit dans le texte [9] permet de calculer facilement l'enveloppe convexe d'un polynôme à coefficients, par exemple, rationnels, donné. C'est ce qui m'a permis de tracer, en Maple, les exemples donnés ici.

Lemme 1.3.7. *Soit $P(X) = a_n X^n + \cdots + a_0 \in K[X]$ un polynôme de degré n, et soient $\alpha_1, \ldots, \alpha_n$ les racines (avec multiplicité) de P dans $\overline{K}$, rangées par valuation décroissante : $v(\alpha_1) \geqslant v(\alpha_2) \geqslant \cdots \geqslant v(\alpha_n)$. Alors, si $i \in \{0, \ldots, n\}$, on a : $v(a_i) \geqslant v(a_n) + \sum_{k=0}^{n-i-1} v(\alpha_{n-k})$, avec égalité si $v(\alpha_i) > v(\alpha_{i+1})$.*

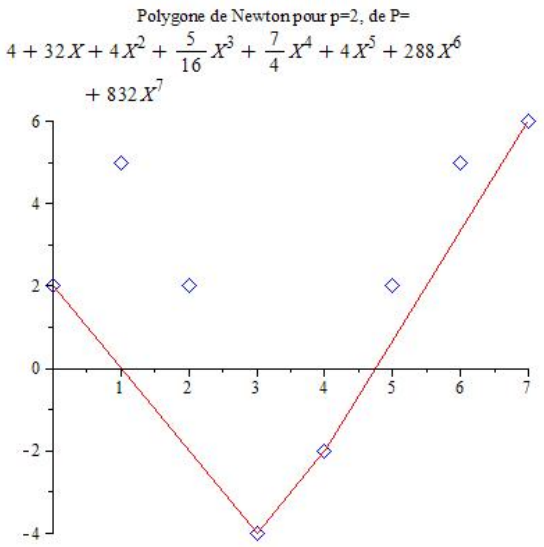


FIGURE 1 – Un premier exemple

Démonstration. Tout est conséquence des relations coefficients-racines, en remarquant que pour le cas d'égalité cité, si $v(\alpha_i) > v(\alpha_{i+1})$, alors dans la fonction symétrique d'ordre $n-i$, tous les autres termes que $\prod_{k=0}^{n-i-1} \alpha_{n-k}$ ont une valuation strictement plus grande que $\sum_{k=0}^{n-i-1} v(\alpha_{n-k})$. □

Corollaire 1.3.8. *Soit $u : [0, n[\to \mathbb{R}$ la fonction définie par $u(x) = -v(\alpha_i)$ si $x \in [i-1, i[$. Alors $Newt_f(x) = v(a_n) + \int_n^x u(t)\mathrm{d}t$.*

Démonstration. D'une part, la fonction $v(a_n) + \int_n^x u(t)\mathrm{d}t$ est affine par morceaux, et convexe car u est croissante (et donc on aura les inégalités nécessaires sur les demi-tangentes). L'inégalité et le cas d'égalité du lemme précédent permettent alors de conclure sur le fait que $Newt_f = v(a_n) + \int_n^x u(t)\mathrm{d}t$. □

Définition 1.3.9. On note $Newt_f$ la fonction convexe associé au polgone de Newton de f. On appelle *pente du polygone de Newton* un élément de $Newt'_f([0, n])$. Si λ est une pente de $Newt_f$, on appelle *segment de pente* λ de $Newt_f$ l'ensemble $\left\{(x, Newt_f(x)) / Newt'_f(x) = \lambda\right\}$. La *longueur* de ce segment sera, par définition, la longueur de son projeté sur l'axe des abscisses.

On peut maintenant reformuler le lemme précédent en termes de polygones de Newton :

Théorème 1.3.10. *P a une racine de valuation λ si et seulement si $-\lambda$ est une pente de $Newt_P$. De plus, le nombre de racines de P de valuation λ, comptées avec multiplicité, est la longueur du segment de pente $-\lambda$ de $Newt_P$.*

Remarque. Du fait que si $P \in K[X]$ est irréductible, toutes ses racines ont même valuation, on obtient que si P est irréductible, alors $Newt_P$ n'a qu'une pente. La réciproque est, bien sûr, fausse (prendre par exemple $(X-1)(X-2)$ sur $\mathbb{Q}$, muni de v_5).

Remarque. Ainsi, si le polygone de Newton de P n'est pas un segment, P n'est pas irréductible. C'est en particulier le cas dans l'exemple donné dans la Figure 1.

Lemme 1.3.11. *Si f et g sont deux polynômes, alors le polygone de Newton de fg a pour pentes celles de f et g, avec longueur la somme de celle de f et de celle de g.*

Démonstration. Ceci est immédiat par la caractérisation des pentes en fonction des valuations des racines sur $\overline{K}$. □

Ceci va permettre de montrer un critère d'irréductibilité, plus fort que le critère d'Eisenstein :

Proposition 1.3.12 (critère de Dumas)**.** *Si $P \in K[X]$, de degré n, avec v valuation discrète normalisée, et si le polygone de Newton de P, $Newt_P$, est un segment qui n'a que $(0, v(a_0))$ et $(n, v(a_n))$ comme points entiers (i.e. comme points de $\mathbb{Z}^2$), alors P est irréductible.*

Remarque. La réciproque est fausse : $1 + X + X^2$ est irréductible sur $\mathbb{Q}$ (car par exemple unitaire, irréductible sur $\mathbb{F}_2$ donc sur $\mathbb{Z}$ donc sur $\mathbb{Q}$), mais son polygone de Newton est le segment $[0, 2]$ (de l'axe des abscisses).

Démonstration. Nous allons montrer le résultat par contraposée. Supposons que $P = fg = \sum_{j=0}^{n} a_j X^j$ sur K, avec $f \neq 1$, $g \neq 1$. Soit λ une pente de P, de longueur l_λ.

Supposons d'abord que λ est une pente de f mais pas de g. P a alors comme pente λ, toujours de longueur l_λ, joignant les sommets $(i, v(a_i)$ et $(i + l_\lambda, v(a_{i+l_\lambda}))$. Comme $g \neq 1$, ce ne sont pas les seules pentes de $Newt_P$: $(i, v(a_i)$ et $(i+l_\lambda, v(a_{i+l_\lambda}))$ ne peuvent être exactement égaux à $(0, v(a_0))$ et $(n, v(a_n))$, et donc $Newt_P$ a nécessairement un point entier autre que $(0, v(a_0))$ et $(n, v(a_n))$.

Maintenant, si λ est pente de f et g, de longueur respectivement l_1 et l_2 dans chaque polygone, alors P a pour sommets (consécutifs), pour un certain i, $(i, v(a_i))$ et $(i + l_1 + l_2, v(a_{i+l_1+l_2}))$, avec $\lambda = \frac{v(a_{i+l_1+l_2} - v(a_i)}{l_1+l_2}$. Mais alors, montrons que $(i + l_1, \lambda(i + l_1) + (v(a_i) - \lambda i)) = (i + l_1, v(a_i) + \lambda l_1)$ est un point entier de $Newt_P$. D'une part, on peut noter que ce point est bien un point de $Newt_P$, comme il est, de part sa définition, sur le segment joignant $(i, v(a_i))$ et $(i + l_1 + l_2, v(a_{i+l_1+l_2}))$, qui est de pente λ.

Ainsi, il reste, comme $v(a_i) \in \mathbb{Z}$, seulement à montrer que λl_1 est bien un entier.

Or, par définition, si $f = \sum_{j=0}^{m} b_j X^j$, on a λ qui est la pente du segment joignant les deux sommets consécutifs de $Newt_f$, $(j, v(b_j))$ et $(j+l_1, v(b_{j+l_1}))$. Ainsi, $\lambda = \frac{v(b_{j+l_1})-v(b_j)}{j+l_1-j} = \frac{v(b_{j+l_1})-v(b_j)}{l_1}$, et donc $\lambda l_1 \in \mathbb{Z}$, ce qui clôt la démonstration. □

Corollaire 1.3.13 (Critère d'Eisenstein)**.** *Si $P(X) = a_0 + \cdots + a_{n-1}X^{n-1} + X^n$ vérifie $v(a_i) \geqslant 1$ quel que soit $0 \leqslant i \leqslant n-1$ et $v(a_0) = 1$, alors P est irréductible.*

Démonstration. On remarque que son polygone de Newton est le segment de longueur n joignant $(0, 1)$ et $(n, 0)$ (de pente $\frac{-1}{n}$) donc la proposition précédente s'applique directement. □

Pour finir, les figures 2 et 3 présentent deux exemples, dont l'un où l'on peut appliquer le critère de Dumas, mais pas celui d'Eisenstein.

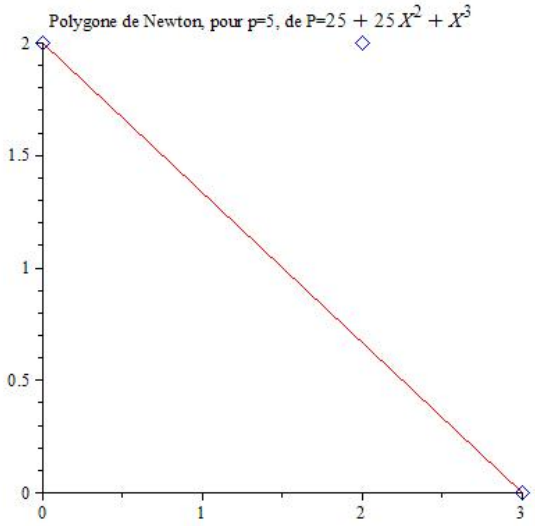


FIGURE 2 – Un cas d'irréductibilité, par le critère de Dumas.

1.3.4 Le complété d'un corps algébriquement clos

On a vu qu'il existe une unique manière de prolonger une valuation à la clôture algébrique d'un corps valué complet, mais cette clôture algébrique n'a aucune raison d'être complète (et elle, en général, ne le sera pas). Cela dit, on peut la compléter, mais est-ce que le résultat sera algébriquement clos, ou devra-t-on prendre la clôture algébrique, puis encore le complété... Le résultat suivant permet de voir que l'on peut s'arrêter au complété d'un corps algébriquement clos.

Lemme 1.3.14. *Soit $P(X) = X^n + a_{n-1}X^n + \cdots + a_0 \in O_K[X]$. Alors les racines de P (dans une clôture algébrique) sont de valuation positive.*

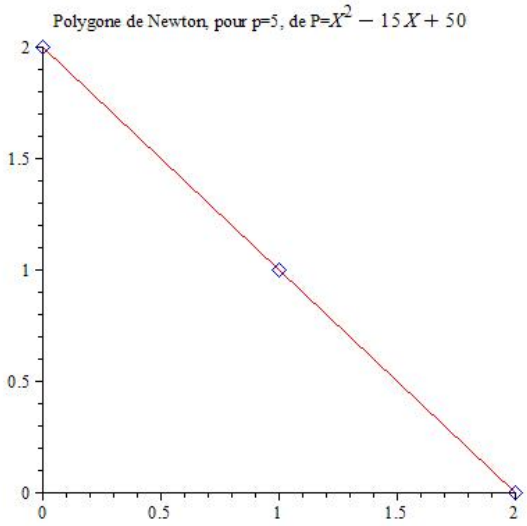


FIGURE 3 – Un cas de non-irréductibilité, le critère ne s'applique pas.

Démonstration. Si $x \in]0, n[$, alors les taux d'accroissement de $Newt_P$ à gauche et à droite de x sont, par convexité, inférieurs à $\frac{v(a_n)-Newt_P(x)}{n-x} = \frac{-Newt_P(x)}{n-x}$. Or, les $v(a_i)$ sont positives, donc par convexité, $Newt_P(x) \geqslant 0$, et donc on en déduit que les pentes du polygone de Newton de P sont toutes négatives, ce qui veut dire que toutes les racines de P sont de valuation positive. □

Théorème 1.3.15. *Si K est un corps algébriquement clos muni d'une valuation, son complété, $\widehat{K}$ est algébriquement clos.*

Démonstration. Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire irréductible de $\widehat{K}[X]$. Montrons que P a une racine dans $\widehat{K}$. Quitte à changer P en $\alpha^n P\left(\frac{X}{\alpha}\right)$, ce qui revient à multiplier chaque a_i par α^{n-i}, on peut supposer que les coefficients de P sont de valuation positive.

On suppose d'abord que P est séparable, c'est-à-dire que $P \wedge P' = 1$. Soit alors $U, V \in \widehat{K}[X]$ tels que $UP + VP' = 1$. On note comme plus haut v_G la valuation de Gauss sur $\widehat{K}[X]$. Soit $C > \sup(0, -v_G(U), -2v_G(V))$, et soit, pour $i \in \{0, \ldots, n-1\}$, $b_i \in K$ tel que $v(b_i - a_i) \geqslant C$ (c'est bien possible car, par définition du complété, K est dense dans $\widehat{K}$). Comme K est algébriquement clos, soit $x_0 \in K$ une racine de $Q(X) = X^n + \sum_{i=0}^{n-1} b_i X^i$. Comme Q a ses coefficients de valuation positive, alors nécessairement, $v(x_0) \geqslant 0$.

Ainsi, on a :

$$\begin{aligned} v(U(x_0)P(x_0)) &= v(U(x_0)) + v((P-Q)(x_0)) \\ &\geqslant \inf_i(v(u_i) + iv(x_0)) + \inf_i(v(a_i - b_i) + iv(x_0)) \\ &\geqslant v_G(u) + C > 0, \end{aligned}$$

et on a montré au passage que $v(P(x_0)) \geqslant C$. Comme $1 = U(x_0)P(x_0)+V(x_0)P'(x_0)$, alors $v(P'(x_0)V(x_0)) = 0$, d'où $v(P'(x_0)) = -v(V(x_0))$. Or, $V(x_0) \geqslant \inf_i(v_i + iv(x_0)) \geqslant v_G(V)$. De plus, On a donc $v(P'(x_0)) \leqslant -v_G(V) < \frac{C}{2} \leqslant \frac{1}{2}v(P(x_0))$. On est alors dans les conditions d'application du lemme de Hensel, qui donne ainsi l'existence d'une solution $x \in \widehat{K}$ à $P(x) = 0$.

Maintenant, si P est irréductible mais non séparable, alors on est nécessairement en caractéristique $p \neq 0$, et donc il existe Q irréductible et séparable, et $m \in \mathbb{N}$ tel que $P(X) = Q(X^{p^m})$. Si x est une racine de Q et x_n une suite d'éléments de K tendant vers x dans $\widehat{K}$, alors la suite $x_n^{p^m}$ est une suite de K qui est de Cauchy (car on a $p^m v(x-y) = v((x-y)^{p^m}) = v(x^{p^m} - y^{p^m})$), donc qui converge dans $\widehat{K}$, vers une racine de P. D'où le résultat. □

1.3.5 Le corps résiduel d'un corps algébriquement clos

Tout ce qui précéde nous permet maintenant d'étudier le comportement du corps résiduel par rapport au passage à la clôture algébrique, ou au fait d'être algébriquement clos.

Lemme 1.3.16. *Soient K un corps valué complet, et L une extension finie de K, alors k_L est une extension algébrique de k_K de degré $\leqslant [L : K]$.*

Démonstration. On a $O_K \cap m_L = m_K$, donc k_K s'injecte dans k_L, et ainsi k_L est une extension de k_K. Soient $\overline{\alpha}_1, \ldots, \overline{\alpha}_d$ des éléments de k_L formant une famille libre sur k_K. Pour chaque $i \in \{1, \ldots, d\}$, soit $\alpha_i \in O_L$ tel que son image dans k_L est $\overline{\alpha}_i$. Supposons que les α_i forment une famille liée sur K, et soit $(\lambda_1, \ldots, \lambda_d)$ une famille d'éléments non tous nuls de K telle que $\lambda_1\alpha_1 + \cdots + \lambda_d\alpha_d = 0$. Quitte à diviser par l'élément de valuation la plus faible, on peut supposer tout les λ_i dans O_K, et que l'un d'entre eux est égal à 1. C'est une contradiction lorsqu'on réduit modulo m_L comme les $\overline{\alpha}_1, \ldots, \overline{\alpha}_d$ forment une famille libre sur k_K. Ainsi, $[k_L : k_K] \leqslant [L : K]$, ce qu'on souhaitait démontrer. □

Lemme 1.3.17. *Si K est un corps ultramétrique algébriquement clos, alors k_K est algébriquement clos.*

Démonstration. Soit $\overline{P}(X) \in k_K[X]$ unitaire de degré $n \geqslant 1$, et soit $P(X) \in O_K[X]$ relevant $\overline{P}$. Soit $\alpha \in K$ une racine de P, on a alors $\alpha \in O_K$ avec le lemme [**?**]. L'image de α dans k_K est alors une racine de k_K, ce qui permet de conclure. □

Lemme 1.3.18. *Si K est un corps ultramétrique et $\widehat{K}$ dénote son complété, alors $k_K = k_{\widehat{K}}$.*

Démonstration. On a $O_K \cap m_{\widehat{K}} = \{x \in O_K / v(x) > 0\} = m_K$, et donc l'application naturelle de k_K dans $k_{\widehat{K}}$ est injective. D'autre part, comme O_K est dense dans $O_{\widehat{K}}$, cette application est surjective. En effet, soit $\overline{y} \in k_{\widehat{K}}$, et soit $y \in O_{\widehat{K}}$ qui relève $\overline{y}$. Il existe $x \in O_K$ tel que $v(x-y) > 0$. Alors, par définition, $\overline{x}$, classe de x modulo m_K est naturellement envoyé sur $\overline{y}$, ce qui permet de conclure. □

En corollaire de tout ce qui précède, on peut conclure :

Corollaire 1.3.19. *Si K est un corps valué complet, alors le corps résiduel de $\widehat{\overline{K}}$ est une clôture algébrique de k_K.*

Définition 1.3.20. On définit $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$. Comme $k_{\mathbb{Q}_p} = \mathbb{F}_p$, on a $k_{\mathbb{C}_p} = \overline{\mathbb{F}_p}$.

2 Extensions de corps locaux et présentation des théorèmes

Avec ce que l'on vient de voir sur les corps valués, nous pouvons maintenant débuter l'étude des corps locaux, et en particulier celle de leurs extensions. Ceci nous permettra d'énoncer les théorèmes qui constituent l'objectif de ce texte. Pour cela, bien sûr, on commence par une définition d'un corps local.

2.1 Extensions de corps locaux

2.1.1 Corps locaux

Définition 2.1.1. On appelle *corps local* un corps complet pour une valuation dicrète. En particulier, si K est un corps local muni de la valuation v, alors il existe $a \in \mathbb{Z}$ tel que $v(K^*) = a\mathbb{Z}$. On appelle *uniformisante* de K un élément π de K tel que $v(\pi) = a$.

On a alors la propriété immédiate suivante :

Proposition 2.1.2. *L'idéal maximal m_K de l'anneau O_K de K est principal, et un élément de K en est un générateur si et seulement si c'est une uniformisante.*

Exemple.
- $\mathbb{Q}_p$ muni de v_p est un corps local, et p en est une uniformisante.
- Si K est un corps, alors $K((T))$, corps des séries de Laurent à coefficient dans K, muni de la valuation v_T, est un corps local, et T en est une uniformisante.

2.1.2 Écriture et corps résiduel

Nous allons voir que les corps locaux possèdent tous une écriture particulière pour leurs éléments, sous forme de série, à partir de leur corps résiduel.

Définition 2.1.3. Si A est un anneau et I un idéal de A, on dit que A est *séparé et complet* pour la topologie I-adique si l'application naturelle de A dans $\lim_{\leftarrow}(A/I^nA)$ est un isomorphisme d'anneaux topologiques, $\lim_{\leftarrow}(A/I^nA)$ étant muni de la topologie produit, chacun des A/I^nA étant muni de la topologie discrète.

Lemme 2.1.4. *(i) Si K est un corps complet pour une valuation v, et si $\pi \in K$ vérifie $v(\pi) > 0$, alors O_K est séparé et complet pour la topologie π-adique.*
(ii) Si A est un anneau, si $\pi \in A$, si S est un système de représentants de $A/\pi A$ dans A, et si A est séparé et complet pour la topologie π-adique, alors tout élément de A peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} s_n\pi^n$, avec $s_n \in S$.

Démonstration. (i) On note $\iota : O_K \to \lim_{\leftarrow}(O_K/\pi^nO_K)$ l'application qui, à $x \in O_K$, associe la suite des images de x modulo π^n. On a alors :
- $\iota(x) = 0 \Leftrightarrow v(x) \geqslant nv(\pi)$ quel que soit $n \in \mathbb{N} \Leftrightarrow v(x) = +\infty \Leftrightarrow x = 0$, ce qui montre que ι est injective.
- Si $(x_n)_{n\in\mathbb{N}} \in \lim_{\leftarrow}(O_K/\pi^nO_K)$, et si $\widehat{x_n} \in O_K$ est un relèvement de x_n, alors $v(\widehat{x_{n+k}}-\widehat{x_n}) \geqslant nv(\pi)$ quel que soit $n \in \mathbb{N}$. On en déduit que $\iota(x) = (x_n)_{n\in\mathbb{N}}$, ce qui prouve la surjectivité de ι.
- $v(x-y) \geqslant nv(\pi) \Leftrightarrow x = y$ dans O_K/π^kO_K pour tout $k \leqslant n$, ce qui montre que la topologie induite par v sur O_K correspond bien à la topologie produit sur $\lim_{\leftarrow}(O_K/\pi^nO_K)$, chaque O_K/π^nO_K étant muni de la topologie discrète.

(ii) Soit $s : A \to S$ l'application qui à x associe l'unique élément $s(x)$ de S vérifiant $x - s(x) \in \pi A$. Si $x \in A$, on définit par récurrence une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de A en posant $x_0 = x$ et, si $n \geqslant 1$, $x_n = \frac{1}{\pi}(x_{n-1} - s(x_{n-1}))$. On a alors $x = \sum_{i=0}^{n} s(x_i)\pi^i + \pi^{n+1}x_{n+1}$, quel que soit $n \in \mathbb{N}$, et donc $x = \sum_{n=0}^{+\infty} s(x_n)\pi^n$, série qui est bien convergente car A est séparé et complet pour la topologie π-adique, et que cette série converge bien pour la topologie π-adique. Ceci prouve l'existence de l'écriture sous la forme annoncée.
Pour ce qui est de l'unicité, si $\sum_{n=0}^{+\infty} s_n\pi^n = \sum_{n=0}^{+\infty} s'_n\pi^n$, en réduisant modulo π, on trouve $s_0 = s'_0$, et on procéde à partir de là par récurrence.

□

Corollaire 2.1.5. *Si K est un corps local, si S est un système de représentants de k_K dans O_K, si π est une uniformisante de K, alors tout élément de O_K peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} s_n\pi^n$, avec $s_n \in S$.*

2.1.3 Ramification et inertie

Nous allons maintenant voir que la théorie de la ramification pour les corps locaux (de corps résiduel de caractéristique non nulle) se trouve bien plus simple que celle des corps de nombres.

Dans toute cette partie, sauf mention du contraire, F désigne un corps complet pour une valuation discrète, dont le corps résiduel k_F est de caractéristique p.

Définition 2.1.6. Si K est une extension finie de F, on a vu que k_K est une extension finie de k_F. Le degré de k_K sur k_F est l'*indice d'inertie* de l'extension K/F, et sera noté $f = f(K/F)$.

Définition 2.1.7. Si $x \in K$, on a $v(x) = \frac{1}{[K:F]} v(N_{L/K}(x))$, donc $v(K^*) \subset \frac{1}{[K:F]} v(F^*)$ et $v(F^*)$ est un sous groupe d'indice fini $e = e(K/F)$ de $v(K^*)$ (en tant que sous-groupes, discrets, de $\mathbb{R}$). e est appelé l'indice de ramification de l'extension K/F.

Lemme 2.1.8. *Soient $e = e(K/F)$ et $f = f(K/F)$, soient $u_1, \ldots, u_f$ des éléments de O_K dont les réductions modulo m_K forment une base de k_K sur k_F, et soit π_K une uniformisante de O_K. Alors les $\pi_K^j u_i$, pour $0 \leqslant j \leqslant e-1$ et $1 \leqslant i \leqslant f$ forment une base de O_K sur O_F.*

Démonstration. Soit S_F un système de représentants de k_F dans O_F, et soit $S_K = S_F u_1 + \cdots + S_F u_F$, ce qui forme, par définition, un système de représentants de k_K dans O_K. Soit π_F une uniformisante de F. D'après la définition d'uniformisante, la définition de l'indice de ramification, π_K^e a même valuation que π_F. On en déduit que $O_K/\pi_F O_K = O_K/\pi_K^e O_K$. Alors, avec le corollaire précédent, $S_K + \pi_K S_K + \cdots + \pi_K^{e-1} S_K$ est un système de représentants de $O_K/\pi_F O_K$, et ainsi, tout élément de O_K peut s'écrire de manière unique sous la forme :

$$\sum_{n=0}^{+\infty} \pi_F^n \left(\sum_{j=0}^{e-1} \pi_K^j \left(\sum_{i=1}^{f} s_{i,j,n} u_i \right) \right) = \sum_{j=0}^{e-1} \sum_{i=1}^{f} \pi_K^j u_i \left(\sum_{n=0}^{+\infty} \pi_F^n s_{i,j,n} \right),$$

avec $s_{i,j,n} \in S_F$, ce qui implique, sachant que tout élément de O_F peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} \pi_F^n s_n$, avec $s_n \in S_F$, que tout élément de O_K peut s'écrire de manière unique sous la forme $\sum_{j=0}^{e-1} \sum_{i=1}^{f} \pi_K^j u_i y_{i,j}$, avec $y_{i,j} \in O_F$, ce qui permet de conclure. □

Corollaire 2.1.9. $e(K/F) f(K/F) = [K : F]$

Démonstration. Ceci vient du fait qu'une base de O_K sur O_F est aussi une base de K sur F. □

Définition 2.1.10. On dit que l'extension K/F est *non ramifiée* si $e(K/F) = 1$, et si k_K/k_F est séparable. Elle est *totalement ramifiée* si $e(K/F) = [K : F]$. Elle est *modérément ramifiée* si $e(K/F)$ est premier à la caractéristique du corps résiduel et si k_K/k_F est séparable, et *sauvagement ramifiée* dans le cas contraire.

Lemme 2.1.11. *Si L/K et K/F sont deux extensions finies, alors $e(L/F) = e(L/K)e(K/F)$ et $f(L/F) = f(L/K)f(K/F)$.*

Démonstration. Pour la seconde égalité, c'est simplement la multiplicativité des degrés. Pour la première, la multiplicativité des degrés, le corollaire précédent, et la seconde égalité permettent de conclure. □

2.2 Structure des extensions

À travers cette théorie de la ramification, nous allons étudier les différents types d'extensions que l'on vient de définir, jusqu'à arriver à un théorème de structure sur les extensions.

2.2.1 Extensions totalement ramifiées

Nous allons d'abord voir que l'on peut caractériser les extensions totalement ramifiées en termes de polynômes d'Eisenstein.

Définition 2.2.1. Si K est un corps local, on appelle *polynôme d'Eisenstein* de degré $d \in \mathbb{N}$ un polynôme $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ tel que a_0 soit une uniformisante de K et $a_1, \ldots, a_{d-1} \in m_K$.

Remarque. Un polynôme d'Eisenstein est irréductible (c'est le critère d'Eisenstein !), d'après ce qu'on a vu sur les polygones de Newton.

Lemme 2.2.2. *Soit K un corps complet pour une valuation discrète, et P un polynôme d'Eisenstein de degré d. Soit $L = K[X]/P$ et x l'image de X dans L. alors :*

(i) Si $v(K^*) = u\mathbb{Z}$ avec $u > 0$, alors $v(x) = \frac{u}{d}$ et L/K est totalement ramifiée.
(ii) x est une uniformisante de L.
(iii) Si $y = \sum_{i=0}^{d-1} a_i x^i$, avec les a_i dans K, alors $v(y) = \inf_i(v(a_i) + i\frac{u}{d})$.
(iv) $1, x, \ldots, x^{d-1}$ forment une base de O_L (respectivement L) sur O_K (respectivement K).

Démonstration. Pour le (i), on a la formule $v(x) = \frac{1}{[K:F]}v(N_{K/F}(x))$ et P étant d'Eisenstein, a_0 est une uniformisante, donc $v(N_{K/F}(x)) = (\frac{[L:K]}{d})u = u$. Le (i) donne alors le (ii), comme on connait $v(L^*)$. Pour le (iii), cela vient directement du fait que chaque terme a une valuation différente. Pour voir le fait qu'elles soient différentes, il suffit de constater que $v(a_i) + i\frac{u}{d} = u(v_i + \frac{i}{d})$ avec $v_i \in \mathbb{Z}$, d'après la définition de u, et tout les $v_i + \frac{i}{d}$ ont une partie fractionnaire disctincte (comme $i \leqslant d$). Le (iv) est enfin, une conséquence immédiate du (iii), donnant la liberté du système tandis que le fait qu'il soit générateur est issu de la définition. □

Proposition 2.2.3. *Si K/F est totalement ramifiée et si π_K est une uniformisante de K, alors π_K engendre O_K en tant que O_F-algèbre, et le polynôme minimal de π_K sur F est un polynôme d'Eisenstein.*

Réciproquement, si $P \in F[X]$ est un polynôme d'Eisenstein, si $K = F[X]/P$, et si x est l'image de X dans K, alors K est une extension totalement ramifiée de F et x en est une uniformisante.

Démonstration. Par la section précédente, les $\pi_K^j u_i$ forment une base de O_K sur O_F, mais ici, $f = 1$ et $u_1 = 1$. Si $[K : F] = d$, le polynôme minimal de P de π_K est irréductible de degré d. Son polygone de Newton n'a donc qu'une pente. Par ailleurs, si $P = X^d + a_{d-1} + \cdots + a_0$, on a $a_0 = \pm N_{K/F}(\pi_K)$, donc $v(a_0) = dv(\pi_K)$, et ainsi, a_0 est une uniformisante de F. De plus, comme le polygone de Nexton de P n'a qu'une seule pente, alors par convexité, $v(a_i) \geqslant (d-i)v(\pi_K) > 0$, et donc $a_i \in m_K$, si $1 \leqslant i \leqslant d$. Ainsi, P est d'Eisenstein. Pour la réciproque, elle est une simple conséquence du lemme précédent. □

2.2.2 Monogénéité de l'anneau des entiers

Nous allons voir que les extensions totalement ramifiées ne sont pas les seules à être monogènes sur O_F (c'est-à-dire telles que $O_K = O_F[x]$), mais qu'en fait, une très large classe d'entre elles vérifient cette propriété.

Proposition 2.2.4. *Si K est une extension finie de F, et si k_K/k_F est séparable, alors O_K est une extension monogène de O_F.*

Démonstration. Soient π_F et π_K des uniformisantes de F et K respectivement. Soit $y \in O_K$ dont la réduction $\overline{y}$ modulo π_K est un élément primitif de k_K sur k_F (qui existe car l'extension k_K/k_F est supposée séparable, et ainsi, le théorème de l'élément primitif peut s'appliquer). Soit $P \in O_F[X]$ unitaire dont la réduction $\overline{P}$ modulo π_F est le polynôme minimal de $\overline{y}$ sur k_F. On a ainsi $P(y) = 0$ modulo π_K, et $P'(y) \neq 0$ modulo π_K. En effet, $\overline{y}$ est racine simple de $\overline{P}$: $\overline{P}$ est le polynôme minimal de $\overline{y}$, d'une part, et d'autre part, ne peut pas être de dérivée nulle, sinon, il serait un polynôme élevé à la puissance p, avec p caractéristique de k_F, et ne serait donc pas minimal. Ainsi, $a \mapsto P(y+a\pi_K) = P(y)+a\pi_K P'(y) \mod \pi_K^2$ n'est pas identiquement nulle sur O_K, et donc il existe $x = y+a\pi_K$ tel que $P(x)$ soit une uniformisante de K (il convient par exemple de ne pas annuler $P(y) + a\pi_K P'(y)$ modulo π_K^2, comme $P(y) + a\pi_K P'(y) = 0 \mod \pi_K$). Mais alors, on comme on a vu précédemment, les $x^i P(x)^j$ avec $0 \leqslant i \leqslant f-1$ et $0 \leqslant j \leqslant e-1$ forment une base de O_K sur O_F, et donc x engendre O_K comme O_F-algèbre. □

2.2.3 Extensions non ramifiées et dévissage des extensions finies

Maintenant, quelques résultats sur les extensions non-ramifiées. On pourra caractériser l'extension non ramifiée maximale de $\mathbb{Q}_p$.

Théorème 2.2.5. – *Soit k une extension finie séparable de k_F, alors il existe une extension non ramifiée $F(k)$ de F dont le corps résiduel est k. En terme de diagramme, de* $\begin{array}{c} k \\ | \\ {\scriptstyle \text{sep}} \\ | \\ k_F \end{array}$ *donne* $\begin{array}{c} F(k) \\ | \\ {\scriptstyle \text{nr}} \\ | \\ F \end{array}$.

– *Si L est une extension finie de F, et si k_L/k_F est une extension séparable, alors $F(k_L) \subset L$, l'extension $L/F(k_L)$ est totalement ramifiée, et $F(k_L)$ est l'unique extension non ramifiée de F ayant ces deux propriétés. En terme de diagramme,* $\begin{array}{c} L \\ | \\ F \end{array}$ *et* $\begin{array}{c} k_L \\ | \\ {\scriptstyle \text{sep}} \\ | \\ k_F \end{array}$ *donnent* $\begin{array}{c} L \\ | \\ {\scriptstyle \text{t.r.}} \\ | \\ F(k_L) \\ | \\ {\scriptstyle \text{n.r.}} \\ | \\ F \end{array}$ *et* $\begin{array}{c} k_L \\ | \\ k_L \\ | \\ k_F \end{array}$.

Démonstration. Nous allons d'abord construire $F(k)$. Soit $\overline{\alpha}$ un élément primitif de k/k_F (qui existe car l'extension est séparable), et soient $\overline{P} \in k_F[X]$ son polynôme minimal, et $P \in O_F[X]$ unitaire dont la réduciton est $\overline{P}$. Comme on l'a vu plus haut, avec le lemme de Hensel, si L est une extension finie de F dont le corps résiduel contient k, alors L contient une unique racine α de P dont l'image dans k_L est $\overline{\alpha}$. Ainsi, $[F(\alpha) : F] \leqslant \deg P = [k : k_F]$. D'autre part, le corps résiduel de $F(\alpha)$ contient $\overline{\alpha}$ par construction, on a pour l'indice d'inertie $f(F(\alpha)/F) \geqslant [k : k_F]$, ce dont on déduit $[F(\alpha) : F] = [k : k_F] = f(F(\overline{\alpha})/F)$, ce qui implique que $F(\alpha)/F$ est non ramifiée.

Maintenant, si L est une extension finie de F, de corps résiduel k, on a $F(\alpha) \subset L$, si on prend α comme ce qui précède, on a $F(\alpha) \subset L$ et, $F(\alpha)$ ayant même corps résiduel que L, on en déduit que l'extension $L/F(\alpha)$ est totalement ramifiée. En particulier, si l'extension L/F est non ramifiée, alors $L = F(\alpha)$. Ceci permet de conclure si l'on pose $F(k) = F(\alpha)$. □

Remarque. Par multiplicativité des degrés et le bon comportement de la notion de séparabilité, la composée de deux extensions non ramifiées est encore une extension non ramifiée. Ainsi, si $\overline{F}$ est une clôture algébrique de F, on peut définir F^{nr}, l'extension maximale non ramifiée de F, réunion de toutes les extensions non ramifiées de F. F^{nr} est un sous-corps de $\overline{F}$.

Exemple. Le polynôme $X^q - X$ n'a que des racines simples dans $\overline{\mathbb{F}}_p$, $q = p^d$ (il suffit de considérer sa dérivée), et ses racines sont exactements les éléments de $\mathbb{F}_q$. Avec les notations précédentes, $\mathbb{Q}_p(\mathbb{F}_q)$ est alors le corps engendré par les racines du polynôme $X^{q-1}-1$, c'est à dire les racines $(q-1)$-ièmes de l'unité. Par exemple, du fait que $q^{k+1}-1 = (q-1)(1+\cdots+q^k)$ et si $y \wedge n = 1$, $y^{\phi(n)} = 1 \mod n$, alors si $n \in \mathbb{N}$ est tel que $n \wedge q = 1$, il existe $f \in \mathbb{N}$ tel que n divise $q^f - 1$ (par exemple $f = n(\phi(n)-1)$). On en déduit que $\mathbb{Q}_p^{nr}$ contient toutes les racines de l'unité d'ordre premier à p de $\overline{\mathbb{Q}_p}$. Le théorème précédant donnant une correspondance (bijective) entre extensions non ramifiées finies de F et extensions finies séparables de k, on en déduit que $\mathbb{Q}_p^{nr}$ est en fait engendré par les racines de l'unité de $\overline{\mathbb{Q}_p}$ d'ordre premier à p.

2.2.4 Extensions modérément ramifiées

Au tour maintenant des extensions modérément ramifiées.

Proposition 2.2.6. *Soit L/F une extension totalement ramifiée de degré $n = n_0 p^k$ avec $n_0 \wedge p = 1$. Alors L contient une unique extension K de F vérifiant $[K:F] = n_0$. De plus, il existe une uniformisante π_K de K telle que $\pi_K^{n_0} \in F$. En terme de diagramme,*

$$\begin{array}{c} L \\ \Big| \text{ tr, } n{=}n_0p^k \\ F \end{array} \quad \textit{donne} \quad \begin{array}{c} L \\ {\scriptstyle p^k}\Big| \text{ t.r., s.r.} \\ K \\ {\scriptstyle n_0}\Big| \text{ t.r., m.r.} \\ F \end{array}$$

Démonstration. Soit π_L une uniformisante de L. D'après ce qu'on a vu auparavant, π_L est racine d'un polynôme d'Eisenstein, et il existe π_F uniformisante de F, $a_1, \ldots, a_{n-1} \in O_F$ tels que l'on ait $\pi_F + \sum_{i=1}^{n-1} a_i \pi_L^i + \pi_L^n = 0$, ou encore $\pi_L^n = u\pi_F$, avec $u = (1 + a_1\pi_L + \cdots + a_{n-1}\pi_L^{n-1}) \in O_L^*$ tel que $v(u-1) > 0$. Comme $n_0 \wedge p = 1$, le lemme de Hensel montre que l'équation $X^{n_0} = u$ a une unique solution, x, dans $1 + m_L$. Alors, $(x^{-1}\pi_L^{p^k})^{n_0} = \pi_F$, ce qui montre que L contient l'extension K définie par le polynôme d'Eisenstein $P(X) = X^{n_0} - \pi_F$, qui est donc, avec ce qui précède, totalement ramifiée, et de degré n_0 sur F.

Maintenant, supposons que L contienne deux extensions K_1 et K_2 de F de degré n_0. Si on applique ce qui précède à ces deux extensions, on voit que si $i \in \{1,2\}$, il existe une uniformisante π_i de K_i telle que $\pi_i^{n_0} \in F$. Mais alors, $v(\pi) = \frac{1}{n_0}$, et donc $x = \frac{\pi_1}{\pi_2} \in O_L^*$, est tel que sa puissance n_0-ème soit dans F. Comme L/F est totalement ramifiée, les corps résiduels de L et F sont les mêmes, et on peut trouver $u \in O_F$ tel que $v(xu^{-1} - 1) > 0$ (on relève dans O_F l'image de x dans $k_L = k_F$). Mais alors, xu^{-1} est l'unique racine n_0-ème de $x^{n_0}u^{-n_0} \in 1 + m_F$ telle

que $v(xu^{-1}-1) > 0$, et ainsi par le lemme de Hensel, $xu^{-1} \in 1+m_F$. Alors, $x \in F$ puisque $u \in F$, ce qui prouve que $K_1 = K_2$. □

2.2.5 Extensions galoisiennes

Le cas particulier des extensions galoisiennes nous permet de définir les groupes d'inertie et d'inertie sauvage. On voit le lien entre groupe de Galois de l'extension et groupe de Galois de l'extension correspondante sur les corps résiduels.

Si L est une extension galoisienne finie de F, et si $\sigma \in Gal(L/F)$, alors $v(\sigma(x)) = v(x)$ pour tout $x \in L$, et donc $\sigma(O_L) = O_L$, $\sigma(m_L) = m_L$, et σ passe au quotient : on a une application naturelle de $Gal(L/K)$ dans $Aut_{k_F}(k_L)$, qui est de plus un morphisme de groupes.

Définition 2.2.7. On appelle *sous-groupe d'inertie* de $Gal(L/F)$ le noyau $I_{L/F}$ de l'application naturelle de $Gal(L/F)$ sur $Aut_{k_F}(k_L)$. Par définition, c'est un sous-groupe distingué de $Gal(L/F)$.

Proposition 2.2.8. *Soit L une extension finie de F telle que k_L/k_F soit séparable.*
(i) Si L/F est galoisienne, alors k_L est une extension galoisienne de k_F.
(ii) Si L/F est non ramifiée, et si k_L/k_F est galoisienne, alors L/F est aussi galoisienne, et on a $Gal(F(k)/F) \simeq Gal(k/k_F)$.
(iii) Si L/F est galoisienne, alors l'application naturelle $Gal(L/F) \to Gal(k_L/k_F)$ est surjective, et le corps fixé par le sous-groupe d'inertie $I_{L/F}$ est $F(k_L)$.

Démonstration. Pour le (i), nous devons montrer que k_L/k_F est normale. Pour cela, nous allons montrer que cette extension est un corps de décomposition d'un polynôme irréductible.

Supposons que L/F est galoisienne. k_L/k_F est séparable, et on peut donc prendre $\overline{\alpha} \in k_L$ un élément primitif de k_L/k_F. Soit $\overline{P} \in k_F[X]$ son polynôme minimal (unitaire, il est irréductible), soit $P \in O_F[X]$ unitaire dont la réduction modulo m_F est $\overline{P}$, et,vu la démonstration du théorème sur l'extension non ramifiée d'un (sur)corps résiduel donné, soit $\alpha \in F(k_L) \subset L$ une racine de P se réduisant sur $\overline{\alpha}$ modulo m_L. L'extension L/F est supposée galoisienne, donc P se décompose sur L sous la forme $P(X) = (X-\alpha_1)\dots(X-\alpha_f)$. P est par définition, unitaire à coefficients entiers, donc, comme vu plus haut, ses racines sont de valuation positive, et donc les réduction $\overline{\alpha_i}$ des α_i modulo m_L sont des racines de $\overline{P}$. Ainsi, $\overline{P}$ se décompose sur k_L, et ceci permet de montrer que k_L est le corps de décomposition de $\overline{P}$, et donc l'extension k_L/k_F est galoisienne.

Réciproquement, pour le point (ii), si on suppose que L/F est non ramifiée et k_L/k_F est galoisienne $\overline{P}$ défini comme plus haut se décompose sur k_L, sous la forme $\overline{P}(X) = (X-\overline{\alpha_1})\dots(X-\overline{\alpha_f})$, et de plus, si $P \in O_F[X]$ relève $\overline{P}$, on a vu que (par Hensel), pour tout i, il existe $\alpha_i \in F(k_L) = L$ (car extension non ramifiée)

relevant $\overline{\alpha_i}$, tel que $P(X) = (X - \alpha_1)\dots(X - \alpha_f)$, et $F(\alpha_1) = L$. Alors P est irréductible (par critère de réduction), et se décompose dans $L = F(\alpha_1)$, donc L est un corps de décompositino d'un polynôme irréductible, et L/F est bien galoisienne. L'application naturelle $Gal(L/F) \to Gal(k_L/k_F)$ qui à une permutation des α_i associe une permutation des $\overline{\alpha_i}$ est clairement un isomorphisme.

Enfin, pour le (iii), ce qui précède montre que $Gal(F(k_L)/F) \simeq Gal(k_L/k_F)$, et on a $Gal(F(k_L)/F) = Gal(L/F)/I_{L/F}$, L/F étant galoisienne.On a alors $Gal(L/F(k_L)) = I_{L/F}$ et $F(k_L) = L^{I_{L/F}}$, par correspondance de Galois. □

Proposition 2.2.9. *Si L/F est une extension galoisienne telle que k_L/k_F est séparable, et si $I_{L/F}$ est le sous-groupe d'inertie de $Gal(L/F)$, alors $I_{L/F}$ a un unique p-sous-groupe de Sylow $I^+_{L/F}$, qui est distingué dans $I_{L/F}$ et $Gal(L/F)$.*

Démonstration. On pose $K = L^{I_{L/F}}$. D'après la proposition précèdente, K est l'extension maximale non ramifiée de F contenue dans L, et L/K est galoisienne totalement ramifiée, de groupe de Galois $I_{L/F}$. Les p-sous-groupes de Sylow de $I_{L/F}$ correspondent donc, via correspondance de Galois, aux extensions de K contenues dans L, et de degré premier à p. Hors, on a vu dans le paragraphes "extensions modérément ramifiées" qu'il n'y a qu'une unique telle extension de degré maximal. On en déduit que le groupe $I_{L/F}$ n'a qu'un seul p-sous-groupe de Sylow. On le notera $I^+_{L/F}$, et il est distingué dans $I_{L/F}$ (et même caractéristique), en tant qu'unique p-sous-groupe de Sylow.

Si $g \in Gal(L/F)$, alors $gI^+_{L/F}g^{-1}$ est un p-groupe contenu dans $I_{L/F}$ puisque $I_{L/F}$ est distingué dans $Gal(L/F)$. Il est donc inclus dans $I^+_{L/F}$ puisque $I^+_{L/F}$ est l'unique p-Sylow de $I_{L/F}$, ce qui permet de conclure. □

Définition 2.2.10. Le p-Sylow $I^+_{L/F}$ de $I_{L/F}$ est le sous-groupe d'inertie sauvage.

2.2.6 Conclusion sur la structure des extensions finies

Les théorèmes et propositions précédentes, mises dans l'ordre, permettent de montrer le résultat suivant sur les extensions finies de F.

Théorème 2.2.11. *Si L est une extension finie de F telle que k_L/k_F soit séparable, alors L contient deux sous-extensions $L_0 \subset L_1$ de F qui sont uniquement déterminées par les propriétés suivantes :*

(i) L_0/F est non ramifiée.

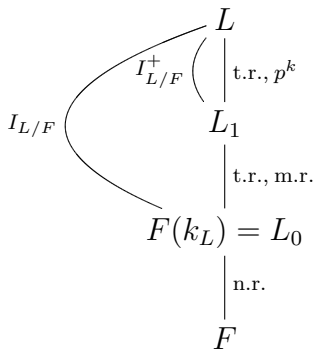
(ii) L/L_1 est totalement ramifiée de degré une puissance de p.

(iii) L_1/L_0 est totalement ramifiée de degré une puissance de p.

De plus, $L_0 = F(k_L)$, et il existe une uniformisante π de L_1 telle que $\pi^{[L_1:L_0]} \in L_0$. Enfin, si L/F est galoisienne, alors $L_0 = L^{I_{L/F}}$ e $tL_1 = L^{I^+_{L/F}}$.

Ceci peut se résumer avec les diagrammes suivants :

Pour L/F avec $\begin{array}{c} k_L \\ \Big\vert \text{sep} \\ k_F \end{array}$ *, on a*



, avec l'action des groupes (à gauche sur le diagramme) seulement si l'extension L/F est galoisienne.

2.3 Énoncé des théorèmes

Le but de ce qui suit dans ce texte va maintenant être de montrer le résultat suivant, but de la théorie du corps de classes, donnant une classification des extensions abéliennes finies d'un corps local de caractéristique nulle K, ainsi que quelques unes de ses conséquences :

Théorème 2.3.1. *L'application*

$$L \mapsto \left\{ \prod_{\sigma \in Gal(L/K)} \sigma(a),\ a \in L \right\} \subset K^*$$

définit une correspondance bijective entre les extensions abéliennes finies de K et les sous-groupes d'indice fini de K^*.

L'intérêt étant qu'on connait assez bien K^* :

Proposition 2.3.2. *On a la décomposition suivante pour K^*, avec π une uniformisante de K, μ_{q-1} le groupe des racines $q-1$-èmes de l'unité de K, et $U_K^{(l)} = 1+\langle\pi\rangle^l$:*

$$K^* = \langle\pi\rangle \times \mu_{q-1} \times U_K^{(1)}.$$

On en déduira aussi :

Théorème 2.3.3 (Kronecker-Weber)**.** *Toute extension abélienne finie $L/\mathbb{Q}$ est contenue dans un corps $\mathbb{Q}(\zeta)$, avec ζ une racine de l'unité.*

Pour montrer ces résultats, on utilisera des outils développés dans la partie suivante, notamment cohomologiques, puis on montrera des résultats généraux, dont l'essence serait aussi utile en théorie du corps de classes globale (pour des corps qui ne sont pas des corps locaux), et enfin on concluera sur les résultats, et leurs applications directes.

3 Quelques outils

3.1 Théorie de Galois infinie

Nous allons définir, si k est un corps et Ω une extension galoisienne de k (finie ou infinie, éventuellement même sa clôture algébrique), $Gal(\Omega/k)$, sa topologie, et voir qu'il est en fait un groupe profini, comme défini en première partie.

3.1.1 Quelques définitions

Définition 3.1.1. On définit $G = Gal(\Omega/k)$ comme le groupe des k-automorphismes de Ω. Sur G, on appelle *topologie de Krull* la topologie définie en prenant comme base de voisinage de $\sigma \in G$ les $\sigma Gal(\Omega/K)$ (aussi notés $\sigma G(\Omega/K)$) où K parcourt les extensions finies galoisiennes K/k de k.

Lemme 3.1.2. *G, muni de la topologie de Krull, est un groupe topologique.*

Démonstration. Pour la multiplication, l'image réciproque du voisinage ouvert de base $\sigma\tau G(\Omega/K)$ de $\sigma\tau$ contient le voisinage ouvert $\sigma G(\Omega/K) \times \tau G(\Omega/K)$ de $\sigma \times \tau$ dans $G \times G$. Donc la multiplication est bien continue.

On procède de même pour l'inverse, avec le fait que l'image réciproque de $\sigma^{-1}G(\Omega/K)$ soit $G(\Omega/K)\sigma$, qui est bien ouvert grâce à la continuité de la multiplication. □

3.1.2 Compacité et correspondance de Galois

Proposition 3.1.3. *Si Ω/k est une extension galoisienne (finie ou infinie), alors le groupe de Galois $G(\Omega/k)$ est compact (séparé) pour la topologie de Krull.*

Démonstration. Si $\sigma, \tau \in G$, tels que $\sigma \neq \tau$, alors il existe K une sous-extension finie de Ω sur k telle que $\sigma_{|K} \neq \tau_{|K}$ (ils différent au moins en un point de Ω, donc ils différent sur le corps engendré par ce point). Ceci veut dire que $\sigma G(\Omega/K) \neq \tau G(\Omega/K)$, et même $\sigma G(\Omega/K) \cap \tau G(\Omega/K) = \emptyset$. En effet, si $x = \sigma g_1 = \tau g_2$ avec $g_i \in G(\Omega/K)$, alors $\tau^{-1}\sigma = g_2 g_1^{-1} \in G(\Omega/K)$ et donc $\tau^{-1}\sigma$ est l'identité sur K, ce qui est absurde. Ceci montre que G est séparé.

Pour montrer la compacité, on considère l'application :

$$h \,:\, G \to \prod_K G(K/k),\ \ \sigma \mapsto \prod_K \sigma_{|K},$$

où K parcours les sous-extensions finies galoisiennes de Ω sur k. Les $G(K/k)$ sont des groupes finis, et ainsi des groupes topologiques compacts. Leur produit est alors, par le théorème de Tychonov, un compact. Le morphisme de groupes h est injectif, étant donné que si $\sigma_{|K} = 1$ pour tout K, alors $\sigma = 1$. Les ensembles

$U = \prod_{K \neq K_0} G(K/k) \times \{\overline{\sigma}\}$, où K_0/k est une sous-extension finie galoisienne de Ω sur k et où $\overline{\sigma} \in G(K_0/k)$, forment une base de voisinages ouverts dans le produit $\prod_K G(K/k)$. Si $\sigma \in G$ est relève $\overline{\sigma}$ dans G, alors $h^{-1}(U) = \sigma G(\Omega/K_0)$, ce qui montre que h est continue, et aussi que $h(\sigma G(\Omega/K_0)) = h(G) \cap U$. Ainsi, h est de plus ouverte. Enfin, montrons que $h(G)$ est fermé dans $\prod_K G(K/k)$. Pour cela, on pose, pour chaque paire $L \subset L'$ de sous-extensions galoisiennes finies de Ω sur k,

$$M_{L'/L} = \left\{ \prod_K \sigma_K \in \prod_K G(K/k) \diagup (\sigma'_L)_{|L} = \sigma_L \right\}.$$

On a directement $h(G) = \bigcap_{L \subset L'} M_{L'|L}$. Or, si $G(L/k) = \{\sigma_1, \ldots, \sigma_n\}$ et si $S_i \subset G(L'/k)$ est l'ensemble des prolongements de σ_i sur L', alors :

$$M_{L'/L} = \bigcup_{i=1}^{n} \left(\prod_{K \neq L', L} G(K/k) \times S_i \times \{\sigma_i\} \right),$$

et ainsi $M_{L'/L}$ est fermé (union finie de produits de fermés), et ainsi, comme intersection de fermés, $h(G)$ est fermé, et c'est donc un compact de $\prod_K G(K/k)$.

Ainsi, h est un homéomorphisme de G sur le compact $h(G)$, et donc G est compact. □

Théorème 3.1.4. *Soit Ω/k une extension galoisienne de k (finie ou infinie). Alors l'application $K \mapsto G(\Omega/K)$, de l'ensemble des sous-extensions de Ω sur k dans l'ensemble des sous-groupes de $G(\Omega/k)$, définie une correspondance bijective entre les sous-extensions K/k de Ω/k et les sous-groupes fermés de $G(\Omega/k)$. De plus, les sous-groupes ouverts de $G(\Omega/k)$ correspondent aux sous-extensions finies de Ω/k.*

Démonstration. On remarque tout d'abord qu'un sous-groupe ouvert A de $G(\Omega/k)$ est aussi fermé. En effet, les σA, $\sigma \in G$, avec $\sigma \in G(\Omega/k) \setminus A$ sont ouverts et leur union est le complémentaire de A dans $G(\Omega/k)$. Par ailleurs, si K/k est une sous-extension finie de Ω sur k, alors $G(\Omega/K)$ est ouvert, car tout $\sigma \in G(\Omega/K)$ admet pour voisinage ouvert $\sigma G(\Omega/N) \subset G(\Omega/K)$, où N/k est la clôture normale de K/k (extension finie).

Si K/k est une sous-extension de Ω/k, alors

$$G(\Omega/K) = \bigcap_i G(\Omega/K_i),$$

avec K_i/k parcourant les sous-extensions finies de K/k. Ainsi, $G(\Omega/K)$ est fermé.

Maintenant, considérons l'application définie dans l'énonce, $K \mapsto G(\Omega/K)$. Cette application est injective car si $G = G(\Omega/K)$ pour un K donné, alors $K = \Omega^G$ par correspondance de Galois.

Pour ce qui est de la surjectivité, montrons que si H est un sous-groupe fermé de $G(\Omega/k)$, alors $H = Gal(\Omega/\Omega^H)$. Déjà, on a $H \subset Gal(\Omega/\Omega^H)$. Réciproquement, si $\sigma \in Gal(\Omega/\Omega^H)$, si L est une extension galoisienne finie intermédiaire entre Ω^H et Ω, alors $\sigma G(\Omega/L)$ est un voisinage ouvert de σ dans $G(\Omega/\Omega^H)$. Montrons que l'application $\phi : H \to G(L/\Omega^H)$, $a \mapsto a|_L^L$, est surjective. Pour cela on remarque que $\phi(H)$ a Ω^H comme corps fixe, donc par correspondance de Galois (on considère des extensions finies), $\phi(H) = G(L/\Omega^H)$.

On peut alors prendre $\tau \in H$ tel que $\tau_{|L} = \sigma_{|L}$, et on a $\tau \in H \cap \sigma G(\Omega/L)$ car $\tau \in H$ et $\tau\sigma^{-1}$ fixe L. Ainsi tout voisinage ouvert de σ rencontre H, et donc σ est dans la fermeture de H, c'est-à-dire dans H car H est supposé fermé, et ainsi, on a montré que $H = G(\Omega/K)$.

Maintenant, si H est un sous-groupe ouvert de $G(\Omega/k)$, alors il est aussi fermé, avec ce qui précéde, et donc de la forme $H = G(\Omega/K)$. Or, $G(\Omega/k)$ est l'union disjointe des classes d'équivalence modulo H, de la forme σH. Il n'y en a qu'un nombre fini car elles forment un recouvrement ouvert de $G(\Omega/k)$, qui est compact. Ainsi, $H = G(\Omega/k)$ est d'indice fini dans $G(\Omega/k)$, ce qui implique que K/k est de degré fini. Réciproquement, une extension finie correspondra bien à un sous-groupe ouvert, car elle correspondra de la même manière à un groupe d'indice fini. □

3.1.3 Groupes de Galois et groupes profinis

Proposition 3.1.5. *Le groupe de Galois $G = G(\Omega/k)$ d'une extension galoisienne Ω/k est un groupe profini. On a $G(\Omega/k) = \lim_{\leftarrow} G(K/k)$.*

Démonstration. En effet, on a vu que G est compact, et si K/k parcour les sous-extensions galoisiennes finies de Ω/k, alors les sous-groupes distingués de $G(\Omega/K)$ forment une base de voisinages ouverts de l'élément neutre. De plus, comme $G/G(\Omega/K) = G(K/k)$, on a : $G(\Omega/k) = \lim_{\leftarrow} G(K/k)$. □

Nous allons voir le cas particulier de $G(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.

Proposition 3.1.6. *On a $G(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \widehat{\mathbb{Z}}$.*

Démonstration. Pour tout $n \in \mathbb{N}^*$, on a un isomorphisme canonique $G(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$, qui envoie l'automorphisme de Frobenius $\phi \in \overline{\mathbb{F}_p}$ sur $1 \in \widehat{\mathbb{Z}}$. Vu la définition de $\widehat{\mathbb{Z}}$, ceci permet de conclure. De plus, le groupe $\langle\phi\rangle$ est naturellement envoyé sur le sous-groupe (dense) $\mathbb{Z}$ de $\widehat{\mathbb{Z}}$. □

3.2 G-modules

Ici, nous allons définir les objets de base et donner les premières propriétés concernant la notion de G-module, permettant de développer les groupes de coho-

mologie H^0 et H^1 qui interviendront de manière cruciale au fil de notre démonstration.

3.2.1 Quelques définitions

Soit G un groupe, dont on notera 1 le neutre.

Définition 3.2.1. Soit A un groupe abélien. A est un *G-module* si on a une action de G sur A vérifiant :
(i) $\forall a \in A,\ 1a = a$.
(ii) $\forall \sigma \in G,\ \forall a, b \in A,\ \sigma(a+b) = \sigma a + \sigma b$.
(iii) $(\sigma\tau)a = \sigma(\tau a)$.
On définit le *module invariant* d'un G-module A comme le sous-groupe de A :

$$A^G = \{a \in A / \sigma a = a,\ \forall \sigma \in G, \forall a \in A\}.$$

A est appelé un G-module *trivial* si $A = A^G$.

Si G est un groupe profini, alors nous ajoutons la condition de continuité suivante :
(iv) $A = \bigcup_U A^U$, où U parcourt les sous-groupes ouverts de G.

Remarque. Cette dernière condition est équivalente au fait que l'action soit continue, pour A muni de la topologie discrète. En effet, ceci signifie que l'application $h : G \times A \to A$, $(\sigma, a) \mapsto \sigma a$ est continue, ce qui revient au fait que : pour tout $(\sigma, a) \in G \times A$, il existe un sous-groupe ouvert $U \subset G$ tel que $\sigma U \times \{a\} \subset h^{-1}(\{\sigma a\}$, ce qui se réécrit simplement en $a \in A^U$.

Définition 3.2.2. On appelle *G-homomorphisme*, entre A et B deux G-modules, un morphisme de groupes abéliens $f : A \to B$ tel que : $\forall \sigma \in G,\ \forall a \in A,\ f(\sigma a) = \sigma f(a)$.

On notera $Hom_G(A, B)$ le groupe des G-homomorphismes de A dans B.

Définition 3.2.3. Si G est un groupe fini, alors tout G-module A contient le *groupe des normes* :

$$N_G A = \left\{ N_G a = \sum_{\sigma \in G} \sigma a / a \in A \right\}.$$

On appelera *norme* de a l'élément $\sum_{\sigma \in G} \sigma a$, mais le terme *trace* est parfois utilisé.

Remarque. Si $a \in A$, $\tau \in G$, alors $\tau N_G a = \sum_{\sigma \in G} \tau\sigma a = N_G a$, et ainsi on a bien $N_G A \subset A^G$.

Définition 3.2.4. On appelle alors *groupe résiduel des normes*, ou groupe de cohomologie d'ordre 0 du G-module A, le quotient :

$$H^0(G, A) = A^G/N_G A.$$

Ce dernier aura un rôle primordial dans la suite. Nous allons aussi définir un groupe de cohomologie d'ordre 1.

Définition 3.2.5. Tout d'abord, on appelle *homomorphisme croisé* (ou 1-cocycle) une application $f : G \to A$ telle que

$$\forall \sigma, \tau \in G,\ f(\sigma\tau) = f(\sigma) + \sigma f(\tau).$$

Les homomorphismes croisés de A forment un groupe abélien, noté $Z^1(G, A)$.

On remarque que pour tout $a \in A$, l'application

$$f_a : G \to A,\ \sigma \mapsto f_a(\sigma) = \sigma a - a,$$

est un homomorphisme croisé : $f_a(\sigma\tau) = (\sigma\tau)a - a = \sigma(\tau a - a) + \sigma a - a = f_a(\sigma) + \sigma f_a(\tau)$. L'ensemble des fonctions f_a, $a \in A$ forme un sous-groupe de $Z^1(G, 1)$, noté $B^1(G, A)$, appelé groupe des 1-cobords, et on définit le premier groupe de cohomologie par :

$$H^1(G, A) = Z^1(G, A)/B^1(G, A).$$

3.2.2 Quelques suites exactes

Le comportement des groupes de cohomologie par rapport aux suites exacts sera crucial, en particulier par le théorème suivant, qui permet de déduire une suite exacte "longue" d'une suite exacte courte.

Proposition 3.2.6. *Si $0 \to A \to^i B \to^j C \to 0$ est une suite exacte de G-modules (et G-homomorphismes), alors on a la suite exacte :*

$$0 \to A^G \to^i B^G \to^j C^G \to^\delta H^1(G, A) \to^{i_*} H^1(G, B) \to^{j_*} H^1(G, C).$$

Démonstration. On va d'abord identifier A à son image, et ainsi i devient une inclusion. La définition de G-homomorphisme donne déjà directement le fait que les applications i et j de la deuxième suite sont bien définies. L'exactitude en A^G est immédiate, comme on ne fait que restreindre i. De même, l'exactitude en B^G est directe : $Ker(j) \cap B^G = Im(i) \cap B^G = A \cap B^G = A^G$. Regardons maintenant la définition de δ et l'exactitude en C^G. Soit $c \in C^G$ et soit $b \in B$ tel que $j(b) = c$ (bien défini du fait que j est surjective). Alors $j(\sigma b - b) = \sigma c - c = 0$, c'est-à-dire $\sigma b - b \in A$. Soit $f : G \to A$, $\sigma \mapsto f(\sigma) = \sigma b - b$. C'est un homomorphisme croisé,

et on définit, si $c \in C^G$, $\delta(c) = f \bmod B^1(G,A)$. $\delta(c)$ n'est pas un 1-cobord en génétal car on a *a priori* $b \in B$ et pas nécessairement $b \in A$.

L'application $\delta : c \mapsto \delta(c)$, $C^G \to H^1(G,A)$ est bien définie. En effet, si $b' = b + a$, avec $a \in A$, est un autre antécédent de c, alors l'homomorphisme croisé $f'(\sigma) = \sigma b' - b' = f(\sigma) + \sigma a - a = f(\sigma) + f_a(\sigma)$ ne différe de f que d'un 1-cobord de A. Maintenant, si c est tel que $\delta c = 0$, alors $f(\sigma) = \sigma b - b = \sigma a - a$ pour un certain $a \in A$, et ainsi $\sigma(b-a) = b - a$, c'est-à-dire $b - a = b' \in B^G$, et $j(b') = j(b) = c$, et $c \in j(B^G)$. Réciproquement, si $c \in j(B^G)$, alors $c = j(b)$ pour un certain $b \in B^G$, et donc $\forall \sigma \in G$, $\sigma b - b = 0$, ce qui veut dire que $\delta c = 0$. On a donc bien montré l'exactitude en C^G.

Montrons l'exactitude en $H^1(G,A)$. On va noter i_* la composition par i à gauche, qui envoie $H^1(G,A)$ dans $H^1(G,B)$, et on fera de même pour j. Tout d'abord, on a $i_* \circ \delta(c) = i \circ f$ avec $f : \sigma \mapsto \sigma b - b$, $G \to A$, avec $b \in B$ tel que $c = j(b)$. Soit $\sigma \in G$, alors $i \circ f(\sigma) = i(\sigma b - b) = \sigma b - b$ car i est l'inclusion. Donc $i_* \circ \delta(c) = 0$ dans $H^1(G,B)$, et $i_* \circ \delta = 0$.

Réciproquement, si $f \in H^1(G,A)$ est tel que $i_*(f) = 0$, alors pour un certain $b \in B$, i étant l'inclusion, soit $\sigma \in G$, on a : $f(\sigma) = i \circ f(\sigma) = \sigma b - b$. Posons $c = j(b)$, alors $f = \delta(c)$, et on a bien l'exactitude.

Enfin, pour la dernière exactitude à montrer, soit $f \in H^1(G,A)$, alors, pour $\sigma \in G$, $j_* \circ i_*(f)(\sigma) = j \circ i \circ f(\sigma)$ et $j \circ i = 0$ dans C, donc $j \circ i(f)(\sigma) = 0$ et $j_* \circ i_*(f) = 0$. Réciproquement, si $f \in H^1(G,B)$ tel que $j \circ f = 0$ dans $H^1(G,C)$, alors il existe $c \in C$ tel que si $\sigma \in G$, on a $j \circ f(\sigma) = \sigma c - c$. j est surjectif, donc il existe $b \in B$ tel que $c = j(b)$. Mais alors on $j(f(\sigma) - \sigma b + b) = 0$ donc $f(\sigma) - \sigma b + b \in A$. Mais alors, dans $H^1(G,B)$, $f = i \circ u$ avec $u \in H^1(G,A)$, tel que $u(\sigma) = f(\sigma) - \sigma b + b$. Ceci permet de conclure sur l'exactitude en $H^1(G,B)$, et clôt la démonstration. □

Remarque. En fait, si l'on définit les groupes de cohomologie supérieure, la "suite exacte longue" se poursuit avec tout les groupes de cohomologie supérieure.

Remarque. Si g est un sous-groupe de G, alors tout G-module est aussi un g-module. Mais si g est distingué, alors de plus, A^g est un G/g-module.

Ceci nous amène à l'existence de la suite exacte suivante :

Proposition 3.2.7. *Si g est un sous-groupe distingué de G, et si A est un G-module, alors on a la suite exacte :*

$$0 \to H^1(G/g, A^g) \to H^1(G,A) \to H^1(g,A).$$

Démonstration. La flèche de gauche est définie ainsi : si $\overline{f} : G/g \to A^g$ est un homomorphisme croisé, alors la composée $f : G \to^{can} G/g \to^{\overline{f}} A$ est un homomorphisme croisé de G, avec *can* la surjection canonique de G dans G/g. Il n'y a ensuite pas de souci pour passer au quotient par les B^1.

Si $\overline{f}$ est tel que $f(\sigma) = \sigma a - a$ pour un certain $a \in A$, alors si $\overline{\sigma} = \sigma \mod g$, on a par définition $\overline{f}(\overline{\sigma}) = f(\sigma) = \sigma a - a \in A^g$. Mais si $\tau \in g$, $f(\sigma\tau) = f(\sigma) = \overline{f}(\overline{\sigma})$, donc $\sigma\tau a - a = \sigma a - a$ donc $a = \tau a$ et $a \in A^g$, ce qui montre bien que $\overline{f} = 0$ dans $H^1(G/g, A^g)$. Ainsi, la flèche de gauche est bien injective.

Pour ce qui est de la flèche de droite, on l'obtient par restriction des homomomophismes croisés $G \to A$ à g, ils deviennent des homomorphismes croisés $g \to A$ et il n'y a pas de problème pour passer au quotient.

Pour l'exactitude, soit $\overline{f} \in H^1(G/g, A^g)$, et $f \in H^1(G, A)$ obtenu par la flèche de droite. Alors en restreignant f à g, on tombe bien sur 0 (avant de quotienter, dans Z^1, on a $f \circ can_{|g}$ et $can_{|g} = 0$). Réciproquement, si $f \in H^1(G, A)$ est tel que $f(\tau) = \tau a - a$ pour un certain $a \in A$ et tout $\tau \in g$, alors l'homomorphisme croisé $f' : f'(\sigma) = f(\sigma) - (\sigma a - a)$ est dans la même classe modulo $B^1(G, A)$ que f, et ne dépend, modulo $B^1(g, A)$ que de la classe de σ modulo g, comme $f'(\sigma\tau) = f'(\sigma)$ pour tout $\tau \in g$. En effet, $f'(\sigma\tau) = f(\tau) + \sigma f(\tau) - (\tau\sigma a - a) = f(\sigma) + \sigma\tau a - \sigma a - \tau\sigma a + a = f'(\sigma)$. De plus, $f'(\sigma) \in A^g$ puisque $f'(\sigma) = f'(\tau\sigma) = \tau f'(\sigma)$. En effet, classes à gauche et à droite modulo g sont les mêmes (g est distingué dans G), et $f'(\tau\sigma) = f(\tau) + \tau f(\sigma) - (\tau\sigma a - a) = \tau f(\sigma) - \tau(\sigma a - a) = \tau f'(\sigma)$. Ainsi, f' est la composée $G \to^{can} G/g \to^{\overline{f}} a^g$, avec $\overline{f}(\sigma \mod g) = f'(\sigma)$. Ceci conclut la démonstration de l'exactitude de la suite. □

Définition 3.2.8. À chaque g-module B, on associe, de manière canonique, un G-module, appelé *G-module induit*, définit comme suit :

$$A = M_G^g(B) = \{f \ : \ G \to B / \forall \tau \in g, \forall x \in G, f(\tau x) = \tau f(x)\}.$$

L'action de G sur A est définie par : si $\sigma \in G$, $f \in A$, $x \in G$ alors $(\sigma f)(x) = f(x\sigma)$. De plus, on a un g-homomorphisme canonique :

$$\pi \ : \ M_G^g(B) \to B, \ f \mapsto f(1),$$

qui donne un isomorphisme entre B et le sous-g-module de $M_G^g(B)$,

$$B' = \{f \in M_G^g(B) / \forall x \notin g, \ f(x) = 0\}.$$

On identifiera B' et B.

Remarque. Si g est d'indice fini dans G, alors on montre que l'on a l'égalité de G-modules :

$$M_G^g(B) = \bigoplus_{\sigma \in G/g} \sigma B,$$

où la somme sur σ est prise dans un ensemble de représentants de G/g. Si $g = \{1\}$, on notera $M_G(B)$ pour $M_G^g(B)$.

Proposition 3.2.9. *Si g est un sous-groupe d'un groupe fini G, et si B est un g-module, alors on a canoniquement :*

$$H^i(G, M_G^g(B)) \simeq H^i(g, B),\ i = 0, 1.$$

Démonstration. On traitera d'abord le cas $i = 0$, puis le cas $i = 1$. Soit $A = M_G^g(B)$. Si $f \in A^G$, alors $f(\sigma) = f(1)$ pour tout $\sigma \in G$, et $f(1) = f(\tau) = \tau f(1)$ pour tout $\tau \in g$. Ceci montre que $\pi : A \to B$ induit un isomorphisme $\pi : A^G \to B^g$, $f \mapsto f(1)$ ($f \in A^G$ est entièrement déterminé par sa valeur en 1, et tout $y \in B^g$ permet de définir un $f \in A^G$ avec $f(1) = y$).

Montrons alors que π envoie isomorphiquement $N_G A$ sur $N_g B$. Soit $f \in A$ et $h = N_G f \in N_G A$. Soit σ_i un ensemble de représentants de G/g, alors :

$$h(1) = \sum_{\tau \in g} \sum_i (\tau \sigma_i f)(1) = \sum_{\tau \in g} \sum_i f(\tau \sigma_i) = \sum_{\tau \in g} \tau \left(\sum_i f(\sigma_i) \right) \in N_g B.$$

Ainsi, $\pi(N_G A) \subset N_g B$. Réciproquement, soit $N_g b \in N_g B$, avec $b \in B$, et soit $f \in A$ tel que $f(x) = 0$ pour tout $x \notin g$ et $f(\tau) = \tau b$ pour $\tau \in g$. Si on pose $h = N_G f$, alors :

$$h(1) = \sum_{\sigma \in G} (\sigma f)(1) = \sum_{\tau \in g} f(\tau) = \sum_{\tau \in g} \tau b = N_g b.$$

Ainsi, on a bien le fait que π envoie isomorphiquement $N_G A$ sur $N_g B$. Ceci permet de conclure pour l'isomorphisme canonique, par π, concernant les H^0.

Nous allons maintenant montrer le résultat pour le cas $i = 1$. Par définition de $Z^1(G, A)$ et $M_G^g(B)$, $Z^1(G, A)$ est constitué des fonctions $\gamma : G \times G \to B$ telles que :

(i) $\gamma(x, \tau y) = \tau \gamma(x, y)$ pour $\tau \in g$ (pour le fait que $\gamma(x, \cdot)$ soit dans $M_G^g(B)$).

(ii) $\gamma(xy, z) = \gamma(x, z) + \gamma(y, zx)$ (pour avoir un homomorphisme croisé, tout en utilisant la définition de l'action sur $M_G^g(B)$).

Les $\gamma \in B^1(G, A)$ sont ceux tels que $\gamma(x, z) = f(zx) - f(z)$ avec $f \in A$. Si on considère l'application :

$$\rho : Z^1(G, A) \to Z^1(g, B),\ \gamma(x, z) \mapsto \overline{\gamma}(x) = \gamma(x, 1),$$

alors celle-ci est bien définie, avec les propriétés (i) et (ii). De plus, elle est surjective. En effet, soit $\beta \in Z^1(g, B)$ et soit σ_k un système de représentants de G/g. On étend β en une application $\beta : G \to$ en posant $\beta(\tau \sigma_k) = \beta(\tau)$, pour $\tau \in g$. Alors on a directement $\beta(\tau x) = \tau \beta(x) + \beta(\tau)$ pour $\tau \in g$ et $x \in G$. On vérifie alors que la fonction $\gamma(x, z) = \beta(zx) - \beta(z)$ satisfait les conditions (i) et (ii), et donc est dans $Z^1(G, A)$. Comme $\gamma(x, 1) = \beta(x) - \beta(1) = \beta(x)$, alors ρ est bien surjective.

Il reste à montrer que l'image réciproque de $B^1(g,B)$ par ρ est $B^1(G,A)$. Si $\gamma(x,z) = f(zx) - f(z)$ est une fonction de $B^1(G,A)$, alors son image par ρ est la fonction $\overline{\gamma}(x) = f(x) - f(1) = xf(1) - f(1)$ qui est donc dans $B^1(g,B)$. Réciproquement, si $\gamma \in Z^1(G,A)$ est envoyé dans $B^1(g,B)$ par ρ, alors on a $\gamma(x,1) = xb - b$ pour $x \in g$. Ainsi, $f(x) = \gamma(x,1) + b$ est une fonction dans $M_G^g(B)$. Alors $\gamma(x,z) = \gamma(zx,1) - \gamma(z,1) = f(zx) - f(z)$. Ainsi, $\gamma \in B^1(G,A)$, et on peut conclure sur la démonstration du résultat. □

3.2.3 Le quotient de Herbrand

Un autre outil important concernant nos considérations cohomologiques est le quotient de Herbrand, concernant en particulier les groupes de cohomologie d'ordre -1.

Dans tout ce paragraphe, G est un groupe cyclique fini, et σ est un générateur de G.

Définition 3.2.10. Si A est un G-module, alors on définit $H^{-1}(G,A)$ par :

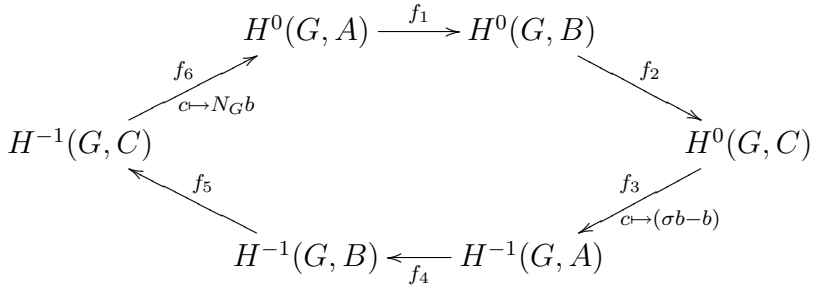
$$H^{-1}(G,A) = {}_{N_G}A / I_G A,$$

avec

$$ {}_{N_G}A = \{a \in A \diagup N_G a = 0\}$$
$$ I_G A = \{\sigma a - a \diagup a \in A\},$$

qui est clairement un sous-groupe distingué de ${}_{N_G}A$.

Proposition 3.2.11. *Si* $0 \to A \to^i B \to^j C \to 0$ *est une suite exacte de* G*-modules, alors on a l'hexagone exact suivant :*



Démonstration. Les morphismes f_1 et f_2 sont directement induits par les morphismes i et j. De la même manière, les morphismes f_4 et f_5 sont aussi induits par i et j. Pour simplifier, on identifiera A avec son image dans B par l'injection i, et i devient une inclusion.

Définissons maintenant f_3.

Soit $c \in C^G$ et soit $b \in B$ tel que $j(b) = c$ (j est surjective). Alors $j(\sigma b - b) = \sigma c - c = 0$ donc $\sigma b - b \in Ker j = A$, et $N_G(\sigma b - b) = N_G(\sigma b) - N_G(b) = 0$ et ainsi

$\sigma b - b \in {}_{N_G}A$. On pose alors $f_3 : c \mod N_G C \mapsto (\sigma b - b) \mod I_G A$. f_3 est bien défini : il ne dépend pas de b car si $b' = b + a$ (on a $Kerj = A$), $\sigma a - a \in I_G A$, et il ne dépend pas du choix du représentant modulo $N_G(C)$. En effet, si $c = \sum_{\tau \in G} \tau c'$, alors $c = j(b)$ avec $b = \sum_{\tau \in G} \tau b'$) et $j(b') = c'$. On a alors clairement $\sigma b - b = 0$.

Pour ce qui est de f_6, soit $c \in {}_{N_G}C$ et soit $b \in B$ tels que $j(b) = c$. Alors $j(N_G b) = N_G c = 0$ et donc $N_G b \in kerj = A$. De plus, $\sigma N_G b = N_G b$ (vu la définition de N_G), donc $N_G b \in A^G$. On pose ainsi $f_6 : c \mod I_G C \mapsto N_G b \mod N_G A$. On montre de même, directement, que f_6 est bien défini.

Prouvons maintenant l'exactitude en $H^0(G, A)$. Soit $a \in A^G$ tel que $f_1(a \mod N_G A) = 0$, c'est-à-dire $a = N_G b$ avec $b \in B$. On pose $c = j(b)$ et on a $f_6(c \mod I_G C) = a \mod N_G A$, avec ce qui précède. De plus, vu la définition de f_6, $f_6(c)$ est une norme de B, donc on a bien $f_1 \circ f_6 = 0$, ce qui montre l'exactitude à $H^0(G, A)$.

L'exactitude en $H^0(G, B)$ est immédiate avec l'exactitude de la suite exacte initiale.

Pour l'exactitude à $H^0(G, C)$, si $b \mod N_G B \in H^0(G, B)$, alors $f_2(b \mod N_G B) = j(b) \mod N_G(C)$, et $f_3 \circ f_2(b \mod N_G B) = \sigma b - b \mod I_G A = 0 \mod I_G A$. Par ailleurs, si $c \mod N_G(C) \in ker(f_3)$, avec $\sigma c = c$ et $c = j(b)$ pour un $b \in B$, alors $f_3(c \mod N_G(C)) = 0 = \sigma b - b \mod I_G A$. Mais alors il existe $a \in A$ tel que $\sigma b - b = \sigma a - a$, d'où $b - a \in B^G$. Comme $j(a) = 0$ car $a \in A$, on a $j(b - a) = c$ et donc on en déduit que $c \mod N_G C = f_2(b - a \mod N_G B)$.

Considérons maintenant l'exactitude à $H^{-1}(G, A)$. Soit $a \in {}_{N_G}A$ tel que $f_4(a \mod I_G A) = 0$, c'est-à-dire $a = \sigma b - b$, pour un $b \in B$. Posons $c = j(b)$, on voit alors que $f_3(c \mod N_G C) = a \mod I_G A$, vu la définition de f_3. Réciproquement, f_4 envoie tout $(\sigma b - b) \mod I_G A$, $b \in B$ sur $0 \mod I_G B$, ce qui montre l'exactitude à $H^{-1}(G, A)$.

L'exactitude en $H^{-1}(G, B)$ est aussi immédiate avec l'exactitude de la suite exacte initiale.

Enfin, pour l'exactitude en $H^{-1}(G, C)$, soit $b \mod I_G B \in H^{-1}(G, B)$, $b \in {}_{N_G}B$. Alors $f_5(b \mod I_G B) = j(b) \mod I_G C$ et $f_6 f_5(b \mod I_G B) = N_G b \mod N_G A$, or $b \in {}_{N_G}B$ donc $N_G b = 0$, et on a bien $f_6 \circ f_5 = 0$. Réciproquement, si $c \in {}_{N_G}C$ est tel que $f_6(c \mod I_G C) = 0 \mod N_G A$, alors soit $b \in B$ tel que $c = j(b)$, étant donné que $kerj = A$, on a $n_G b = N_G a$, pour un certain $a \in A$. Mais alors, $N_G(b - a) = 0$ et $c = j(b - a)$ donc $b - a \in {}_{N_G}B$ et $c = f_5(b - a)$.

On a ainsi montré que l'hexagone était exact, ce qu'il fallait démontrer. □

Nous allons maintenant introduire la notion de quotient d'Herbrand :

Définition 3.2.12. Si G est un groupe cyclique fini, et si A est un G-module, alors le *quotient de Herbrand* de A est défini par :

$$h(G,A) = \frac{\sharp H^0(G,A)}{\sharp H^{-1}(G,A)},$$

lorsque les ordres de ces deux groupes sont finis.

La puissance du quotient de Herbrand vient en particulier de son caractère multiplicatif par rapport aux suites exactes.

Proposition 3.2.13. *Si $0 \to A \to B \to C \to 0$ est une suite exacte de G-modules, alors*

$$h(G,B) = h(G,A)h(G,C)$$

au sens où si deux de ces quotients de Herbrand sont bien définis, alors le troisième l'est aussi et on a bien l'égalité. De plus, si A est un G-module fini, alors $h(G,A) = 1$.

Démonstration. On considère l'hexagone exact de la proposition précédente. Si on note $n_i = \sharp Im(f_i)$, alors, par exactitude de l'hexagone, on a $\frac{\sharp H^0(G,B)}{\sharp ker f_2} = n_2 = \frac{\sharp H^0(G,B)}{\sharp im f_1} = \frac{\sharp H^0(G,B)}{n_1}$. On fait de même pour les autres sommets du diagramme et on obtient : $\sharp H^0(G,A) = n_6 n_1$, $\sharp H^0(G,B) = n_1 n_2$, $\sharp H^0(G,B) = n_2 n_3$, $\sharp H^{-1}(G,A) = n_3 n_4$, $\sharp H^{-1}(G,B) = n_4 n_5$ et $\sharp H^{-1}(G,C) = n_5 n_6$.

Ainsi, $\sharp H^0(G,A) \times \sharp H^{-1}(G,B) \times \sharp H^0(G,C) = \sharp H^0(G,B) \times \sharp H^{-1}(G,A) \times \sharp H^{-1}(G,C)$. On en déduit donc que lorsque deux des quotients $h(G,A)$, $h(G,B)$, ou $h(G,C)$ sont définis, alors le troisième l'est aussi, et on obtient bien l'égalité voulue.

De plus, si A est un G-module fini, alors on a les suites exactes :

$$0 \to A^G \to A \to^f I_G A \to 0,$$

$$0 \to {}_{N_G}A \to A \to^g N_G A \to 0$$

,

avec $f(a) = \sigma a - a$ et $g(a) = N_G(a)$. On en déduit que $\sharp A = \sharp A^G \times \sharp I_G A = \sharp_{n_G} A \times \sharp N_G A$, et ainsi, que $h(G,A) = 1$. □

Proposition 3.2.14. *Si G est un groupe fini cyclique, alors $H^1(G,A) \simeq H^{-1}(G,A)$.*

Démonstration. Soit σ un générateur de G, et soit n l'ordre de g. Si $f \in Z^1(G,A)$ est un homomorphisme croisé, alors pour $k \geqslant 1$,

$$f(\sigma^k) = \sigma f(\sigma^{k-1}) + f(\sigma) = \sigma^2 f(\sigma^{k-2}) + \sigma f(\sigma) + \sigma = \sum_{i=0}^{k-1} \sigma^i f(\sigma)$$

et $f(1) = 0$ car $f(1) = f(1) + f(1)$ (avec $\sigma = 1$).

Ainsi, comme G est cyclique d'odre n,

$$N_G f(\sigma) = \sum_{i=0}^{n-1} \sigma^i f(\sigma) = f(\sigma^n) = f(1) = 0.$$

Alors, $f(\sigma) \in {}_{N_G}A$. De plus, si $a \in {}_{N_G}A$, on obtient un homomorphisme croisé f en posant $f(\sigma) = a$ et

$$f(\sigma^k) = \sum_{i=0}^{k-1} \sigma^i a.$$

L'application $f \mapsto f(\sigma)$ est alors un isomorphisme entre $Z^1(G, A)$ et ${}_{N_G}A$. Cet isomorphisme envoie $B^1(G, A)$ sur $I_G A$ car $f \in B^1(G, A)$ si et seulement si $f(\sigma^k) = \sigma^k a - a$ pour un certain $a \in A$, soit si et seulement si $f(\sigma) = \sigma a - a$ (par téléscopage sur la formule de développement de $f(\sigma^k)$ précédente), ce qui revient à dire $f(\sigma) \in I_G A$, et montre le résultat. □

3.3 Théorie de Kummer

Dans cette sous-partie, nous allons étudier les extensions dites de Kummer, pour obtenir un premier résultat de correspondance. Pour cela on commencera par montrer le fameux théorème *Hilbert 90*. Sa démonstration nécessite le lemme suivant :

Lemme 3.3.1 (lemme de Dedekind)**.** *Soient G un groupe et K un corps. Soit $(\sigma_i)_{i\in I}$ une famille d'homomorphismes de groupe de G dans K^* qui sont tous distincts. Alors $(\sigma_i)_{i\in I}$ est une famille libre du K-espace vectoriel K^G des applications de G dans K.*

Démonstration. On procéde par récurrence sur $n \in \mathbb{N}^*$ pour montrer la propriété $P(n)$: "si $\sigma_1, \ldots, \sigma_n$ sont n homomorphismes distincts de G dans K^*, alors $(\sigma_i)_{1\leqslant i\leqslant n}$ est une famille libre de K^G".

Pour ce qui est de $P(1)$, on remarque que si $\lambda \in K$ et $\sigma \in Hom(G, K^*)$ vérifient $\lambda\sigma = 0$, alors $\forall g \in G,\ \lambda\sigma(g) = 0$ donc $\lambda = \lambda\sigma(e) = 0$, et on a le résultat.

Maintenant, supposons $P(n-1)$ pour un certain $n \in \mathbb{N}$, $n \geqslant 2$. Soient $\sigma_1, \ldots, \sigma_n$ n homomorphismes distincts de G dans K^*. Soit $(\lambda_1, \ldots, \lambda_n) \in K^n$ tel que $\sum_{i=1}^n \lambda_i\sigma_i = 0$. On a donc $\forall g \in G, \sum_{i=1}^n \lambda_i\sigma_i(g) = 0$.

On en déduit, compte tenu de la qualité de morphisme des σ_i :

$$\forall (x, y) \in G^2, \sum_{i=1}^n \lambda_i\sigma_i(x)\sigma_i(y) = 0.$$

On peut aussi écrire, par simple multiplication de $0 = \sum_{i=1}^n \lambda_i\sigma_i(x)$ par $\sigma_n(y)$:

$$\forall (x, y) \in G^2, \sum_{i=1}^n \lambda_i\sigma_i(x)\sigma_n(y) = 0.$$

En combinant ces deux égalités, on trouve :

$$\forall (x,y) \in G^2, \sum_{i=1}^{n-1} \lambda_i \sigma_i(x)(\sigma_n(y) - \sigma_i(y)) = 0,$$

ce qui peut se réécrire, comme K est un corps donc commutatif,

$$\forall y \in G, \forall x \in G, \sum_{i=1}^{n-1} \lambda_i (\sigma_n(y) - \sigma_i(y))\sigma_i(x) = 0.$$

Or, d'après $P(n-1)$, $(\sigma_i)_{1 \leqslant i \leqslant n-1}$ est une famille libre du K-espace vectoriel K^G, donc $\forall i \in \{1, \ldots, n-1\}, \forall y \in G, \lambda_i(\sigma_n(y) - \sigma_i(y)) = 0$. Or, pour chaque $i \neq n$, $\sigma_i \neq \sigma_n$, donc $\exists y \in G, \sigma_n(y) - \sigma_i(y) \neq 0$. Ainsi, $\lambda_1 = \cdots = \lambda_{n-1} = 0$. Enfin, comme $\sum_{i=1}^{n} \lambda_i \sigma_i = 0$, alors avec $P(1)$, $\lambda_n = 0$, et on a montré $P(n)$. Par récurrence, on a donc $\forall n \in \mathbb{N}^*, P(n)$.

Au final, si $(\sigma_i)_{i \in I}$ est une famille liée de K^G, alors elle admet une sous-famille finie liée, ce qui est absurde avec ce qui précède.

□

Théorème 3.3.2 ("Hilbert 90"). *Soit L/K une extension Galoisienne finie, de groupe de Galois $G = G(L/K)$. Alors le groupe multiplicatif L^* est un G-module et*

$$H^1(G, L^*) = \{1\}.$$

De plus, si G est cyclique et si σ est un générateur de G, alors tout élément a de L^* de norme $N_{L/K}(a) = 1$ s'écrit :

$$a = \frac{\sigma b}{b}$$

pour un certain $b \in L^*$.

Démonstration. Soit $f : G \to L^*$ un homomorphisme croisé. Pour $c \in L^*$, on pose :

$$\alpha = \sum_{\sigma \in G} f(\sigma)\sigma c.$$

Du fait de l'indépendance linéaire des automorphismes σ, application directe du lemme précédent, $c \in L^*$ peut être choisi tel que $\alpha \neq 0$. On obtient alors pour $\tau \in G$, du fait que $\tau(f(\sigma)\sigma c) = (\tau(f(\sigma)))(\tau\sigma c)$ et $f(\tau\sigma) = f(\tau)\tau f(\sigma)$:

$$\tau\alpha = \sum_{\sigma} \tau f(\sigma)(\tau\sigma c) = \sum_{\sigma} f(\tau)^{-1} f(\tau\sigma)(\tau\sigma c) = f(\tau)^{-1}\alpha.$$

Ainsi, $f(\tau) = \frac{\tau\alpha^{-1}}{\alpha^{-1}}$, et donc $f \in B^1(G, L^*)$, et $H^1(G, L^*) = 1$.

De plus, si G est cyclique, on a vu que $H^{-1}(G, L^*) = H^1(G, L^*) = 1$, donc ${}_{n_G}L^* = I_G L^*$, et ainsi, tout élément $a \in L^*$ avec $N_G a = N_{L/K}(a) = 1$ est de la forme $a = \frac{\sigma b}{b}$ pour un certain $b \in L^*$. □

Maintenant, soit K un corps tel que $X^n - 1$ soit scindé sur K, et soit μ_n le groupe de ses racines n-èmes de l'unité, avec n un entier naturel premier avec la caractéristique de K (si celle-ci est non nulle).

Définition 3.3.3. On appelle *extension de Kummer* de K une extension de la forme

$$L = K(\sqrt[n]{\Delta})$$

où Δ est un sous-groupe de K^* contenant le groupe K^{*n} des puissances n-ème de K. Ainsi, L est engendré par les racines $\sqrt[n]{a}$, $a \in \Delta$.

Remarque. Une extension de Kummer L/K est abélienne d'exposant n, c'est-à-dire qu'elle est galoisienne (pas nécessairement finie), que son groupe de Galois est abélien et que $\sigma^n = 1$ pour tout $\sigma \in G(L/K)$. En fait, pour tout $a \in \Delta$, la sous-extension $K(\sqrt[n]{a})/K$ est cyclique de degré divisant n, donc la restriction de σ^n à $K(\sqrt[n]{a})$ est 1, et ainsi $\sigma^n = 1$ car L est engendré par les racines $\sqrt[n]{a}$.

Réciproquement, on a la proposition suivante :

Proposition 3.3.4. *Si L/K est une extension abélienne d'exposant n, alors $L = K(\sqrt[n]{\Delta})$ avec $\Delta = L^{*n} \cap K^*$.*

Démonstration. Déjà, on a $K(\sqrt[n]{\Delta}) \subset L$. Par ailleurs, nous pouvons d'abord réduire le problème car L/K est la composée de ses sous-extensions cycliques : L/K est la composée de ses sous-extensions finies L'/K et le groupe abélien fini $G(L'/K)$ est le produit direct de groupes cycliques (par le théorème de structure des groupes abéliens finis (ou de type fini)), et chacun de ces sous-groupes cycliques peut être vu comme le groupe de Galois d'une sous-extension cyclique de L'/K. Ainsi, L/K est la composée de ses sous-extensions cycliques.

Soit maintenant M/K une sous-extension cyclique de L/K, alors $G(M/K)$ est d'ordre d divisant n. Soit σ un générateur. Alors, $M = K(\sqrt[n]{a})$ pour un certain $a \in M^{*n} \cap K^*$.

En effet, soit ζ_0 une racine primitive n-ème de l'unité, alors $\zeta = \zeta_0^{\frac{n}{d}} \in K$ donc $N_{M/K}(\zeta) = \zeta^d = 1$. Par le théorème d'Hilbert 90, il existe $c \in M$ tel que $\sigma(c) = c\zeta$. Alors, $\sigma(c^n) = (\sigma(c))^n = c^n\zeta^n = c^n$ donc $c^n \in M^{G(M/K)} = K$. De plus, par récurrence, on montre que $\sigma^i(c) = c\zeta^i$ et donc les $\sigma^i(c)$ sont tous distincts, pour $0 \leqslant i \leqslant d-1$. Par conséquent, le polynôme minimal de c sur K les a tous comme racine, et il est donc de degré $\geqslant d$. Ainsi, $[K(c) : K] \leqslant d$ et $[M : K] = d$ et $M \supset K(c)$, donc $K(c) = M$ et $c^n \in K$. On a donc bien $M \subset K(c) \subset K(\sqrt[n]{\Delta})$. Ainsi $L \subset K(\sqrt[n]{\Delta})$, ce qui permet de conclure. □

Nous pouvons maintenant montrer le théorème de correspondance de Kummer.

Théorème 3.3.5. *Les extensions de Kummer L/K (contenues dans une clôture algébrique donnée) sont en correspondance bijective avec les sous-groupes Δ de K^* contenant K^{*n}. Si $L = K(\sqrt[n]{\Delta})$, alors $\Delta = L^{*n} \cap K^*$ et on a un isomorphisme canonique :*

$$Hom(G(L/K), \mu_n) \simeq \Delta/K^{*n}.$$

Un élément $a \mod K^{*n} \in \Delta/K^{*n}$ est associé à un caractère $\chi_a : G(L/K) \to \mu_n$ donné par :

$$\chi_a(\sigma) = \frac{\sigma \sqrt[n]{a}}{\sqrt[n]{a}}.$$

Remarque. La composée de deux extensions de Kummer d'exposant n est encore une extension de Kummer d'exposant n, et on peut donc considérer que toutes les extensions de Kummer d'exposant n sont contenues dans une extension maximale de Kummer d'exposant n, $\tilde{K} = K(\sqrt[n]{K^*})$, vérifiant :

$$Hom(G(\tilde{K}/K), \mu_n) \simeq K^*/K^{*n},$$

en considérant que pour les groupes $G(L/K)$ et μ_n sont munis de la topologie de Krull et discrète, et que ce sont les morphismes continus que l'on regarde dans Hom.

Démonstration. Soit L/K une extension de Kummer. Alors $L = K(\sqrt[n]{\Delta})$ où $\Delta = L^{*n} \cap K^*$ d'après la proposition précédente.

Remarquons tout d'abord que, du fait que $G(L/K)$ agit trivialement sur K et que $\mu_n \subset K$ par hypothèse, alors on a $H^1(G(L,K), \mu_n) = Hom(G(L,K), \mu_n)$.

On définit l'homomorphisme suivant, $\Delta \to Hom(G(L/K), \mu_n)$, $a \mapsto \chi_a$, avec $\chi_a(\sigma) = \frac{\sigma \sqrt[n]{a}}{\sqrt[n]{a}}$. Le noyau de ce morphisme est K^{*n} car $\chi_a = 1$ équivaut à $\forall \sigma \in G(L/K), \sigma \sqrt[n]{a} = \sqrt[n]{a}$, soit $\sqrt[n]{a} \in K^*$, et finalement ceci équivaut à $a \in K^{*n}$. On a donc un homomorphisme injectif :

$$\Delta/K^{*n} \to Hom(G(L/K), \mu_n).$$

Nous allons prouver la surjectivité de ce morphisme, d'abord en considérant le cas où L/K est une extension finie, par le théorème de Hilbert 90, puis nous généraliserons ensuite.

Soit $\chi \in Hom(G(L/K), \mu_n)$. Alors $\chi : G(L/K) \to L^*$ est un homomorphisme croisé et le théorème Hilbert 90 nous dit qu'il existe un $b \in L^*$ tel que $\chi(\sigma) = \frac{\sigma b}{b}$ pour tout $\sigma \in G(L/K)$. Alors, $\sigma(b^n) = (\sigma b)^n = \chi(\sigma)^n b^n = b^n$, puique $\chi(\sigma) \in \mu_n$, et ce pour tout $\sigma \in G(L/K)$. Ainsi, $b^n = a \in K^* \cap L^{*n} = \Delta$, et on a $\chi = \chi_a$, ce qui donne la surjectivité.

Maintenant, si L/K est de degré infini, on regarde Δ_i/K^{*n} pour Δ_i parcourant les sous-groupes finis de Δ/K^{*n}., et on pose $L_i = K(\sqrt[n]{\Delta_i})$. Alors $\Delta/K^{*n} =$

$\bigcup_i \Delta_i/K^{*n}$ et $L = \bigcup_i L_i$, puisque L/K est une extension d'exposant n : tout élément y est d'ordre fini.

Ainsi, les groupes $G(L/L_i)$ forment une base de voisinages ouverts de $1 \in G(L/K)$. Le noyau d'un homomorphisme continu χ est ouvert, il doit donc contenir un sous-groupe $G(L/L_i)$.

Comme L/K est abélienne car de $Kummer$, le théorème de correspondance de Galois nous permet de voir que $Gal(L_i/K) = Gal(L/K)/Gal(L/L_i)$. Comme $G(L/L_i)$ est inclus dans le noyau de χ, on en déduit que si $\sigma = \tau\rho$ avec $\sigma \in Gal(L/K)$, $\tau \in Gal(L_i/K)$, $\rho \in Gal(L/L_i)$, alors $\chi(\sigma) = \chi(\tau) \times 1$.

Ainsi χ fournit un homomorphisme $\overline{\chi} : G(L_i/K) \to \mu_n$, avec $\overline{\chi}(\sigma) = \chi(\sigma_{|L_i})$. Avec ce qu'on a vu dans le cas précédent, $\overline{\chi}$ est de la forme $\overline{\chi_a} : G(L_i/K) \to \mu_n$, $a \in \delta_i$. Mais alors, $\chi(\sigma) = \overline{\chi_a}(\sigma_{|L_i}) = \frac{\sigma\sqrt[n]{a}}{\sqrt[n]{a}} = \chi_a(\sigma)$, et ainsi $\chi = \chi_a$, ce qui prouve la surjectivité.

Considérons maintenant la correspondance. On prend Δ un groupe entre K^* et K^{*n}, et on pose $L = K(\sqrt[n]{\Delta})$. On veut montrer que $\Delta = L^{*n} \cap K^*$. Ce que l'on vient de montrer nous donne un isomorphisme $L^{*n} \cap K^*/K^{*n} \simeq Hom(G, \mu_n)$.

Par un argument de dualité (c'est vrai pour des groupes finis par un petit bricolage sur le fait qu'un groupe est isomorphe à son dual et à son bidual, on peut le généraliser ici du fait que les considérations topologiques sont bien choisies et permettent de factoriser par des extensions finis), on montre que le sous-groupe Δ/K^{*n} de $L^{*n} \cap K^*/K^{*n}$ est isomorphe, *via* un isomorphisme obtenu à partir du précédent, à un sous-groupe $Hom(G/H, \mu_n)$ de $Hom(G, \mu_n)$, avec H un certain sous-groupe distingué de G.

Cet isomorphisme est donné par l'isomorphisme que l'on a construit : si l'on écrit le fait que $\Delta/K^{*n} \simeq Hom(G/H, \mu_n)$, H est caractérisé par la fait que si $\sigma \in H$, alors pour tout $a \in \Delta/K^{*n}$, on a $\sigma\sqrt[n]{a} = \sqrt[n]{a}$. Ainsi, σ fixe $K(\sqrt[n]{\Delta}) = L$, donc $\sigma = 1$ et en fait $H = \{1\}$.

On en déduit que $\Delta = L^{*n} \cap K^*$, et cela permet de conclure la démonstration du fait que $\Delta \mapsto K(\sqrt[n]{\Delta})$ est une correspondance bijective, et on a montré le théorème. □

4 Théorie du corps de classes générale

4.1 Frobenius et éléments premiers

Dans ce chapitre, nous allons développer des outils, venant purement de la théorie des groupes, qui nous serons utiles dans notre but de démonstration. On pourrait voir ces outils sans réellement parler de corps, et en ne considérant que la structure de groupe dans les groupe de Galois, agrémentée de quelques axiomes (c'est ce que fait [1]), mais nous allons essayer de considérer une approche inter-

médiaire, c'est-à-dire que l'on n'oubliera le fait que les groupes de Galois vont avec les corps sur lesquels ils agissent. L'intérêt de l'approche générale et formelle est qu'elle peut servir dans l'étude de la théorie du corps de classes global.

Notons que dans ce qui suit, K désignera toujours une extension finie d'un corps k.

Les notations seront les suivantes : on considère k un corps, $\overline{k}$ une clôture algébrique de k, $G = G(\overline{k}/k)$ le groupe de Galois de $\overline{k}$ sur k, muni de sa structure de groupe pro-fini.

On considère aussi un homomorphisme continu surjectif :

$$\deg \, : \, G \to \widehat{\mathbb{Z}}.$$

Le noyau de deg a pour corps fixe $\tilde{k}$, et deg induit un isomorphisme $G(\tilde{k}/k) \simeq \widehat{\mathbb{Z}}$.

Définition 4.1.1. On dit qu'une extension dont le groupe de Galois est isomorphe à $\widehat{\mathbb{Z}}$ est une $\widehat{\mathbb{Z}}$-extension.

Comme exemple de $\widehat{\mathbb{Z}}$-extension, on peut penser à l'extension maximale non ramifiée d'un corps local.

Pour toute extension finie K/k, on pose $\tilde{K} = K\tilde{k}$ et $f_K = [K \cap \tilde{k} : k]$, qui correspond, si k est un corps local, au degré d'inertie. deg induit un homomorphisme surjectif

$$\deg_K = \frac{1}{f_K} \deg \, : \, G_K \to \widehat{\mathbb{Z}},$$

ainsi qu'un isomorphisme $\deg_K \, : \, G(\tilde{K}/K) \tilde{\to} \widehat{\mathbb{Z}}$.

Définition 4.1.2. L'élément $\phi_K \in G(\tilde{K}/K)$ tel que $\deg(\phi_K) = 1$ est appelé le *Frobenius* sur K.

Pour toute extension finie L/K, on pose $L^0 = L \cap \tilde{K}$, $f_{L/K} = [L^0 : K] = \frac{f_L}{f_K}$ et $\phi_{L^0/K} = (\phi_K)_{|L^0}$.

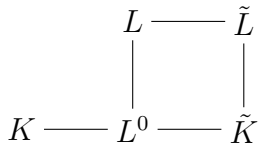
Dans le cas de corps locaux, $L^0 = K^{nr}$.

On note aussi que l'on a le diagramme commutatif :

$$\begin{array}{ccc} G_L & \xrightarrow{\deg_L} & \widehat{\mathbb{Z}} \\ \downarrow & & \downarrow f_{L/K} \\ G_K & \xrightarrow{\deg_K} & \widehat{\mathbb{Z}} \end{array}$$

Il correspond au fait que $(\phi_L)_{\tilde{K}} = \phi_K^{f_{L/K}}$.

Maintenant, soit L/K une extension galoisienne finie. On considère le diagramme suivant, où $L^0 = L \cap \tilde{K}$ et $\tilde{L} = L\tilde{K}$:



deg : $G_K \to \widehat{\mathbb{Z}}$ induit (on connait les sous-groupes compact de $\widehat{\mathbb{Z}}$) un homomorphisme surjectif :

$$\deg \ : \ G(\tilde{L}/K) \to \widehat{\mathbb{Z}},$$

et on pose

$$\Phi(\tilde{L}/K) = \left\{ \tilde{\sigma} \in G(\tilde{L}/K) \diagup \deg_K(\tilde{\sigma}) \in \mathbb{N}^* \right\}.$$

Si $\tilde{\sigma} \in \Phi(\tilde{L}/K)$ et $n = \deg_K(\tilde{\sigma})$, alors $\tilde{\sigma}_{|K} = \phi_K^n$.

Proposition 4.1.3. *L'application $\Phi(\tilde{L}/K) \to G(L/K)$, $\tilde{\sigma} \mapsto \tilde{\sigma}_{|L}$, est surjective. Si $\sigma \in G(L/K)$, et $\tilde{\sigma} \in \Phi(\tilde{L}/K)$ tel que $\sigma = \tilde{\sigma}_L$, on dit que $\tilde{\sigma}$ est un relevé de Frobenius de σ.*

Démonstration. Si $\sigma \in G(L/K)$, alors $\sigma_{|L^0} = \phi_{L^0/K}^n$ pour un certain $n > 0$ (comme on considère une extension finie, le groupe de Galois est fini, et donc on peut prendre $n > 0$ sans que cela pose de problème pour obtenir 1). Soit $\tilde{\phi}$ une extension de ϕ_K à $\tilde{L}$. Alors, $\sigma\tilde{\phi}^{-n}_{|L^0} = 1$, autrement dit, $\sigma\tilde{\phi}^{-n} \in G(L/L^0) \simeq G(\tilde{L}/\tilde{K})$. En effet, L et $\tilde{K}$ sont linéairement disjointes (c'est-à-dire d'intersection égale à L_0) donc, par exemple d'après [7] page 276, on a $G(L/L^0) \simeq G(\tilde{L}/\tilde{K})$. Ainsi, $\sigma\tilde{\phi}^{-n}_{|L} = \tau_{|L}$, avec $\tau \in G(\tilde{L}/\tilde{K})$. Maintenant, on a $\tilde{\sigma} = \tau\tilde{\phi}^n$ qui est un relevé de Frobenius de σ avec $\tilde{\sigma}_{|\tilde{K}} = \tilde{\phi}^n_{|\tilde{K}} = \phi_K^n$, c'est-à-dire $\deg_K(\tilde{\sigma}) = n \in \mathbb{N}^*$. □

Le nom de relevé de Frobenius vient du fait qu'il transforme les éléments de $G(L/K)$ en morphismes de Frobenius :

Proposition 4.1.4. *Soit $\tilde{\sigma} \in \Phi(\tilde{L}/K)$ et soit Σ le corps fixé par $\tilde{\sigma}$. Alors :*
(i) $[\Sigma : K] < \infty$;
(ii) $f_{\Sigma/K} = \deg_K(\tilde{\sigma})$;
(iii) $\tilde{\Sigma} = \tilde{L}$;
(iv) $\tilde{\sigma} = \phi_\Sigma$.

Démonstration. On note $\Sigma^0 = \Sigma \cap \tilde{K}$, qui est le corps fixé par $\tilde{\sigma}_{|\tilde{K}} = \phi_K^{\deg_K(\tilde{\sigma})}$, vu les définitions et les isomorphismes en jeu. Mais alors $f_{\Sigma/K} = [\Sigma^0 : K] = \deg_K(\tilde{\sigma})$, et on a le (ii).

De plus $[\Sigma : \Sigma^0] = [\Sigma\tilde{K} : \tilde{K}] \leqslant [\tilde{L} : \tilde{K}] < \infty$. Comme $[\Sigma^0 : K] = f_{\Sigma/K}$ est aussi finie, alors par multiplicativité des degrés, $[\Sigma : K]$ est fini, et on a le (i).

Pour le (iii), $G(\tilde{L}/\Sigma)$ est topologiquement engendré par $\tilde{\sigma}$ et ainsi, est procyclique. Mais alors, par ce que l'on a vu lors de la définition des groupes procycliques, l'homomorphisme surjectif obtenu par restriction $G(\tilde{L}/\sigma) \to G(\tilde{\Sigma}/\Sigma) \simeq \widehat{\mathbb{Z}}$ est nécessairement un isomorphisme. Alors $\tilde{\Sigma} = \tilde{L}$ et on a (iii).

Enfin, on a par définition $f_{\Sigma/K}\deg_\Sigma(\tilde{\sigma}) = \deg_K(\tilde{\sigma}$ et avec (ii), on a alors $f_{\Sigma/K}\deg_\Sigma = f_{\Sigma/K}$, donc $\deg_\Sigma(\tilde{\sigma}) = 1$, et ainsi, $\tilde{\sigma} = \phi_\Sigma$ est bien un Frobenius. □

Définition 4.1.5. Soit A un G-module noté multiplicativement. Pour tout corps K, on pose : $A_K = A^{G_K} = \left\{a \in A \diagup \forall \sigma \in G(\overline{k}/K),\ a^\sigma = a\right\}$.

Définition 4.1.6. Si L/K est une extension finie, on a $A_K \subset A_L$ et on définit l'*application norme* :

$$N_{L/K}\ :\ A_L \to A_K,\ N_{L/K}(a) = \prod_\sigma a^\sigma,$$

avec σ parcourant un système de représentants à droite de G_K/G_L.

Remarque. Si $K \subset L \subset M$, alors :

$$N_{M/K} = N_{L/K} \circ N_{M/L}.$$

Si L/K est une extension galoisienne, alors A_L est un $G(L/K)$-module et $A_K = A_L^{G(L/K)}$.

Définition 4.1.7. On appelle *valuation henselienne* de A_k par rapport à deg un homomorphisme $v\ :\ A_k \to \widehat{\mathbb{Z}}$ vérifiant :
(i) $v(A_k) = Z \supset \mathbb{Z}$ et $Z/nZ \simeq \mathbb{Z}/n\mathbb{Z}$ pour tout $n \in \mathbb{N}$.
(ii) $v(N_{K/k}A_K) = f_K Z$ pour tout corps K.

Remarque. Pour tout corps K, une valuation henselienne $v\ :\ A_k \to \widehat{\mathbb{Z}}$ définit un homomorphisme $v_K = \frac{1}{f_K} v \circ N_{K/k}\ :\ A_K \to \widehat{\mathbb{Z}}$ d'image Z.

Proposition 4.1.8. *(i) $v_K = v_{K^\sigma} \circ \sigma$ pour tout $\sigma \in G$, où $K^\sigma = \sigma(K)$.*
(ii) Pour toute extension L/K finie, on a le diagramme commutatif :

$$\begin{array}{ccc} A_L & \xrightarrow{v_L} & \widehat{\mathbb{Z}} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle f_{L/K}} \\ A_K & \xrightarrow{v_K} & \widehat{\mathbb{Z}} \end{array}$$

Démonstration. Nous allons d'abord montrer le (i). Si τ parcourt un système de représentant à droite de G_k/G_K, alors $\sigma^{-1}\tau\sigma$ parcourt un système de représentants à droite de $G_k/\sigma^{-1}G_K\sigma = G_k/G_{K^\sigma}$. Ainsi, si $a \in A_K$, alors :

$$v_{K^\sigma}(a^\sigma) = \frac{1}{f_{K^\sigma}} v(\prod_\tau a^{\sigma\sigma^{-1}\tau\sigma}) = \frac{1}{f_K} v((\prod_\tau a^\tau)^\sigma) = \frac{1}{f_K} v(N_{K/k}(a)) = v_K(a).$$

Maintenant pour le (ii), si $a \in A_L$, alors :

$$f_{L/K} v_L(a) = f_{L/K} \frac{1}{f_L} v(N_{L/k}(a)) = \frac{1}{f_K} v(N_{K/k}(N_{L/K}(a))) = v_K(N_{L/K}(a)).$$

□

Définition 4.1.9. Un *élément premier* de A_K est un élément $\pi_K \in A_K$ tel que $v_K(\pi_K) = 1$ (ceci correspond à l'idée d'uniformisante qu'on a vu plus haut). On pose $U_K = \{u \in A_K / v_K(u) = 0\}$.

Si $f_{L/K} = [L : K]$, c'est-à-dire $L^0 = L$ (ce qui correspond à une extension non ramifiée), alors par le (ii) du point précédent, $(v_L)_{|A_K} = v_K$. En particulier, un élément premier de A_K est aussi un élément premier de A_L. D'un autre côté, si $f_{L/K} = 1$, c'est-à-dire si $L^0 = K$ (ce qui correspond à une extension totalement ramifiée) et si π_L est un élément premier de A_L, alors $\pi_K = N_{L/K}(\pi_L)$ est un élément premier de A_K.

4.2 L'application de réciprocité

4.2.1 Une condition axiomatique, conséquence

Dans la suite, on va supposer que le G-module A satisfait la condition axiomatique suivante :

Axiome 1. *Pour toute sous-extension L/K de $\tilde{K}/K$, $\sharp H^0(G(L/K), A_L) = [L : K]$, et $\sharp H^{-1}(G(L/K), A_L) = 1$ et est bien défini.*

Remarque. L/K sous-extension de $\tilde{K}/K$ correspond, pour des corps locaux de corps résiduel de caractéristique non nulle, au fait que L/K soit non-ramifiée. En particulier si le corps résiduel est fini et l'extension fini, on a bien $G(L/K)$ fini et cyclique.

À partir de cela, nous allons construire l'application de réciprocité, pièce centrale de la théorie du corps de classes. On commence par une conséquence directe de l'axiome.

Proposition 4.2.1. *Si L/K est une sous-extension finie de $\tilde{K}/K$, alors pour $i = 0$ ou -1,*

$$H^i(G(L/K), U_L) = 0$$

Démonstration. Soit $n = [L : K]$. On va considérer $Z = v_L(A_L)$ comme un $G(L/K)$-module trivial. On a, vu les définitions, $H^0(G(L/K), Z) = Z/nZ$ et $H^{-1}(G(L/K), Z) = 0$, en se rappellant que $Z \subset \widehat{\mathbb{Z}}$ n'a pas d'élément d'ordre fini (par exemple, on a vu que $\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$).

Par le (i) de la proposition 4.1.8, on a

$$1 \to U_L \to A_L \to Z \to 0$$

qui est une suite exacte courte de $G(L/K)$-modules. On en déduit, avec l'hexagone exact donné lors de l'étude du quotient de Herbrand, proposition 3.2.11, que l'on a la suite exacte suivante :

$$1 \to H^0(G(L/K), U_L) \to H^0(G(L/K), A_L) \to^{v_L^*} H^0(G(L/K), Z) \to H^{-1}(G(L/K), U_L) \to 1.$$

Si π_K est un élément premier de A_K, alors $v_L(\pi_K) = v_K(\pi_K) = 1$, ce qui montre que l'application $v_L^* : H^0(G(L/K), A_L) \to H^0(G(L/K), Z) = Z/nZ$ est surjective, et ainsi bijective comme $\sharp H^0(G(L/K), A_L) = n$ (c'est notre axiome). À partir de là, on en déduit directement, le diagramme étant exact, que $H^i(G(L/K), U_L) = 0$ pour $i = 0$ ou -1. □

4.2.2 Définition de l'application réciprocité

Définition 4.2.2. Soit L/K une extension galoisienne finie. On définit *l'application réciprocité* $r_{L/K} : G(L/K) \to A_K/N_{L/K}A_L$ par :

$$r_{L/K}(\sigma) = N_{\Sigma/K}(\pi_\Sigma) \mod N_{L/K}A_L,$$

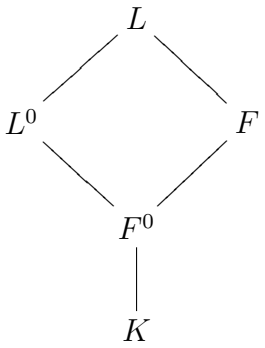
avec Σ le corps fixé par un relevé de Frobenius $\tilde{\sigma} \in \Phi(\tilde{L}/K)$ de $\sigma \in G(L/K)$ et $\pi_\Sigma \in A_\Sigma$ un élément premier.

Nous allons bien sûr montrer que cette application est bien définie, cela sera le premier but de cette sous-section.

Pour cela, on pose $N = N_{L|L^0}$ (voir 4.1.6). Soit F/K une sous-extension de L/K telle que $FL^0 = L$. Alors $F^0 = F \cap L^0$ et ainsi on peut montrer que, en revenant aux définitions :

$$N_{|A_F} = N_{F|F^0}.$$

On rappelle que l'on est dans la situation suivante :



On fixe $\phi \in \Phi(\tilde{L}/K)$ qui prolonge ϕ_K à $\tilde{L}$. On a la décomposition :

$$N_{F|K} = N \circ \mathscr{N}_F$$

où l'homomorphisme $\mathscr{N}_F : A_F \to A_L$ est défini par :

$$\mathscr{N}_F(a) = \prod_{\nu=0}^{f-1} a^{\phi^\nu}, \ f = [F^0 : K].$$

En effet, le groupe $G(F^0/K)$ est d'ordre f et est engendré par $\phi_{F^0/K} = (\phi_K)_{|F^0}$, c'est ce qu'on a vu au tout début de cette partie, et ainsi, pour $a \in A_F$,

$$N(\mathscr{N}_F(a)) = \prod_{\nu=0}^{f-1} N_{F/F^0}(a)^{\phi^\nu} = N_{F^0/K}(N_{F/F^0}(a)) = N_{F/K}(a).$$

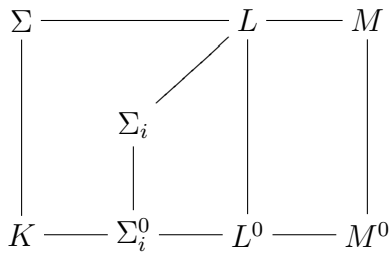
Lemme 4.2.3. *Soit $\tilde{\sigma}_1$, $\tilde{\sigma}_2$, $\tilde{\sigma}_3 \in \phi(\tilde{L}/K)$ et tels que $\tilde{\sigma}_3 = \tilde{\sigma}_1\tilde{\sigma}_2$. Si Σ_i est le corps fixé par $\tilde{\sigma}_i$ et si $\pi_i \in A_{\Sigma_i}$ est un élément premier pour $i = 1, 2$ ou 3, alors :*

$$N_{\Sigma_3/K}(\pi_3) = N_{\Sigma_1/K}(\pi_1)N_{\Sigma_2/K}(\pi_2) \mod N_{L/K}A_L.$$

Démonstration. Soit Σ le corps fixé par ϕ. Alors $\Sigma^0 = \Sigma \cap \tilde{K} = K$ car ϕ est de degré 1. On peut supposer que $\Sigma, \Sigma_i \subset L$, $i = 1, 2, 3$. En effet, si ce n'est pas le cas, on peut trouver une sous-extension galoisienne L'/K de $\tilde{L}/K$ contenant L et Σ et les Σ_i. Alors $\tilde{L}' = \tilde{L}$, et par l'injection canonique $A_L/N_{L/K}A_L \to A_{L'}/N_{L'/K}A_{L'}$, une égalité modulo $N_{L'/K}A_{L'}$ implique l'égalité modulo $N_{L/K}A_L$.

Maintenant, soit $n = [L : K]$ et M/L la sous-extension de $\tilde{L}/L$ de degré n. On dit la sous-extension de degré n car, par exemple, $\widehat{Z}$ n'a qu'un seul sous-groupe d'indice n.

Ceci nous conduit au diagramme suivant :



Soit $n_i = \deg_K(\tilde{\sigma}_i)$, alors $n_3 = n_1 + n_2$. Pour simplifier les notations, on pose $\tilde{\sigma}_4 = \phi^{-n_2}\tilde{\sigma}_1\phi^{n_2}$ avec $\deg_K(\tilde{\sigma}_4) = n_4 = n_1$. Alors $\Sigma_4 = \Sigma_1^{\phi^{n_2}}$ est le corps fixé par $\tilde{\sigma}_4$, et $\pi_4 = \pi_1^{\phi^{n_2}}$ est un élément premier de A_{Σ_4}, du fait que $v_K = v_{K^\sigma} \circ \sigma$. Ainsi, $N_{\Sigma_1/K}(\pi_1) = N_{\Sigma_4/K}(\pi_4)$, on est ramené à montrer la congruence :

$$N_{\Sigma_3/K}(\pi_3) = N_{\Sigma_4/K}(\pi_4)N_{\Sigma_2/K}(\pi_2) \mod N_{L/K}A_L.$$

On pose

$$\tau_i = \tilde{\sigma}_i^{-1}\phi^{n_i} \in G(\tilde{L}/\tilde{K}) = G(M/M^0),$$

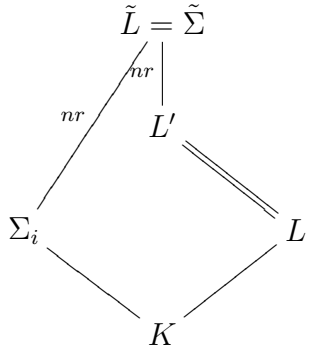
(cette dernière égalité venant d'un lemme classique de théorie de Galois, que l'on peut trouver dans [7] et que l'on a déjà evoqué plus haut) et on a $\tau_3 = \tau_2\tau_4$ et du fait que $\tilde{\sigma}_i \in G_{\Sigma_i}$,

$$\mathscr{N}_{\Sigma_i}(\pi_i)^{\phi-1} = \pi_i^{\phi^{n_i}-1} = \pi_i^{\tilde{\sigma}_i^{-1}\phi^{n_i}-1} = \pi_i^{\tau_i-1}.$$

On écrit $E = \mathscr{N}_{\Sigma_3}(\pi_3)\mathscr{N}_{\Sigma_2}(\pi_2)^{-1}\mathscr{N}_{\Sigma_4}(\pi_4)^{-1} \in U_L$, et on a alors :

$$E^{\phi-1} = \pi_3^{\tau_3-1}\pi_2^{1-\tau_2}\pi_4^{1-\tau_4}.$$

Maintenant, les éléments π_2, π_3, π_4 sont aussi des éléments premiers de A_L, et on peut alors écrire $\pi_2 = \varepsilon_2^{-1}\pi_4$, $\pi_3 = \varepsilon_3\pi_4$ avec $\varepsilon_2, \varepsilon_3 \in U_L$. En effet, on a le diagramme suivant :



et comme $L' = \tilde{\Sigma} \cap L' = \tilde{L} \cap L'$, l'extension $L = L'/\Sigma$ est non ramifiée, ce qui permet de voir que $v_{\Sigma_i} = v_L$.

On pose $\varepsilon_4 = \pi_4^{\tau_2-1} \in U_L$. En effet, L/K étant non ramifiée, $v_L(\tau_2(\pi_4)) = v_K(\tau_2(\pi_4)) = v_{K\tau_2}(\pi_4) = v_K(\pi_4)$ ce qui donne ce résultat.

Remarquant que, du fait que $\tau_3 = \tau_2\tau_4$, $(\tau_3 - 1) + (1 + \tau_2) + (1 - \tau_4) = (\tau_2 - 1)(\tau_4 - 1)$, et ainsi :

$$E^{\phi-1} = \prod_{i=2}^{4} \varepsilon_i^{\tau_i-1}.$$

Soit $f = [L : \Sigma] = f_{L/K}$, tel que $\phi^f = \phi_L$. On a vu que $H^{-1}(G(M/L), U_M) = 0$, on en déduit facilement qu'il existe $\tilde{E}$, $\tilde{\varepsilon}_i \in U_M$, pour $i = 1, 2, 3, 4$ tels que :

$$N_{M/L}(\tilde{E}) = E, \;\; N_{M/L}(\tilde{\varepsilon}_i) = \varepsilon_i.$$

Alors, $\tilde{E}^{\phi-1}$ et $\prod_{i=2}^{4} \tilde{\varepsilon}_i^{\tau_i-1}$ différent seulement d'un élément $x \in U_M$ avec $N_{M/L}(x) = 1$.

Ainsi, $H^{-1}(G(M/L), u_M) = 1$ et on obtient :

$$\tilde{E}^{\phi-1} = \prod_{i=2}^{4} \tilde{\varepsilon}_i^{\tau_i-1}\tilde{u}^{\phi_L-1} = \prod_{i=2}^{4} \tilde{\varepsilon}_i^{\tau_i-1} \left(\prod_{\nu=0}^{f-1}\right)^{\phi-1}$$

avec $\tilde{u} \in U_M$. Comme $\tau_i \in G(M/M^0)$, on a :

$$N(\tilde{E})^{\phi_K-1} = N\left(\prod_{\nu=0}^{f-1} \tilde{u}^{\phi^\nu}\right)^{\phi_K-1}$$

et ainsi

$$N(\tilde{E}) = N\left(\prod_{\nu=0}^{f-1} \tilde{u}^{\phi^\nu}\right) x$$

avec un $x \in U_{M^0}$ tel que $x^{\phi_K - 1} = 1$, c'est-à-dire en fait $x \in U_K$. En posant $u = N_{M/L}(\tilde{u})$ et en se rappellant que $N_{M^0/L^0} \circ N = N \circ N_{M/L}$ et que $N_{F/K} = N \circ \mathscr{N}_F$, on obtient :

$$\begin{aligned} N_{\Sigma_3/K}(\pi_3) N_{\Sigma_2/K}(\pi_2)^{-1} N_{\Sigma_4/K}(\pi_4)^{-1} &= N(E) = N_{M^0/L^0}(N(\tilde{E})) \\ &= \prod_{\nu=0}^{f-1} N(u)^{\phi^\nu} N_{M^0/L^0}(x) = N(N_{L/\Sigma}(u)) x^n \\ &= N_{L/K}(u) N_{L/K}(x) \in N_{L/K} A_L, \end{aligned}$$

et on a ainsi montré le lemme. □

Corollaire 4.2.4. *L'application*

$$r_{L/K} \,:\, G(L/K) \to A_K / N_{L/K} A_L$$

est bien définie et est un homomorphisme.

Démonstration. Soit $\tilde{\sigma}$, $\tilde{\sigma}' \in \Phi(\tilde{L}/K)$ deux relevés de Frobenius de σ. Soit Σ et Σ' les corps fixés par $\tilde{\sigma}$ et $\tilde{\sigma}'$, et soit $\pi \in A_\Sigma$ et $\pi' \in A_{\Sigma'}$ des éléments premiers. On peut supposer que $m = \deg_K(\tilde{\sigma}') - \deg_K(\tilde{\sigma}) \geqslant 0$. Traitons d'abord le cas $m = 0$. On en déduit que $(\tilde{\sigma})_{|\tilde{K}} = (\tilde{\sigma}')_{|\tilde{K}}$ et par hypothèse, $(\tilde{\sigma})_{|L} = (\tilde{\sigma}')_{|L}$. Alors, $\tilde{L} = L\tilde{K}$ et ainsi $\tilde{\sigma} = \tilde{\sigma}'$. Ceci implique $\Sigma = \Sigma'$ et $\pi' = \pi u$ avec $u \in U_\Sigma$. Soit M une sous-extension finie galoisienne de $\tilde{L}/K$ contenant L et Σ (c'est bien possible vu qu'on a montré que $[\Sigma : K] < +\infty$). Comme $H^{-1}(G(M/\Sigma), U_M) = 1$, avec ce qu'on a vu précédemment, il existe $\tilde{u} \in U_M$ tel que $u = N_{M/\Sigma}(\tilde{u})$, et ainsi, en prenant les normes dans $\pi' = \pi u$, on obtient :

$$N_{\Sigma'/K}(\pi') = N_{\Sigma/K}(\pi) N_{M/K}(\tilde{u}) = N_{\Sigma/K}(\pi) \mod N_{L/K} A_L$$

car $N_{M/K}(\tilde{u}) = N_{\Sigma/K} \circ N_{M/\Sigma}(\tilde{u})$ et $N_{M/K}(\tilde{u}) \in N_{M/K} A_M \subset N_{L/K} A_L$ puisque $L \subset M$.

Par ailleurs, si $m > 0$, alors $\tilde{\tau} = \tilde{\sigma}^{-1}\tilde{\sigma}' \in G(\tilde{L}/K)$ est un relevé de Frobenius de $1 \in G(L/K)$ avec $\deg_K(\tilde{\tau}) = m$. Si $M \supset L$ est le corps fixé par $\tilde{\tau}$ et si $\pi_M \in A_M$ est un élément premier, alors par le dernier lemme,

$$N_{\Sigma'/K}(\pi') = N_{\Sigma/K}(\pi) N_{M/K}(\pi_M) = N_{\Sigma/K}(\pi) \mod N_{L/K} A_L.$$

Ceci montre bien l'indépendance de $r_{L/K}(\sigma)$ du choix du relevé de Frobenius et de l'élément premier dans A_Σ.

Le fait d'être un homomorphisme est direct avec le lemme précédant, avec $\sigma_1, \sigma_2 \in G(L/K)$ et $\tilde{\sigma}_3 = \tilde{\sigma}_1 \tilde{\sigma}_2$ qui est une relevé de Frobenius de $\sigma_3 = \sigma_1 \sigma_2$. □

L'intérêt de cette application de réciprocité apparait clairement dans l'énoncé suivant, envoyer des Frobenius sur des éléments premiers :

Théorème 4.2.5. *Si L/K est une sous-extension finie de $\tilde{K}/K$, alors l'application de réciprocité $r_{L/K} : G(L/K) \to A_K/N_{L/K}A_L$ est donnée par*

$$r_{L/K}(\phi_{L/K}) = \pi_K \mod N_{L/K}A_L,$$

et est un isomorphisme.

Démonstration. $\phi_K \in \phi(\tilde{K}/K)$ est un relevé de Frobenius de $\phi_{L/K} \in G(L/K)$, vu les définitions, et il est de corps fixé K. Ainsi, $r_{L/K}(\phi_{L/K}) = \pi_K \mod N_{L/K}A_L$. Le groupe $A_K/N_{L/K}A_L = H^0(G(L/K), A_L)$ est du même ordre, n, que $G(L, K)$, par l'axiome 1 et le fait que l'extension soit non ramifiée. Or $\pi_K \mod N_{L/K}A_L$ est un élément générateur de $A_K/N_{L/K}A_L$, puisque $\pi_K^m = N_{L/K}(a) \in N_{L/K}A_L$ implique $m = v_K(\pi_K^m) = v_K(N_{L/K}(a)) = nv_L(a) = 0 \mod n$. Ainsi, $r_{L/K}$ est bien un isomorphisme. □

4.2.3 Propriétés de nature fonctorielle

L'application de réciprocité vérifient un certain nombre de propriétés de nature fonctorielle, utiles pour la suite.

Proposition 4.2.6. *Soit L/K et L'/K' deux extensions galoisiennes et soit $K \subset K'$ et $L \subset L'$. Alors le diagramme :*

$$\begin{array}{ccc} G(L'/K') & \xrightarrow{r_{L'/K'}} & A_{K'}/N_{L'/K'}A_{L'} \\ \downarrow & & \downarrow N_{K'/K} \\ G(L/K) & \xrightarrow{r_{L/K}} & A_K/N_{L/K}A_L \end{array}$$

est commutatif, la flèche de gauche étant donnée par la restriction $\sigma' \mapsto \sigma'_{|L}$.

Démonstration. Soit $\sigma' \in G(L'/K')$ et $\sigma = \sigma'_{|L} \in G(L/K)$. Si $\tilde{\sigma}' \in \Phi(\tilde{L}'/K')$ est un relevé de Frobenius de σ', alors $\tilde{\sigma} = \tilde{\sigma'}_{\tilde{L}} \in G(\tilde{L}/K)$ est un relevé de Frobenius de σ puisque $\deg_K(\tilde{\sigma}) = f_{K'/K} \deg_{K'}(\tilde{\sigma}') \in \mathbb{N}^*$.

Maintenant, soit Σ' le corps fixé par $\tilde{\sigma}'$. Alors $\Sigma = \Sigma' \cap \tilde{L} = \Sigma' \cap \tilde{\Sigma}$ est le corps fixé par $\tilde{\sigma}$, et $f_{\Sigma'/\Sigma} = 1$. Ainsi, si $\pi_{\Sigma'}$ est un élément premier de $A_{\Sigma'}$, alors $\pi_\Sigma = N_{\Sigma'/\Sigma}(\pi'_{\Sigma'})$ est un élément premier de A_Σ, et on peut déduire la proposition de l'égalité suivante :

$$N_{\Sigma/K}(\pi) = N_{\Sigma/K}(N_{\Sigma'/\Sigma}(\pi')) = N_{\Sigma'/K}(\pi') = N_{K'/K}(N_{\Sigma'/K'}(\pi')).$$

□

Proposition 4.2.7. *Si L/K est une extension galoisienne finie, et si $\sigma \in G$, alors le diagramme :*

$$\begin{array}{ccc} G(L/K) & \xrightarrow{r_{L/K}} & A_K/N_{L/K}A_L \\ \downarrow{\scriptstyle \sigma^*} & & \downarrow{\scriptstyle \sigma} \\ G(L^\sigma/K^\sigma) & \xrightarrow{r_{L^\sigma/K^\sigma}} & A_{K^\sigma}/N_{L^\sigma/K^\sigma}A_{L^\sigma} \end{array}$$

est commutatif et la flèche de gauche est induite par la conjugaison $\tau \mapsto \sigma^{-1}\tau\sigma$.

Démonstration. Soit $\tilde{\tau} \in \Phi(\tilde{L}/K)$ un relevé de Frobenius de $\tau \in G(L/K)$ et soit $\widehat{\tau} \in G(\overline{k}/k)$ qui étend $\tilde{\tau}$ à $\overline{k}$. Alors $(\sigma^{-1}\widehat{\tau}\sigma)_{|\tilde{L}^\sigma}$ est un relevé de Frobenius de $\sigma^*(\tau)$ comme $\deg_{K^\sigma}(\sigma^{-1}\widehat{\tau}\sigma) = \deg_K(\widehat{\tau}) = \deg_K(\tilde{\tau}) \in \mathbb{N}^*$. Si Σ est le corps fixé par $\tilde{\tau}$, alors Σ^σ est le corps fixé par $\sigma^{-1}\widehat{\tau}\sigma_{|\tilde{L}^\sigma}$, et si π est un élément premier de A_Σ, alors du fait que $v_\Sigma = v_{\Sigma^\sigma} \circ \sigma$. On peut alors déduire la proposition de l'égalité de normes $N_{\Sigma^\sigma/K^\sigma}(\pi^\sigma) = N_{\Sigma/K}(\pi)^\sigma$. □

Définition 4.2.8. Soit G un groupe, et soit G' son groupe dérivé. Alors on note $G^{\mathrm{ab}} = G/G'$, l'abélianisé de G.

Définition 4.2.9. Soit G est un groupe et H un sous-groupe d'indice fini de G. Alors on a morphisme de groupes canonique $Ver : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$. Ver est pour *Verlagerung*, et ce morphisme est aussi appelé morphisme de transfert.

Explicitons la manière dont ce morphisme est défini. Soit R un système (fini) de représentants de G modulo H. On a $G = RH$ et on suppose que $1 \in R$. Si $\sigma \in G$, on pose pour $\rho \in R$,

$$\sigma\rho = \rho'\sigma_\rho,\ \sigma_\rho \in H,\ \rho' \in R.$$

Alors $Ver(\sigma \mod G') := \prod_{\rho\in R} \sigma_\rho \mod H'$, et cette définition ne dépend pas du choix des représentants dans R.

On a une autre description de Ver : soit $\sigma \in G$ et soit S le sous-groupe engendré par σ. Soit τ dans un ensemble fini tel que $G = \amalg_\tau S\tau H$. Soit $S_\tau = \tau^{-1}S\tau \cap H$ et soit $f(\tau)$ le plus petit entier naturel tel que $\sigma_\tau = \tau^{-1}\sigma^{f(\tau)}\tau \in H$. Alors σ_τ génère S_τ et $Ver(\sigma \mod G') = \prod_\tau \sigma_\tau \mod H'$. On retrouve la première formule en prenant $R = \{\sigma^i\tau \diagup \tau, 1 \leqslant i \leqslant \tau\}$.

Proposition 4.2.10. *Soit L/K une extension galoisienne finie et soit K' un corps intermédiaire. On alors le diagramme commutatif suivant :*

$$\begin{array}{ccc} G(L/K')^{ab} & \xrightarrow{r_{L/K'}} & A_{K'}/N_{L/K'}A_L \\ {\scriptstyle Ver}\uparrow & & \uparrow \\ G(L/K)^{ab} & \xrightarrow{r_{L/K}} & A_K/N_{L/K}A_L, \end{array}$$

où la flèche de droite est donnée par l'inclusion $A_K \subset A_{K'}$.

Démonstration. On pose $G = G(\tilde{L}/K)$ et $H = G(\tilde{L}/K')$. Soit $\tilde{\sigma}$ un relevé de Frobenius de $\sigma \in G(L/K)$, Σ le corps fixé par $\tilde{\sigma}$ et $S = G(\tilde{L}/\Sigma)$. On considère la décomposition $G = \amalg_\tau S\tau H$ obtenue en quotientant à gauche et à droite, et on pose $S_\tau = \tau^{-1}S\tau \cap H$ et $\tilde{\sigma}_\tau = \tau^{-1}\tilde{\sigma}^{f(\tau)}\tau$ comme plus haut. Soit $\overline{G} = G(L/K)$, $\overline{H} = G(L/K')$, $\overline{S} = (\sigma)$, $\overline{\tau} = \tau_L$ et $\sigma_\tau = (\tilde{\sigma}_\tau)_L$.

Alors on a directement $\overline{G} = \amalg_\tau \overline{S}\overline{\tau}\overline{H}$, et ainsi

$$Ver(\sigma \mod G(L/K)') = \prod_\tau \sigma_\tau \mod G(L/K')'.$$

Pour tout τ, soit ω_τ un système de représentants de H/S_τ. Alors

$$H = \amalg_\tau S_\tau\omega_\tau \text{ et } G = \amalg_{\tau,\omega_\tau} S\tau\omega_\tau.$$

Soit Σ_τ le corps fixé par $\tilde{\sigma}_\tau$, c'est-à-dire le corps fixé par S_τ. Σ^τ est le corps fixé par $\tau^{-1}\tilde{\sigma}\tau$, et ainsi $\Sigma_\tau|\Sigma^\tau$ est une sous-extension de $\tilde{L}/\Sigma^\tau$ de degré $f(\tau)$. si π est un élément premier de A_Σ, alors π^τ est un élément premier de A_{Σ^τ}, et aussi de A_{Σ_τ}.

Par la décomposition décrite, on a

$$N_{\Sigma/K}(\pi) = \prod_{\tau,\omega_\tau} \pi^{\tau\omega_\tau} = \prod_\tau (\prod_{\omega_\tau} (\pi^\tau)^{\omega_\tau}) = \prod_\tau N_{\Sigma_\tau/K'}(\pi^\tau).$$

Comme $\tilde{\sigma}_\tau \in \Phi(\tilde{L}/K')$ est un relevé de Frobenius de $\sigma_\tau \in G(L/K')$, ceci implique :

$$r_{L/K}(\sigma) = \prod_\tau r_{L/K'}(\sigma_\tau) = r_{L/K'}(\prod_\tau \sigma_\tau) = r_{L/K'}(Ver(\sigma \mod G(L/K)')),$$

ce qui permet de conclure. □

4.3 Loi de réciprocité générale

4.3.1 Nouvelle condition axiomatique

Dans cette partie, nous allons imposer une condition axiomatique de plus sur le G-module A, qui concernera les extensions cycliques :

Axiome 2 (Axiome du corps de classes)**.** *Pour toute extension cyclique finie L/K, $\sharp H^0(G(L/K), A_L) = [L : K]$ et $\sharp H^{-1}(G(L/K), A_L) = 1$.*

À partir de celle-ci, on verra que l'application de réciprocité conduit en fait à la construction d'un isomorphisme, premier pas vers la correspondance que l'on souhaite montrer.

4.3.2 Loi de réciprocité générale

Définition 4.3.1. On appelle *théorie du corps de classe* pour un G-module un couple d'homomorphismes $(\deg : G \to \widehat{\mathbb{Z}},\ v : A_k \to \widehat{\mathbb{Z}})$, avec deg continu et surjectif et v une valuation henselienne par rapport à deg.

Le théorème suivant est le théorème principal de la théorie du corps de classe, dernier grand pas dans cette partie formelle de la démonstration des théorèmes que nous avons énoncé.

Théorème 4.3.2 (Loi de réciprocité générale)**.** *Si L/K est une extension galoisienne finie, alors*

$$r_{L/K} : G(L/K)^{ab} \to A_K/N_{L/K}A_L$$

est un isomorphisme.

Démonstration. Si M/K est une sous-extension galoisienne de L/K, alors d'après la première propriété de fonctorialité que nous avons vu, on a le diagramme commutatif suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G(L/M) & \longrightarrow & G(L/K) & \longrightarrow & G(M/K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle r_{L/M}} & & \downarrow{\scriptstyle r_{L/K}} & & \downarrow{\scriptstyle r_{M/K}} & & \\ & & A_M/N_{L/M}A_L & \xrightarrow{N_{M/K}} & A_K/N_{L/K}A_L & \longrightarrow & A_K/N_{M/K}A_M & \longrightarrow & 1 \end{array}$$

Ceci va nous permettre de procéder en quatre étapes, dont les trois premières consisteront à se ramener au cas d'une extension cyclique totalement ramifiée.

Étape 1. Montrons que l'on peut se ramener à montrer le cas où $G(L/K)$ est abélien.

En effet, si l'on a le théorème vrai dans ce cas, alors montrons qu'on en déduit le résultat.

On pose $M = L^{\mathrm{ab}}$ la sous-extension abélienne maximale de L/K. Alors $G(L/K)^{\mathrm{ab}} = G(M/K)$ et le groupe engendré par les commutateurs $G(L/M)$ est exactement le noyau de $r_{L/K}$ dans $G(L/K)$ (c'est direct par une chasse au diagramme sur notre diagramme, en utilisant le fait que $r_{M/K}$ est un isomorphisme et que la suite sur la première ligne est exacte). Ainsi, $G(L/K)^{\mathrm{ab}} \to A_K/N_{L/K}A_L$ est injectif. Pour la surjectivité, on peut procéder par récurrence sur le degré des extensions dans le cas où $G(L/K)$ est résoluble.

En effet, dans ce cas, on a $M = L$, soit $G(L/K)$ abélien, ou bien il existe $H \lhd G$ non trivial tel que G/H abélien (c'est la définition d'être non trivialement résoluble), mais alors $D(G) \subset H \neq G$ et on a donc $[L : M] < [L : K]$. Alors avec l'hypothèse sur les groupes abéliens et l'hypothèse de récurrence, on a $r_{M/K}$ et $r_{L/M}$ qui sont surjectifs, et alors $r_{L/K}$ aussi, vu le diagramme.

Maintenant, si $G(L/K)$ n'est pas résoluble, on peut procéder encore par récurrence : on pose M le corps fixé par un p-sous-groupe de Sylow de $G(L/K)$. L'extension M/K n'est pas nécessairement galoisienne. Si $M = K$, c'est-à-dire $G(L/K)$ est un p-groupe, alors il est résoluble, et on est ramené au cas précédent. Sinon, on peut tout de même utiliser la partie gauche du diagramme, celle considérant $G(L/M)$ et $G(L/K)$. On va montrer que si S_p est un p-Sylow, alors il est atteint par $r_{L/K}$. On a, par hypothèse de récurrence, $r_{L/M}$ qui est surjectif. Or, l'inclusion $A_K \subset A_M$ induit un homomorphisme $i : A_K/N_{L/K}A_L \to A_M/N_{L/M}A_L$ (effectivement, $G_M \subset G_K$ donc on peut bien factoriser l'application $A_K \to A_M \to A_M/N_{L/M}A_L$), qui vérifie $N_{M/K} \circ i = [M : K]$. En effet, si $a \in A_K$, comme $G_M \subset G_K$, $N_{M/K} \circ i(a) = \prod_{\sigma \in G_K/G_M}(i(a))^\sigma = \prod_{\sigma \in G_K/G_M} a^\sigma = a^{\sharp G_K/G_M} = a^{[M:K]}$ vu les définitions.

Or $[M : K]$ est premier avec p, $G(L : K)$ étant un p-Sylow, et par multiplicativité des degrés. Donc $S_p \to S_p$, $a \mapsto a^{[M:K]}$ est surjectif, et ainsi S_p est dans l'image de $N_{M/K}$. Tout p-Sylow est alors dans l'image de $N_{M/K}$, donc $N_{M/K}$ est surjectif. Comme $r_{L/M}$ l'est aussi, on a bien $r_{L/K}$ qui est surjectif.

On est donc ramené à montrer le résultat pour $G(L/K)$ abélien.

Étape 2. Montrons maintenant qu'on peut se ramener à montrer le résultat pour L/K extension cyclique. Ainsi, si M/K parcours les sous-extensions cycliques de L/K, alors notre diagramme commutatif montre que le noyau de $r_{L/K}$ est inclus dans le noyau de $G(L/K) \to \prod_M G(M/K)$. En effet, l'hypothèse sur les extensions cycliques donne, si $a : G(L/K) \to G(M/K)$, $b : A_K/N_{L/K}A_L \to A_K/N_{M/K}A_M$, alors $r_{M/K} \circ a = r_{L/K} \circ b$ avec $r_{M/K}$ bijective, et donc $\ker r_{L/K} \subset \ker a$. Son noyau est donc dans l'intersection des noyaux des $G(L/K) \to G(M/K)$, et donc inclus dans le noyau de $G(L/K) \to \prod_M G(M/K)$.

Or, si L/K est abélienne, le morphisme $G(L/K) \to \prod_M G(M/K)$ est injectif. En effet, si $\sigma \in G$ non nul, $K^\sigma = M$ est bien une extension galoisienne cyclique (tout sous-groupe est distingué dans $G(L/K)$).

On peut montrer la surjectivité de la même manière que plus haut dans le cas résoluble, par récurrence.

On est donc ramené à étudier le cas cyclique.

Étape 3. Maintenant, soit L/K une extension cyclique. Montrons qu'on peut se ramener au cas où $f_{L/K} = 1$. On suppose qu'on a le résultat dans ce cas, et on pose $M = L^0$. On a alors $f_{L/M} = 1$, et alors, par la proposition que l'on a montrée sur les sous-extensions L de $\tilde{K}/K$, $r_{M/K}$ est un isomorphisme. De plus, $N_{M/K}$ est injective. En effet, $\sharp A_M/N_{L/M}A_L = [L : M]$, $\sharp A_K/N_{L/K}A_L = [L : K]$ et $\sharp A_K/N_{M/K}A_M = [M : K]$ vu la condition axiomatique admise, et cela nous donne, avec l'exactitude et la surjectivité, $\sharp Im(N_{M/K}) = \frac{[M:K]}{[L:K]} = [L : M]$ et donc $\sharp Im(N_{M/K}) = \sharp A_M/N_{L/M}A_L$ et $N_{M/K}$ injective. Avec notre hypothèse, $r_{L/M}$ est un isomorphisme, et on a vu que $r_{M/K}$ aussi, donc vu le diagramme, $r_{L/K}$ en est

aussi un.

Ainsi, on est ramené à étudier le cas où $f_{L/K} = 1$.

Étape 4. Soit L/K une extension cyclique avec $f_{L/K} = 1$ (totalement ramifiée donc). Soit σ un générateur de $G(L/K)$. Via l'isomorphisme entre $G(L/K)$ et $G(\tilde{L}/\tilde{K})$ que l'on obtient par un résultat de [7] déjà évoqué, on considèrera σ comme un élément de $G(\tilde{L}/\tilde{K})$. Alors, soit $\tilde{\sigma} = \sigma\phi_L \in \Phi(\tilde{L}/K)$ un relevé de Frobenius de σ avec $\deg_K(\tilde{\sigma}) = \deg_K(\phi_L) = f_{L/K} = 1$. Ainsi, le corps fixé par σ, Σ/K vérifie $f_{\Sigma/K} = 1$ et ainsi $\Sigma \cap \tilde{K} = K$. Soit M/K une sous-extension galoisienne finie de $\tilde{L}/K$ contenant Σ et L. Soit $N = N_{M/M^0}$, avec M^0 la sous-extension non-ramifiée maximale de M/K. Comme $f_{\Sigma/K} = f_{L/K} = 1$, on a $N_{\|A_\Sigma} = N_{\Sigma/K}$, $N_{\|A_L} = N_{L/K}$

Montrons l'injectivité de $r_{L/K}$. Pour cela, montrons que si $r_{L/K}(\sigma^k) = 1$ avec $0 \leqslant k \leqslant n = [L : K]$, alors $k = 0$.

Pour cela, soit $\pi_\Sigma \in A_\Sigma$ et $\pi_L \in A_L$ des éléments premiers. Comme $\Sigma, L \subset M \subset \tilde{L} = \tilde{\Sigma}$, π_Σ et π_L sont aussi des éléments premiers de M.

On pose $\pi_\Sigma^k = u\pi_L^k$, avec $u \in U_M$. On a alors :

$$r_{L/K}(\sigma^k) = N(\pi_\Sigma^k) = N(u)N(\pi_L^k) = N(u) \mod N_{L/K}A_L,$$

or $r_{L/K}(\sigma^k) = 1$, donc $N(u) = N(v)$ pour un certain $v \in U_L$. Ainsi, $N(u^{-1}v) = 1$, et on a $u^{-1}v = a^{\sigma-1}$, avec la condition axiomatique que l'on a imposé. On en déduit que l'on a dans A_M :

$$(\pi_L^k v)^{\sigma-1} = (\pi_L^k v)^{\tilde{\sigma}-1} = (\pi_\Sigma^k u^{-1} v)^{\tilde{\sigma}-1} = (a^{\sigma-1})^{\tilde{\sigma}-1} = (a^{\tilde{\sigma}-1})^{\sigma-1}.$$

Ainsi, on a $x = \pi_L^k v a^{1-\tilde{\sigma}} \in A_{M^0}$. Comme $v_{M^0}(x) \in \widehat{\mathbb{Z}}$ et $n v_{M^0}(x) = v_M(x) = k$, on en déduit que $k = 0$, et ainsi, on a l'injectivité de $r_{L/K}$. Pour la surjectivité, elle est alors directe pour des raisons de cardinaux, à cause de la condition axiomatique que l'on a imposé.

On a ainsi montré le théorème.

□

4.3.3 Conséquences

Ayant un isomorphisme dans le cas du théorème précédent, on peut considérer son application inverse.

Définition 4.3.3. L'application inverse de $r_{L/K} : G(L/K)^{\mathrm{ab}} \to A_K/N_{L/K}A_L$ donne une application surjective :

$$(\ , L/K) : A_K \to G(L/K)^{\mathrm{ab}}.$$

On nomme cette application le *symbole résiduel de norme.*

Les propriétés de fonctorialité que l'on a montré pour $r_{L/K}$ nous donnent directement le résultat suivant sur le symbole résiduel de norme.

Proposition 4.3.4. *Soit L/K et L'/K' deux extensions galoisiennes finies telles que $K \subset K'$ et $L \subset L'$. Soit $\sigma \in G$, on a alors les diagrammes commutatifs :*

$$\begin{array}{ccc} A_{K'} & \xrightarrow{(\ ,L'/K')} & G(L'/K')^{ab} \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow \\ A_K & \xrightarrow{(\ ,L/K)} & G(L/K)^{ab} \end{array} \qquad \begin{array}{ccc} A_K & \xrightarrow{(\ ,L/K)} & G(L/K)^{ab} \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle \sigma^*} \\ A_{K^\sigma} & \xrightarrow{(\ ,L^\sigma/K^\sigma)} & G(L^\sigma/K^\sigma)^{ab} \end{array}$$

et si $K' \subset L$, on a aussi :

$$\begin{array}{ccc} A_{K'} & \xrightarrow{(\ ,L'/K')} & G(L/K')^{ab} \\ \downarrow & & \uparrow{\scriptstyle Ver} \\ A_K & \xrightarrow{(\ ,L/K)} & G(L/K)^{ab} \end{array}$$

En passant à la limite projective, le symbole résiduel de norme s'étend à toutes les extensions galoisiennes L/K. En effet, si L_i/K parcourt les sous-extensions finies de L/K, alors :

$$G(L/K)^{\mathrm{ab}} = \varprojlim G(L_i/K)^{\mathrm{ab}}.$$

Ainsi, si $a \in A_K$, le symbole résiduel de norme donne $(a, L_i/K) \in G(L_i/K)$ et on définit alors $(a, L/K)_{|L_i} = (a, L_i/K)$, en remarquant bien que $(a, L_{i'}/K)_{|L_i} = (a, L_i/K)$ pour $L_{i'} \supset L_i$ (c'est une conséquence de notre première propriété de fonctorialité).

Dans le cas particulier de l'extension $\tilde{K}/K$, on a :

Proposition 4.3.5. $\deg_K \circ(\ , \tilde{K}/K) = v_K$*, et en particulier,*

$$(a, \tilde{K}/K) = \phi_K^{v_K(a)}.$$

Démonstration. On a $(\pi_K, \tilde{K}/K) = \phi_K$ comme $(\pi_K, \tilde{K}/K)_{|L} = (\pi_K, L/K) = \phi_{L/K} = (\phi_K)_{|L}$ pour toute sous-extension finie L/K de $\tilde{K}/K$, et $(u, \tilde{K}/K) = 1$ pour $u \in U_K$. Alors, si $a = \pi_K^n a$ pour $u \in U_K$, on a :

$$\deg_K(a, \tilde{K}/K) = \deg_K(\phi_K^n) = n = v_K(a).$$

On peut ainsi conclure. □

Ceci permet de voir que donner une valuation hensélienne v (avec les v_K) est équivalent à donner le symbole résiduel de norme $(\ , \tilde{K}/K)$. On peut ainsi interpréter ce que l'on a vu par le fait que si une théorie du corps de classes est donné pour les $\widehat{\mathbb{Z}}$-extensions $\tilde{K}/K$, alors, en supposant l'axiome du corps de classes, elle s'etend automatiquement à toute extension abélienne L/K.

4.4 Corps de classes

Le théorème d'isomorphisme précédent va nous permettre de voir une correspondances entre extensions abéliennes finies de K et sous-groupes ouverts (pour une topologie que l'on définira) de A_K pour A satisfaisant l'axiome du corps de classes. On verra plus tard à quel G-module A on appliquera ce résultat pour finir notre démonstration des résultats que l'on a énoncé.

Définition 4.4.1. Soit A un G-module satisfaisant l'axiome du corps de classes, et soit $(\deg : G \to \widehat{\mathbb{Z}}, v : A_k \to \widehat{\mathbb{Z}})$ une théorie du corps de classes. Pour tout corps K, on définit une topologie sur A_K par : pour tout $a \in A_K$, on prend les $aN_{L/K}A_L$, avec L/K parcourant les extensions galoisiennes finies de K, pour base de voisinage de a. Cette topologie est appelée la *topologie de la norme* sur A_K.

On va voir que cette topologie est très proche de la topologie de Krull que l'on a défini précédemment.

Proposition 4.4.2. *(i) Les sous-groupes ouverts de A_K sont exactement les sous-groupes fermés d'indice fini.*
(ii) La valuation $v_K : A_K \to \widehat{\mathbb{Z}}$ est continue.
(iii) Si L/K est une extension finie, alors $N_{L/K} : A_L \to A_K$ est continue.
(iv) A_K est séparé si et seulement si le groupe $A_K^0 = \cap_L N_{L/K}A_L$, appelé groupe des normes universel, est trivial.

Démonstration. (i) Si $\mathscr{N}$ est un sous-groupe de A_K, alors

$$\mathscr{N} = A_K \setminus \cup_{a\mathscr{N} \neq \mathscr{N}} a\mathscr{N}.$$

Maintenant, si $\mathscr{N}$ est ouvert, alors les $a\mathscr{N}$ aussi, et alors $\mathscr{N}$ est fermé. Comme $\mathscr{N}$ doit contenir un voisinage $N_{L/K}A_L$ de 1, et comme $N_{L/K}A_L$ est d'indice fini (c'est l'axiome du corps de classes), on en déduit que $\mathscr{N}$ est d'indice fini.
Réciproquement, si $\mathscr{N}$ est fermé d'indice fini, alors l'union, finie, des $a\mathscr{N}$ tels que $a\mathscr{N} \neq \mathscr{N}$ est un ouvert, dont $\mathscr{N}$ est le complémentaire. Il est donc bien fermé.

(ii) Les groupes $f\widehat{\mathbb{Z}}$, avec $f \in \mathbb{N}^*$, forment une base de voisinages ouverts de $0 \in \widehat{\mathbb{Z}}$. Si L/K est une extension non ramifiée de degré $f = f_{L/K}$, alors on a vu (dans la sous-partie "Frobenius et éléments premiers") que $v_K(N_{L/K}A_L) = fv_L(A_L) \subset f\widehat{\mathbb{Z}}$. On en déduit la continuité de v_K.

(iii) Soit $N_{M/K}A_M$ un voisinage ouvert de $1 \in A_K$. Alors :

$$N_{L/K}(N_{(ML)/L}A_{ML}) = N_{ML/K}(A_{ML}) \subset N_{M/K}(A_M),$$

et on en déduit la continuité de $N_{L/K}$.

(iv) Ce dernier point est direct : étant donné $a \in A_K$, que le groupe des normes universel soit trivial revient à voir qu'on peut séparer 1 et a.

□

On en déduit le résultat de correspondance sur les extensions abéliennes L/K :

Théorème 4.4.3. *L'application*

$$L \mapsto \mathscr{N}_L = N_{L/K} A_L$$

fournit une correspondance bijective entre extensions abéliennes finies L/K et sous-groupes ouverts $\mathscr{N}$ de A_K. En outre,

$$L_1 \subset L_2 \Leftrightarrow \mathscr{N}_{L_1} \supset \mathscr{N}_{L_2},\ \mathscr{N}_{L_1 L_2} = \mathscr{N}_{L_1} \cap \mathscr{N}_{L_2},\ \mathscr{N}_{L_1 \cap L_2} = \mathscr{N}_{L_1} \mathscr{N}_{L_2}.$$

Si L correspond au sous-groupe ouvert $\mathscr{N}$ de A_K, alors L est appelé le corps de classes de $\mathscr{N}$. On a de plus $G(L/K) \simeq A_K/\mathscr{N}$.

Démonstration. Si L_1 et L_2 sont deux extensions abéliennes de K, alors on a directement $\mathscr{N}_{L_1 L_2} \subset \mathscr{N}_{L_1} \cap \mathscr{N}_{L_2}$. Si, réciproquement, $a \in \mathscr{N}_{L_1} \cap \mathscr{N}_{L_2}$, alors l'élément $(a, L_1 L_2/K) \in G(L_1 L_2/K)$ s'envoie trivialement sur $G(L_i/K)$, c'est-à-dire, $(a, L_i/K) = 1$, pour $i = 1, 2$. Ainsi, $(a, L_1 L_2/K) = 1$, soit $a \in \mathscr{N}_{L_1 L_2}$. On a donc bien $\mathscr{N}_{L_1 L_2} = \mathscr{N}_{L_1} \cap \mathscr{N}_{L_2}$. Ainsi, $\mathscr{N}_{L_1} \supset \mathscr{N}_{L_2} \Leftrightarrow \mathscr{N}_{L_1} \cap \mathscr{N}_{L_2} = \mathscr{N}_{L_1 L_2} = \mathscr{N}_{L_2} \Leftrightarrow [L_1 L_2 : K] = [L_2 : K] \Leftrightarrow L_1 \subset L_2$..

Ceci montre directement l'injectivité de la correspondance $L \mapsto \mathscr{N}_L$.

Si $\mathscr{N}$ est un sous-groupe ouvert, alors il contient le groupe de normes $\mathscr{N}_L = N_{L/K} A_L$ pour une certaine extension galoisienne L/K. Mais alors, vu l'isomorphisme réalisé par l'application de réciprocité, comme $\mathscr{N}_L = \mathscr{N}_{L^{\mathrm{ab}}}$, on peut supposer L/K extension abélienne. Or, $(\mathscr{N}, L/K) = G(L/L')$ pour un certain corps intermédiaire L' de l'extension L/K. Comme $\mathscr{N} \supset \mathscr{N}_L$, le groupe $\mathscr{N}$ est exactement l'image réciproque de $G(L/L')$ par l'application $(\ , L/K) : A_K \to G(L/K)$, et ainsi, est exactement le noyau de l'application $(\ , L'/K) : A_K \to G(L'/K)$. On a alors $\mathscr{N} = \mathscr{N}_{L'}$. Ceci montre bien que la correspondance $L \mapsto \mathscr{N}_L$ est surjective.

Enfin, on peut montrer l'égalité $\mathscr{N}_{L_1 \cap L_2} = \mathscr{N}_{L_1} \mathscr{N}_{L_2}$. $L_1 \cap L_2 \subset L_i$, donc $\mathscr{N}_{L_1 \cap L_2} \supset \mathscr{N}_{L_i}$, pour $i = 1, 2$. On a alors $\mathscr{N}_{L_1 \cap L_2} \supset \mathscr{N}_{L_1} \mathscr{N}_{L_2}$. Comme $\mathscr{N}_{L_1} \mathscr{N}_{L_2}$ est ouvert, on a déjà montré que $\mathscr{N}_{L_1} \mathscr{N}_{L_2} = \mathscr{N}_L$ pour une certaine extension abélienne L/K. Comme $\mathscr{N}_{L_i} \subset \mathscr{N}_L$ implique $L \subset L_1 \cap L_2$, vu ce qu'on a montré précédemment, alors $\mathscr{N}_{L_1} \mathscr{N}_{L_2} = \mathscr{N}_L \supset \mathscr{N}_{L_1 \cap L_2}$.

Pour finir, la dernière affirmation est directe par l'isomorphisme réalisé par l'application de réciprocité. □

4.5 Extensions infinies

Soit A un G-module satisfaisant l'axiome du corps de classes et soit ($\deg : G \to \widehat{\mathbb{Z}}$, $v : A_k \to \widehat{\mathbb{Z}}$) une théorie du corps de classes.

Nous allons essayer d'étendre la loi de réciprocité aux extensions infinies. Ainsi, dans la suite, K sera une extension quelque entre k et $\overline{k}$. On va définir A_K un sous-G-module associé à K, même si en toute généralité, on aura $A_K \neq A^{G_K}$: pour K_α et K_β deux extensions finies de k avec $K_\beta \supset K_\alpha$, on peut définir l'application norme $N_{K_\beta/K_\alpha} : A_{K_\beta} \to A_{K_\alpha}$. Vu le comportement de la norme, on forme un système projectif $\left\{A_{K_\alpha},\, N_{K_\beta/K_\alpha}\right\}$ et on peut définir :

$$A_K = \varprojlim A_{K_\alpha}.$$

Si L/K est une extension (de degré fini ou infini), alors pour chaque sous-extension finie L_α/k de L/k, on a l'application de norme : $N_{L_\alpha/K_\alpha} : A_{L_\alpha} \to A_{K_\alpha}$, où $K_\alpha = K \cap L_\alpha$. En passant aux limites projectives, on obtient alors directement un homomorphisme canonique : $N_{L/K} : A_L \to A_K$.

Si $M \supset L \supset K$ sont deux extensions, alors on montre facilement que $N_{M/K} = N_{L/K} \circ N_{M/L}$.

Si L/K est une extension galoisienne, alors A_L est un $G(L/K)$-module. En effet, si L_α parcourt les sous-extensions finies de L/k telles que $L_\alpha/K_\alpha = K \cap L_\alpha$ est galoisienne, alors $A_L = \varprojlim_{\leftarrow} A_{L_\alpha}$, et chaque A_{L_α} a une structure de $G(L/K)$-module à travers l'homomorphisme naturel $G(L/K) \to G(L_\alpha/K_\alpha)$.

Si L/K est une extension finie, on a aussi l'inclusion $A_K \subset A_L$ et $A_K = A_L^{G(L/K)}$ si L/K est une extension galoisienne (ceci est bien cohérent avec la notation que l'on utilisait précédemment).

Pour voir cela, si L_α/k parcours les sous-extensions finies de L/k, soit $K_\alpha = K \cap L_\alpha$. Comme L/K est supposée finie, on a $L = L_\alpha K$ si $L_\alpha \supset L_{\alpha_0}$ pour un certain α_0. Ainsi, si $L_\beta \supset L_\alpha \supset L_{\alpha_0}$, alors on a le diagramme commutatif siuvant :

$$\begin{array}{ccc} A_{K_\beta} & \hookrightarrow & A_{L_\beta} \\ {\scriptstyle N_{K_\beta/K_\alpha}}\downarrow & & \downarrow{\scriptstyle N_{L_\beta/L_\alpha}} \\ A_{K_\alpha} & \hookrightarrow & A_{L_\alpha} \end{array}$$

En passant à la limite projective, on obtient une injection $A_K = \varprojlim_{\leftarrow} A_{K_\alpha} \hookrightarrow \varprojlim_{\leftarrow} A_{L_\alpha} = A_L$. Il ne reste plus qu'à identifier A_K à son image par cette application.

Par ailleurs, si L/K est une extension galoisienne, alors L_α/K_α est aussi galoisienne si L_α est assez grande, et on a $A_L^{G(L/K)} = \varprojlim_{\leftarrow} A_{L_\alpha}^{G(L/K)} = \varprojlim_{\leftarrow} A_{K_\alpha} = A_K$.

Maintenant, on se restreint aux corps K dont le degré d'inertie $f_K = [K \cap \tilde{k} : k]$ est fini. Alors $\deg$ induit un homomorphisme surjectif $\deg_K = \frac{1}{f_K} \deg$, $G_K \to \widehat{\mathbb{Z}}$, qui détermine la $\widehat{\mathbb{Z}}$-extension $\tilde{K} = K\tilde{k}$.

D'un autre côté, si $K_\beta \supset K_\alpha$ sont deux sous-extensions finis de K/k et si K_α contient $K \cap \tilde{k}$, alors on montre que $K_\beta \cap \tilde{K_\alpha} = K_\alpha$. En effet, comme $K \cap \tilde{k} \subset K_\alpha$, la tour d'extension $K \cap \tilde{k} \subset K_\alpha \subset K_\beta \subset K$ est totalement ramifiée, et ainsi $K_\beta \cap \tilde{K_\alpha} = K_\alpha$, ou autrement dit $f_{K_\beta . K_\alpha} = 1$.

On a ainsi, avec $Z = v(A_K)$, le diagramme commutatif suivant :

$$\begin{array}{ccc} A_{K_\beta} & \xrightarrow{v_{K_\beta}} & Z \\ {\scriptstyle N_{K_\beta/K_\alpha}}\downarrow & & \| \\ A_{K_\alpha} & \xrightarrow{v_{K_\alpha}} & Z \end{array}$$

En passant à la limite projective, on obtient un homomorphisme $v_K : A_K \to Z$.

Si L/K est une extension de corps avec degrés d'inertie finis f_L et f_K, alors on montre que les diagrammes suivant sont commutatifs :

$$\begin{array}{ccc} G_L & \xrightarrow{\deg_L} & \widehat{\mathbb{Z}} \\ \downarrow & & \downarrow \\ G_K & \xrightarrow{\deg_K} & \widehat{\mathbb{Z}} \end{array} \qquad \begin{array}{ccc} A_L & \xrightarrow{v_L} & Z \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ A_K & \xrightarrow{v_K} & Z \end{array}$$

Par contre, v_k n'est pas, a priori une valuation hensélienne puisqu'elle n'est pas nécessairement surjective sur Z.

Axiome 3. *Pour toute sous-extension finie de K/k et $\overline{k}/k$, le groupe A_K séparé pour la topologie de la norme, et U_K est compact.*

Proposition 4.5.1. *Si K est un corps d'indice d'inertie sur k $f_K < +\infty$, alors $v_K : A_K \to \widehat{\mathbb{Z}}$ est une valuation henselienne par rapport à $\deg_K$, d'image $Z = v(A_k)$.*

Démonstration. Vu le diagramme précédent, il suffit de montrer que $v_K(A_K) = Z$ et on va voir qu'il s'agit d'une conséquence directe de l'axiome de séparation que l'on a pris. En effet, si $K_\beta \supset K_\alpha \supset K \cap \tilde{k}$ sont des extensions finies de K/k, alors $f_{K_\beta/K_\alpha} = 1$ (on l'a remarqué plus haut) et on a le diagramme exact :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_{K_\beta} & \longrightarrow & A_{K_\beta} & \xrightarrow{v_{K_\beta}} & Z & \longrightarrow & 0 \\ & & \downarrow & & {\scriptstyle N_{K_\beta/K_\alpha}}\downarrow & & \| & & \\ 1 & \longrightarrow & U_{K_\alpha} & \longrightarrow & A_{K_\alpha} & \xrightarrow{v_{K_\alpha}} & Z & \longrightarrow & 0 \end{array}$$

constitué de groupes topologiques et de morphismes continus. Comme les U_{K_γ} sont compacts, on peut passer à la limite projective (voir [1], page 34, pour une référence) avec $U_K = \lim_{\leftarrow} U_{K_\alpha}$ pour obtenir la suite exacte $1 \to U_K \to A_K \to Z \to 0$. □

Nous allons maintenant pouvoir prouver l'axiome du corps de classes pour les extensions infinies de k.

Proposition 4.5.2. *Pour toute extension finie cyclique L/K de K, avec $f_K < +\infty$, on a $\sharp H^0(G(L/K), A_L) = [L : K]$, et $\sharp H^{-1}(G(L/K), A_L) = 0$.*

Démonstration. Soit $i = 0$ ou -1.

Soit L_α/k qui parcourt les sous-extensions finies de L/k et soit $K_\alpha = K \cap L_\alpha$. Alors $L = KL_\alpha$ et L_α/K_α est galoisienne, de groupe de Galois $G(L_\alpha/K_\alpha) \simeq G(L/K)$ (c'est encore le résultat de [7]), pour $L_\alpha \supset L_{\alpha_0}$.

Si $L_\beta \supset L_\alpha$, on a les $G(L/K)$-homomorphismes : $A_L \to^{N_{L/L_\beta}} A_{L_\beta} \to^{N_{L_\beta/L_\alpha}} A_{L_\alpha}$. Ceux-ci induisent des homomorphismes : $H^i(G(L/K), A_L) \to H^i(G(L/K), A_{L_\beta}) \to H^i(G(L/K), A_{L_\alpha})$. La seconde flèche est un isomorphisme. En effet, le premier résultat de fonctorialité suivant la démonstration de la bonne définition de l'application de réciprocité, combiné avec le fait que celle-ci soit un isomorphisme sur les extensions finis, donne la surjectivité, et comme les groupes ont, vu l'axiome du corps de classes, même cardinal, on a le résultat.

Il reste donc à montrer que l'homomorphisme obtenu en passant à la limite projective, $H^i(G(L/K), A_L) \to \lim_{\leftarrow} H^i(G(L/K), A_{L_\alpha})$, est bijective, le groupe de droite étant cyclique d'ordre $[L : K]$ pour $i = 0$ et étant le groupe trivial pour $i = -1$.

On considère, avec $I_L = \lim_{\leftarrow} U_{L_\alpha}$, le diagramme exact suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_L & \longrightarrow & A_L & \xrightarrow{v_L} & Z & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & U_{L_\alpha} & \longrightarrow & A_{L_\alpha} & \xrightarrow{v_{L_\alpha}} & Z & \longrightarrow & 0 \end{array}$$

On peut, en utilisant un hexagone exact donné par Herbrand, proposion 3.2.11, se ramener, comme dans la preuve de la première proposition découlant du premier axiome, à montrer que $H^i(G(L/K), U_L) \simeq \lim_{\leftarrow} H^i(G(L/K), U_{L_\alpha})$. On va voir que cela vient de la compacité de U_{L_α} et U_L. En effet, pour tout α, on a la suite exacte $1 \to N_{L_\alpha/K_\alpha} U_{L_\alpha} \to U_{K_\alpha} \to H^0(G(L/K), U_{L_\alpha}) \to 1$ de groupes topologiques. En admettant encore une fois qu'on peut passer à la limite projective, on obtient la suite exacte

$$1 \to \lim_{\leftarrow} N_{L_\alpha/K_\alpha} U_{L_\alpha} \to U_K \to \lim_{\leftarrow} H^0(G(L/K), U_{L_\alpha}) \to 1$$

. Par définition de la norme $N_{L/K}$, on a $N_{L/K} U_L = \lim_{\leftarrow} N_{L_\alpha/K_\alpha} U_{L_\alpha}$, et ainsi, $\lim_{\leftarrow} H^0(G(L/K), U_{L_\alpha}) = U_K/N_{L/K} U_L = H^0(G(L/K), U_L)$.

Pour le cas $i = -1$, la démonstration est très similaire, en considérant la suite exacte : $1 \to I_{G(L/K)} U_\alpha \to {}_{N_{G(L/K)}} U_\alpha \to H^{-1}(G(L/K), U_L)$. □

Mais alors, les deux propositions précédentes montrent que ($\deg_K : G_K \to \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$, $v_K : A_K \to \widehat{\mathbb{Z}}$) est une théorie du corps de classes. On peut alors appliquer le théorème d'isomorphisme de l'application de réciprocité pour obtenir :

Théorème 4.5.3. *Si L/K est une extension galoisienne finie de K une extension de k avec f_K, alors*

$$r_{L/K} \,:\, G(L/K)^{ab} \to A_K/N_{L/K}A_L$$

est un isomorphisme.

De la même manière qu'avant, on obtient un homomorphisme surjectif $(\,, L/K) : A_K \to G(L/K)^{\mathrm{ab}}$, qui s'étend à des extensions galoisiennes quelconques L/K, en prenant la limite projective.

On peut alors montrer, directement par des arguments similaires à ceux développés précédemment, ou en passant à la limite projective, que le symbole résiduel de normes vérifie encore une propriété de fonctorialité :

Proposition 4.5.4. *Soit L/K et L'/K' deux extensions galoisiennes (de degré fini ou infini) telles que $K \subset K'$, $L \subset L'$ et $f_K, f_{K'} < +\infty$. Alors le diagramme :*

$$\begin{array}{ccc} A_{K'} & \xrightarrow{(\,,L'/K')} & G(L'/K')^{ab} \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow \\ A_K & \xrightarrow{(\,,L/K)} & G(L/K)^{ab} \end{array}$$

est commutatif.

5 Théorie du corps de classes local

Dans cette dernière partie, nous allons voir que les corps locaux, ou au moins certains d'entre eux, vérifient, d'une certaine manière, les axiomes du corps de classes, et que l'on peut leur appliquer les résultats que l'on a montré dans la partie précédente. Enfin, on verra pour conséquence le théorème de Kronecker-Weber, sur lequel s'achèvera ce document.

5.1 L'axiome du corps de classes

Soit K un corps local, de corps résiduel fini. A_K sera le groupe multiplicatif K^*, et nous allons voir que nous pouvons bien lui appliquer la théorie précédente. Pour cela on va commencer par voir que l'on connait une décomposition du groupe K^*. On notera $U_K^{(n)} = 1 + m_K^n$, p la caractéristique de k_K et $q = \sharp k_K$. On supposera la valuation sur K, v_K, normalisée : $v_K(K^*) = \mathbb{Z}$.

Proposition 5.1.1. *Le groupe K^* admet la décomposition en produit direct suivante :*

$$K^* = (\pi) \times \mu_{q-1} \times U_K^{(1)}$$

De plus, on a une chaîne $U_K \supset U_K^{(1)} \supset U_K^{(2)} \supset \dots$ *telle que* $U_K/U_K^{(1)} \simeq k_K^*$ *et* $U_K^{(n)}/U_K^{(n+1)} = k_K$.

Démonstration. On prend π une uniformisante de K. Alors, si $a \in K^*$, a a une décomposition unique en $a = \pi^{v_K(a)}u$, avec $u \in U_K$. Le groupe U_K contient le groupe μ_{q-1} car, par le lemme de Hensel, le polynôme $X^{q-1} - 1 = 0$ est scindé sur K.

Le morphisme $U_K \to k_K^*$, $u \mapsto u \mod m_K$ envoie bijectivement μ_{q-1} sur k_K^*. Il est de noyau $U_K^{(1)}$.

Ceci montre que $U_K = \mu_{q-1} \times U_K^{(1)}$ et $U_K/U_K^{(1)} \simeq k_K^*$.

On a de plus un homomorphisme surjectif $U_K^{(n)} \to k_K$, $1 + a\pi^n \mapsto a \mod m_K$, de noyau $U_K^{(n+1)}$, et ainsi $I_K^{(n)}/U_K^{(n+1)} \simeq k_K$. □

Remarque. Les groupes $U_K^{(n)} = \left\{x \in K^* \middle/ |x-1| < \frac{1}{q^{n-1}}\right\}$ forment une base de voisinages ouverts et compacts de $1 \in K^*$.

Démonstration. En effet, la compacité vient du fait que $U_K^{(n)}$ est la limite projective $U_K^{(n)} = \lim_{\leftarrow} U_K^{(n)}/U_K^{(n+v)}$, et les groupes $U_K^{(n)}/U_K^{(n+v)}$ sont finis. □

Remarque. Or, on a directement $U_K = \bigcup_{\zeta \in \mu_{q-1}} \zeta U_K^{(1)}$ qui est donc ouvert et compact, et K^* est alors un groupe localement compact : tout élément $a \in K^*$ a un voisinage ouvert compact, aU_K.

Théorème 5.1.2. *Si* K *est une extension finie de* $\mathbb{Q}_p$, *et si* $e = v_K(p)$ *et si* $n > \frac{e}{p-1}$, *alors les séries entières* $\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$ *et* $\log(1+x) = x - \frac{x^2}{2!} + \frac{x^3}{3!} - \dots$. *donnent des isomorphismes (et homéomorphismes) réciproques :* $m_K^n \underset{\log}{\overset{\exp}{\rightleftarrows}} U_K^{(n)}$

Démonstration. Soit $v = v_K$. On pose pour $x \in K$, $|x| = q^{-\frac{1}{[K:\mathbb{Q}_p]}v_K(x)}$ (on rappelle que $q = \sharp k_K$). Soit $x \in K$ tel que $v(x) > \frac{e}{p-1}$, ou de manière équivalente, $|x| < p^{-\frac{1}{p-1}}$. Si $p^r \leqslant v < p^{r+1}$ et $v \geqslant 2$, alors

$$\log_p |\frac{x^v}{v}| - \log_p |x| = (v-1)\log_p |x| - \log_p |v| < -\frac{v-1}{p-1} - r < 0.$$

Ceci montre que $\frac{x^v}{v}$ tend vers 0 si $v \to +\infty$ et $|\frac{x^v}{v}| < |x|$, donc la série $\log(1+x)$ converge et vérifie $v(\log(1+x)) = v(x)$. Ainsi, si $n > \frac{e}{p-1}$, alors log envoie $U_K^{(n)}$ sur m_K^n.

D'un autre côté, on considère maintenant les termes $|\frac{x^v}{v!}|$. En écrivant $v = a_0 + \dots + a_r p^r$, avec $0 \leqslant a_i \leqslant p-1$.

Pour considérer la série exponentielle, on va montrer que $val_p(v!) = \frac{E(v-(a_0+\cdots+a_r))}{p-1}$.

En effet, on a : $E(\frac{v}{p}) = a_1 + \cdots + a_r p^{r-1}$, $E(\frac{v}{p^2}) = a_2 + \cdots + a_r p^{r-2}$, $\ldots$, et $E(\frac{v}{p^r}) = a_r$. Il y a $E(\frac{v}{p^i})$ éléments de $1, 2, \ldots, v$ qui sont divisibles par p^i. En effet, cela est direct vu qu'un tel nombre est de la forme $\alpha p^i \leqslant v$.

On en déduit que

$$val_p(v!) = E(\frac{v}{p}) + \cdots + E(\frac{v}{p^r}) = a_1 + (p-1)a_2 + \cdots + (p^{r-1} + \cdots + 1)a_r,$$

et donc

$$(p-1)val_p(v!) = (p-1)a_1 + (p^2-1)a_2 + \cdots + (p^r-1)a_r = v - (a_0 + \cdots + a_r),$$

ce qui prouve le résultat.

Maintenant, pour $v(x) > \frac{e}{p-1}$, ou de manière équivalente si $|x| < p^{\frac{1}{p-1}}$ et si $v \geqslant 2$, on a

$$\log_p |\frac{x^v}{v!}| = v \log_p |x| - \log_p |v!| < v \left(\log_p |x| + \frac{1}{p-1} \right)$$

et ainsi

$$\log_p |\frac{x^v}{v!}| - \log_p |x| = (v-1) \log_p |x| - \log_p |v!| < -\frac{v-1}{p-1} - \frac{1}{p-1}(v-(a_0+\cdots+a_r)) \leqslant 0.$$

Ceci montre que $\frac{x^v}{v!}$ tend vers 0 quand $v \to +\infty$, et que $|\frac{x^v}{v!}| < |x|$ pour $v \geqslant 2$. Ainsi, la série $\exp(x)$ converge et $v(\exp(x) - 1) = v(x)$.

Ainsi, si $n > \frac{e}{p-1}$, alors exp envoie m_K^n sur $U_K^{(n)}$. De plus, pour $|x|$, $|y| < p^{-\frac{1}{p-1}}$, on a

$$\exp \log(1+x) = 1 + x \text{ et } \log \exp x = x,$$

et

$$\exp(x+y) = \exp(x) \exp(y), \ \log((1+x)(1+y)) = \log(1+x) + \log(1+y).$$

En effet, ce sont des égalités de séries formelles, et toutes ces séries convergent.

On a donc montré le théorème. □

Nous pouvons maintenant fournir une démonstration du fait que les extensions finies de $\mathbb{Q}_p$ vérifient l'axiome du corps de classes. Pour une version plus générale concernant les corps locaux, on peut se référer à *Artin & Tate* [8].

Théorème 5.1.3. *Si L/K est une extension cyclique finie d'un corps local, alors $\sharp H^0(G(L/K), L^*) = [L : K]$ et $\sharp H^{-1}(G(L/K), L^*) = 1$.*

Démonstration. Soit $G = G(L/K)$. Par le théorème de Hilbert 90, on a $H^{-1}(G, L^*) = 1$, et ainsi, le quotient de Herbrand du G-module L^* est $h(G, L^*) = \sharp H^0(G, L^*)$.

On a la suite exacte de G-modules

$$1 \to U_L \to L^* \to^{v_L} \mathbb{Z} \to 0$$

dans laquelle $\mathbb{Z}$ est vu comme un G-module trivial.

On en déduit que

$$h(G, L^*) = h(G, \mathbb{Z})h(G, U_L) = [L : K]h(G, U_L).$$

Il reste donc à prouver que $h(G, U_L) = 1$. Soit $n > \frac{e}{p-1}$, $e = v_L(p)$. Alors, par le théorème précédent, $U_L^{(n)} \simeq m_L^n$. Comme $U_L/U_L^{(n)}$ est fini, on a vu à la proposition 3.2.13 que $h(G, U_L/U_L^{(n)}) = 1$, et on a :

$$h(G, U_L) = h(G, U_L/U_L^{(n)})h(G, U_L^{(n)}) = h(G, m_L^n).$$

Maintenant, soit $\{\tau\alpha / \tau \in G\}$ une base normale de L/K (ce qui existe car on a pris une extension galoisienne finie). Soit M le G-module :

$$M = \bigoplus_{\tau \in G} O_K \tau\alpha = \bigoplus_{\tau \in G} \tau B,$$

avec $B = O_K\alpha$. Alors, vu la définition, $M = M_G(B)$, avec $g = \{1\}$.

En multipliant éventuellement α par π_K^l pour un l assez grand, $\alpha\pi_K^l$ donne toujours une base normale de L/K, mais le G-module M est alors inclus dans m_L^n. On peut donc supposer que M est un sous-module ouvert (O_K est ouvert) de m_L^n. Mais alors, m_L^n/M est fini et on a $h(G, m_L^n) = h(G, m_L^n/M)h(G, M) = 1 \times h(g, B)$ avec $g = \{1\}$. On en déduit que $h(G, U_L) = h(G, m_L^n) = h(g, B) = 1$, et on a le résultat. □

Corollaire 5.1.4. *Si L/K est une extension finie non ramifiée, alors pour $i = -1$ ou 0, on a $H^i(G(L/K), U_L) = 1$ et $H^i(G(L/K), U_L^{(n)}) = 1$ pour $n \in \mathbb{N}^*$.*

En particulier, $N_{L/K}U_L = U_K$ et $N_{L/K}U_L^{(n)} = U_K^{(n)}$.

Démonstration. Soit $G = G(L/K)$. On va d'abord montrer que $H^i(G, k_L^*) = 1 = H^i(G, k_L)$. Il suffit de le montrer pour $i = -1$ car $h(G, k_L^*) = h(G, k_L) = 1$ comme k_L est fini.

Maintenant, par le théorème de Hilbert 90, $H^{-1}(G, k_L^*) = 1$.

Si on pose ϕ pour le Frobenius de k_L/k_K et $f = [k_L : k_K]$, on a :

$$\sharp_{N_G(k_L)}k_L = \sharp \left\{ x \in k_L / \sum_{i=0}^{f-1} x^{\phi^i} = \sum_{i=0}^{f-1} x^{q^i} = 0 \right\} \leqslant q^{f-1}$$

et $\sharp I_G k_L = q^{f-1}$ comme $I_G k_L$ est l'image de l'application $\phi - 1 : k_L \to k_L$, qui est k_K pour noyau, et donc $\sharp I_G k_L = \frac{\sharp k_L}{\sharp k_K} = q^{f-1}$. Ainsi, $H^{-1}(G, k_L) = {}_{N_G} k_L / I_G k_L = 0$.

Maintenant, $H^i(G, U_L) = 1$ pour $i = 0, -1$. Ceci vient du théorème précédent. Les extensions finies non ramifiées sont cycliques sur K, puique k_K est fini. Cela donne le premier axiome admis pour définir l'application de réciprocité (voir l'axiome 1), dont un corollaire est exactement ce résultat.

On peut alors appliquer l'hexagone exact, développé lors de la sous-partie sur le quotient de Herbrand, à la suite exacte $1 \to U_L^{(1)} \to U_L \to k_L^* \to 1$. Si π est un élément premier de K, alors π est aussi un élément premier de L (l'extension est supposée non ramifiée), donc $U_L^{(n)} \to k_L$, $1 + a\pi^n \mapsto a \mod m_L$, est un G-homomorphisme. En considérant la suite exacte

$$1 \to U_L^{(n+1)} \to U_L^{(n)} \to k_L \to 0$$

de G-modules, on trouver de la même manière que plus haut, par récurrence, on trouve $H^i(G, U_L^{(n+1)}) = H^i(G, U_L^{(n)}) = 1$ puisque $H^i(G, k_L) = 0$.

Enfin, le fait que $N_{L/K} U_L^{(n)} = (U_L^{(n)})^G = U_K^{(n)}$ repose alors sur le fait qu'un élément premier π de K est un élément premier de L. □

Proposition 5.1.5. *Si $m \in \mathbb{N}^*$, si on pose K^{*m} et U_K^m les groupes des puissances m-èmes de K^* et de U_K, alors on a :*

$$(K^* : K^{*m}) = m(U_K : U_K^m) = \frac{m}{|m|_p} \sharp \mu_m(K).$$

Les groupes U_K^m forment une base de voisinages ouverts de 1 dans K^*.

Démonstration. On peut voir tout groupe abélien comme un G-module trivial, avec G cyclique d'ordre m. Par les mêmes arguments que pour la preuve du théorème précédent, on a

$$h(G, K^*) = mh(G, U_K) = mh(G, m_K^n),$$

$n > \frac{e}{p-1}$, $e = v_K(p)$, et ainsi :

$$h(G, U_J) = \frac{(U_K : U_K^m)}{\sharp \mu_m(K)} = (m_K^n : m \times m_K^n) = (m_K^n : m_K^{n+v_K(m)}) = q^{v_K(m)} = \frac{1}{|m|_p},$$

et $(K^* : K^{*m}) = m(U_K : U_K^m)$. Ceci montre la formule pour l'indice.

U_K^m est ouvert car il contient le sous-groupe ouvert

$$(U_K^{(n)})^m = \exp(m \times m_K^n) = \exp(m_K^{n+v_K(m)}) = U_K^{(n+v_K(m))}.$$

Si $n \in \mathbb{N}^*$ et si $m = (U_K : U_K^{(n)})$, alors $U_K^m \subset U_K^{(n)}$, ce qui montre que les U_K^m forment une base de voisinages de 1.

□

5.2 Corps de classes local

5.2.1 Rappels et notations

Ce paragraphe a pour but de fixer les notations et appliquer quelques résultats que l'on a montré, afin de pouvoir conclure lors du paragraphe suivant.

Soit k un corps local, $\overline{k}$ sa clôture séparable, $G = G(\overline{k}/k)$, $\tilde{k}$ son extension maximale non ramifiée. On a vu que $\tilde{k}$ est engendrée par les racines de l'unité d'ordre premier à $p = car(O_k/m_k)$. Le groupe de Galois $G(\tilde{k}/k)$ est topologiquement engendré par l'automorphisme de Frobenius $\phi_k \in G(\tilde{k}/k)$ qui est donné par $a^{\phi_k} = a^{\sharp k_k} \mod m_{\tilde{k}}$, pour $a \in O_{\tilde{k}}$.

Si L/k est une sous-extension finie de $\tilde{k}/k$, alors le groupe de Galois $G(L/K)$ est cyclique, et engendré par $\phi_{L/k} = (\phi_k)_{|L}$. Si $n = [L : k]$, alors on a l'isomorphisme canonique $G(L/k) \simeq \mathbb{Z}/n\mathbb{Z}$ qui envoie $\phi_{L/k}$ sur $1 \mod n\mathbb{Z}$. En passant à la limite projective, on obtient un homéomorphisme $G(\tilde{k}/k) \simeq \widehat{\mathbb{Z}}$, qui envoie ϕ_k sur 1, et un morphisme surjectif $\deg : G \to \widehat{\mathbb{Z}}$.

Si K/k est une extension finie le nombre $f_K = f_{K/k} = [K \cap \tilde{k} : k]$ est le degré d'inertie. deg induit un homomorphisme surjectif $\deg_K = \frac{1}{f_K} \deg : G_K \to \widehat{\mathbb{Z}}$ qui détermine l'extension maximale non ramifiée de K, $\tilde{K} = K\tilde{k}$. À travers l'isomorphisme $G(\tilde{K}/K) \simeq \widehat{\mathbb{Z}}$ qu'on en déduit, $\phi_K \in G(\tilde{K}/K)$, l'élément qui est envoyé sur 1, est le Frobenius de $\tilde{K}/K$, avec $(\phi_K)_{\tilde{k}} = \phi_k^{f_K}$, ainsi $a^{\phi_K} = a^{\phi_k^{f_k}} = a^{q_k^{f_K}} = a^{q_K} \mod m_{\tilde{k}}$ si $a \in O_{\tilde{k}}$, et ainsi pour tout $a \in O_{\tilde{K}}$ car $\tilde{K} = K\tilde{k}$.

On considère le G-module $A = \overline{k}^*$. Si K/k est une extension finie, alors $A_K = K^*$. La valuation normalisée usuelle $v : k^* \to \mathbb{Z} \subset \widehat{\mathbb{Z}}$ est henselienne par rapport à deg, vu ce que l'on a pu voir lors des deux premières parties sur les valuations. Comme, par la sous-partie précédente, A vérifie l'axiome du corps de classes, le couple ($\deg : G \to \widehat{\mathbb{Z}}$, $v : k^* \to \widehat{\mathbb{Z}}$) est une théorie du corps de classes. On en déduit alors que l'on a la *loi de réciprocité locale* :

Théorème 5.2.1. *Pour toute extension galoisienne L/K d'un corps local K, on a l'isomorphisme canonique :*

$$r_{L/K} : G(L/K)^{\mathrm{ab}} \to K^*/N_{L/K}L^*.$$

On rappelle la définition de $r_{L/K}$: si $\sigma \in G(L/K)$ et $\tilde{\sigma} \in \phi(\tilde{L}/K)$ un relevé de Frobenius, relevé de σ à $\tilde{L}$ tel que $\deg_K(\tilde{\sigma}) \in \mathbb{N}$, ou encore $\tilde{\sigma}_{|\tilde{K}} = \phi_K^n$. Si Σ est le corps fixé par $\tilde{\sigma}$ et π_Σ un élément premier de Σ, alors $r_{L/K}(\sigma) = N_{\Sigma/K}(\pi_\Sigma) \mod N_{L/K}L^*$. L'inverse de $r_{L/K}$ permet de définir le symbole résiduel de norme, $(\,, L/K) : K^* \to G(L/K)^{\mathrm{ab}}$, de noyau $N_{L/K}L^*$.

5.2.2 La classification des extensions abéliennes

Dans ce qui suit, on ne s'intéresse qu'à des corps locaux de caractéristique nulle.

Théorème 5.2.2. *L'application*

$$L \mapsto \mathscr{N}_L = N_{L/K}L^*$$

est une correspondance bijective entre les extensions abéliennes finies L d'un corps local K et les sous-groupes $\mathscr{N}$ d'indice fini de K^*. De plus, on a

$$L_1 \subset L_2 \Leftrightarrow \mathscr{N}_{L_1} \supset \mathscr{N}_{L_2},\ \mathscr{N}_{L_1L_2} = \mathscr{N}_{L_1} \cap \mathscr{N}_{L_2},\ \mathscr{N}_{L_1 \cap L_2} = \mathscr{N}_{L_1}\mathscr{N}_{L_2}.$$

Démonstration. Par ce que l'on a déjà démontré dans la partie précédente, nous avons juste à montrer que les sous-groupes d'indice fini $\mathscr{N}$ dans K^* sont exactement les sous-groupes ouverts de K^* pour la topologie de la norme.

Si $\mathscr{N}$ est un sous-groupe ouvert, alors il est d'indice fini. En effet, il contient, étant ouvert, un groupe de normes $N_{L/K}L^*$, avec L/K extension galoisienne finie, et par le théorème précédent, $G(L/K)^{\text{ab}} \simeq K^*/N_{L/K}L^*$, et ainsi $N_{L/K}L^*$ est d'indice fini, et donc $\mathscr{N}$ aussi.

Réciproquement, si $(K^* : \mathscr{N}) = m$ est fini, alors $\mathscr{N} \supset K^{*m}$. En effet, si $x \in K^*$, $x = an$ avec $n \in \mathscr{N}$, $a \in K^*$, $x^m = a^m n^m$ et comme $K^*/\mathscr{N}$ est d'ordre m, $a^m = 1$ dans $K^*/\mathscr{N}$, et $x^m \in \mathscr{N}$. Nous allons maintenant montrer que K^{*m} contient un groupe de normes, et l'on pourra conclure. Pour cela, nous allons utiliser les résultats développés plus haut sur la théorie de Kummer.

Tout d'abord, on peut supposer que K^* contient le groupe μ_m des racines m-ème de l'unité. En effet, si ce n'est pas le cas, on pose $K_1 = K(\mu_m)$ et si on a le résultat pour K_1, alors K_1^{*m} contient un groupe de normes $N_{L_1/K_1}L_1^*$ et si L/K est une extension galoisienne finie contenant L_1, alors :

$$N_{L/K}L^* = N_{K_1/K}(N_{L/K_1}L^*) \subset N_{K_1/K}(N_{L_1/K_1}L_1^*) \subset N_{K_1/K}(K_1^{*m}) \subset K^{*m}.$$

La première inclusion vient directement de la définition de la norme et du deuxième théorème d'isomorphisme : $G_{K_1}/G_{L_1} = (G_{K_1}/G_L)/(G_{L_1}/G_L)$. La seconde est une de nos hypothèses. Ceci permet de conclure pour ce cas.

Maintenant, si $\mu_m \subset K$, on pose $L = K(\sqrt[m]{K^*})$ l'extension abélienne maximale d'exposant m. Alors on a vu que :

$$Hom(G(L/K), \mu_m) \simeq K^*/K^{*m}.$$

On a aussi vu, dans la proposition 5.1.5, que K^*/K^{*m} est fini, donc, $G(L/K)$ étant abélien d'exposant m, il est aisé de voir qu'il est inclus dans son bidual, et donc lui aussi fini.

Comme $K^*/N_{L/K}L^* \simeq G(L/K)$ est d'exposant m, on a $K^{*m} \subset N_{L/K}L^*$ et par l'isomorphisme plus haut, on obtient $\sharp K^*/K^{*m} = \sharp G(L/K) = \sharp(K^*/N_{L/K}L^*)$, et ainsi, on peut en déduire que $K^{*m} = N_{L/K}L^*$. □

Au passage, on a aussi prouvé que :

Corollaire 5.2.3. *Si $X^m - 1$ est scindé que K et si $L = K(\sqrt[m]{K^*})$, alors*

$$N_{L/K}L^* = K^{*m} \text{ et } G(L/K) \simeq K^*/K^{*m}.$$

ce théorème est souvent appelé *théorème d'existence* d'une théorie du corps de classes locale, car il dit que pour tout sous-groupe $\mathscr{N}$ d'indice fini de K^*, il existe un corps de classes, c'est-à-dire une extension L/K avec $N_{L/K}L^* = \mathscr{N}$.

Tout sous-groupe $\mathscr{N} \subset K^*$ d'indice fini contient un groupe de la forme $(\pi^f) \times U_K^{(n)}$ qui est aussi d'indice fini. Ainsi, toute extension abélienne finie L/K est contenu dans le corps de classes d'un groupe $(\pi^f) \times U_K^{(n)}$. Pour cette raison, les corps de classe de ces groupes ont un intérêt particulier (voir [**?**]). Nous allons maintenant considérer le fait que dans le cas $K = \mathbb{Q}_p$, on peut montrer que le corps de classes du groupe $(p) \times U_K^{(n)}$ est précisément le corps $\mathbb{Q}_p(\mu_{p^n})$ engendré par les racines p^n-èmes de l'unité.

5.3 Théorème de Kronecker-Weber

Proposition 5.3.1. *Soit ζ une racine primitive p^n-ème de l'unité et soit $K = \mathbb{Q}_p$ et $L = \mathbb{Q}_p(\zeta)$. Alors :*

(i) L/K est totalement ramifiée de degré $p^{n-1}(p-1)$.

(ii) $\lambda = \zeta - 1$ est un élément premier de L, et $N_{L/K}(-\lambda) = p$.

Démonstration. Le polynôme cyclotomique $\phi_n(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}} = X^{p^{n-1}(p-1)} + \cdots + X^{p^{n-1}} + 1$ est irréductible sur $\mathbb{Q}_p$. En effet, on peut appliquer le critère d'Eisenstein à $\phi(X+1)$, modulo p. Ainsi, c'est le polynôme minimal de ζ.

Ainsi, $[L : K] = p^{n-1}(p-1)$ et $\phi_n(X) = \prod_{\sigma \in G(L/K)}$. En prenant $X = 1$, on obtient $p = \prod_\sigma (1 - \zeta^\sigma) = N_{L/K}(1 - \zeta)$.

Comme $v_L(1 - \zeta^\sigma) = v_L(1 - \zeta)$ (σ est une isométrie), on a $v_L(1 - \zeta) = \frac{v_L(p)}{[L:K]} = \frac{1}{[L:K]}$. On en déduit que L/K est totalement ramifiée et que $1 - \zeta$ en est un élément premier. On a bien montré ce que l'on souhaitait. □

Théorème 5.3.2. *Le groupe de normes de $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ est le groupe $(p) \times U_{\mathbb{Q}_p}^{(n)}$.*

Démonstration. On va encore écrire $K = \mathbb{Q}_p$ et $L = \mathbb{Q}_p(\mu_{p^n})$. L'application $m_K \to m_K^s$ donnée par $a \mapsto p^{s-1}(p-1)a$ est un isomorphisme. Comme on a vu que exp est un isomorphisme pour $m_K^v \to U_K^{(v)}$ avec $v \geqslant 1$ pour $p \neq 2$ et $v \geqslant 2$ pour $p = 2$, et comme exp envoie l'application $a \mapsto p^{s-1}(p-1)a$ sur l'application $x \mapsto x^{p^{s-1}(p-1)}$, on en déduit :

$$(U_K^{(1)})^{p^{n-1}(p-1)} = U_K^{(n)} \text{ si } p \neq 2, \text{ et } (U_K^{(2)})^{2^{n-2}} = U_K^{(n)} \text{ pour } p = 2, \text{ si} n > 1.$$

Ceci montre que $U_K^{(n)} \subset N_{L/K}L^*$ pour $p \neq 2$. Pour $p = 2$, le cas $n = 1$ est trivial, et sinon, on remarque que :

$$U_K^{(2)} = U_K^{(3)} \cup 5U_K^{(3)} = (U_K^{(2)})^2 \cup 5(U_K^{(2)})^2.$$

En effet, un nombre congru à 1 mod 4 et soit congru à 1 mod 8, soit congru à 5 mod 8. On a alors :

$$U_K^{(n)} = (U_K^{(2)})^{2^{n-1}} \cup 5(U_K^{(2)})^{2^{n-1}}.$$

On a directement que $5^{2^{n-2}} = N_{L/K}(2+i)$ $(i^2 = -1)$, et ainsi, on a aussi $U_K^{(n)} \subset N_{L/K}L^*$ pour $p = 2$.

Par la proposition précédente, on peut déduire que $(p) \times U_K^{(n)} \subset N_{L/K}L^*$.

Comme ces deux derniers groupes sont d'indice $p^{n-1}(p-1)$ dans K^* (par définition ou vu la proposition précédente), on en déduit l'égalité $N_{L/K}L^* = (p) \times U_K^{(n)}$. □

Comme conséquence, on en déduit d'abord une version locale du théorème de Kronecker-Weber.

Corollaire 5.3.3 (Kronecker-Weber)**.** *Toute extension abélienne finie $L/\mathbb{Q}_p$ est contenue dans un corps $\mathbb{Q}_p(\zeta)$, avec ζ une racine de l'unité. En d'autres termes, l'extension abélienne maximale $\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p$ est obtenue en prenant toutes les racines de l'unité.*

Démonstration. On a $(p^f) \times U_{\mathbb{Q}_p}^{(n)} \subset N_{L/\mathbb{Q}_p}L^*$ pour un certain f et un certain n. Ainsi, L est contenue dans un corps de classes M du groupe :

$$(p^f) \times U_{\mathbb{Q}_p}^{(n)} = ((p^f) \times U_{\mathbb{Q}_p}) \cap ((p) \times U_{\mathbb{Q}_p}^{(n)}).$$

Or, notre théorème de correspondance nous dit que M est le composé du corps de classes de $(p^f) \times U_{\mathbb{Q}_p}$, qui est une extension non-ramifiée de degré f, et le corps de classes $\mathbb{Q}_p(\mu_{p^n})$ de $(p) \times U_{\mathbb{Q}_p}^{(n)}$. Ainsi, M est bien engendré par les $(p^f - 1)p^n$-ème racines de l'unité. □

On peut déduire de cette forme locale du théorème de Kronecker-Weber sa forme globale :

Théorème 5.3.4 (Kronecker-Weber)**.** *Toute extension abélienne finie $L/\mathbb{Q}$ est contenue dans un corps $\mathbb{Q}(\zeta)$, avec ζ une racine de l'unité.*

Démonstration. Soit S l'ensemble des nombres premiers qui se ramifient dans L (S est fini, voir par exemple [3] page 49). Soit L_p le complété de L par rapport

à une extension de v_p. Alors $L_p/\mathbb{Q}_p$ est abélienne, donc $L_p \subset \mathbb{Q}_p(\mu_{n_p})$ pour un certain n_p. Soit $e_p = v_p(n_p)$, et soit :

$$n = \prod_{p \in S} p^{e_p}.$$

Montrons que $L \subset \mathbb{Q}(\mu_n)$. Soit $M = L(\mu_n)$. Alors $M/\mathbb{Q}$ est abélienne et si p se ramifie dans $M/\mathbb{Q}$, alors p se ramifie dans $L/\mathbb{Q}$. Aussi, si M_p est le complété de M pour une extension correcte de v_p, alors :

$$M_p = L_p(\mu_n) \subset \mathbb{Q}_p(\mu_{p^{e_p} n'}) = \mathbb{Q}_p(\mu_{p^{e_p}})\mathbb{Q}_p(\mu_{n'})$$

avec $(n', p) = 1$. Comme $\mathbb{Q}_p(\mu_{n'}) = \mathbb{Q}_p$ est non ramifiée, le groupe d'inertie I_p de $M_p/\mathbb{Q}_p$ est isomorphe à $G(\mathbb{Q}_p(\mu_{p^{e_p}})/\mathbb{Q}_p)$, qui est d'ordre $\phi(p^{e_p})$, avec ϕ l'indicatrice d'Euler. Soit $I \subset G(M/\mathbb{Q})$ le groupe engendré par tout les I_p avec p ramifié dans L. Le corps fixé par I est non ramifié sur $\mathbb{Q}$, et par le théorème de Minkowski (voir [3] page 207), est égal à $\mathbb{Q}$. Ainsi, $I = G(M/\mathbb{Q})$.

D'un autre côté, on a :

$$\sharp I \leqslant \prod_{p \in S} \sharp I_p = \prod_{p \in S} \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}],$$

et ainsi $[M : \mathbb{Q}] = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$, donc $M = \mathbb{Q}(\mu_n)$, ce qui montre que $L \subset \mathbb{Q}(\mu_n)$. □

Conclusion

Au final, connaître les extensions abéliennes revient à connaître, dans les cas que nous avons considérés, le groupe K^*, plus simple en général. Pour en arriver là, on aura défini $\mathbb{Q}_p$ et ses extensions. On aura aussi vu que toute extension abélienne de $\mathbb{Q}$ est incluse dans une extension cyclotomique. Les outils que l'on a développé : cohomologie, théorie du corps de classes générale,... sont utiles pour poursuivre vers la théorie du corps de classes global, voir [1]. Par contre, celle-ci est plus difficile. Quand à l'étude des extensions non-abéliennes, elle constitue encore un sujet de recherche.

Remerciements

Je souhaite remercier Xavier Caruso pour avoir encadré mon stage, en particulier par la clarté de ses réponses à mes questions. Merci aussi à David Lubicz et Jérémy Le Borgne pour toute l'aide qu'ils ont pu m'apporter durant ce stage, grâce à leur grande disponibilité envers toutes mes questions.

Références

[1] Neukirch, Jürgen Class Field Theory (Springer, 1986)

[2] Serre, Jean-Pierre Corps locaux (Hermann, 1968)

[3] Neukirch, Jürgen Algebraic Number Theory (Springer, 1999)

[4] Colmez, Pierre Cours de M2 (http ://www.math.jussieu.fr/ colmez/M2.html, 2005-2009)

[5] Robert, Alain M. A course in p-adic analysis

[6] Gozard, Ivan Théorie de Galois (Ellipses, 1997)

[7] Lang, Serge Algèbre (Dunod, 2004, 3ème édition)

[8] Artin, Emil & Tate, John Class Field Theory (Benjamin, New York-Amsterdam 1967)

[9] Chambert-Loir, Antoine & Coste, Michel Calculer une enveloppe convexe (préparation à l'agrégation, option Calcul formel, université de Rennes 1) : http ://perso.univ-rennes1.fr/antoine.chambert-loir/2007-08/agreg/convex.pdf