Le Théorème de Kronecker-Weber Local

Giancarlo Lucchini Servetto, Li Wang

Sous la direction de Benjamin Schraen

École Normale Supérieure

Juin 2009

Table des matières

Introduction Le théorème de Kronecker-Weber affirme que chaque extension abélienne de $\mathbb{Q}$ est contenue dans une extension cyclotomique. La preuve de ce théorème est assez compliquée. Néanmoins, il y a une version analogue sur une famille de corps obtenues à partir de $\mathbb{Q}$: les corps p-adiques $\mathbb{Q}_p$. On appelle cette version le théorème de Kronecker -Weber local. Dans cet article on donne une preuve complète de ce résultat comme une façon d'introduire les corps p-adiques. Le théorème de Kronocker-Weber peut être obtenu à partir de ce dernier de façon élémentaire, d'où l'intérêt d'étudier ces corps.

1 Construction de $\mathbb{Q}_p$

La construction du corps $\mathbb{Q}_p$ à partir du corps $\mathbb{Q}$ des nombres rationnels, ne diffère de celle de $\mathbb{R}$ qu'en la façon de "mesurer" la distance entre les nombres. C'est-à-dire, ce qui change est la notion de valeur absolue des nombres. On commence alors par introduire des nouvelles formes de construire des valeurs absolues.

1.1 Valuations discrètes

Définition 1.1. Soit K un corps, une *valuation discrète* sur K est une surjection

$$v : K^* \to \mathbb{Z}$$

qui satisfait :

i) $v(xy) = v(x) + v(y) \quad \forall x, y \in K$;

ii) $v(x+y) \geq \min\{v(x), v(y)\} \quad \forall x, y \in K$.

Remarque 1.2. On peut étendre v à tout K avec la convention $v(0) = \infty$.

Pour p premier, pour tout $x \in \mathbb{Q}^*$ il existe un unique $n = n(x)$ dans $\mathbb{Z}$ tel que $x = p^n \frac{a}{b}$ avec $\text{pgcd}(p,a) = \text{pgcd}(p,b) = 1$. On vérifie que l'application

$$\mathbb{Q}^* \to \mathbb{Z}, \quad x \mapsto n(x)$$

est une valuation de $\mathbb{Q}$ que l'on notera v_p.

Proposition 1.3. *Soit K un corps muni d'une valuation discrète v. L'ensemble*

$$\mathcal{O} = \{x \in K : v(x) \geq 0\}$$

est un sous-anneau de K. L'ensemble

$$\mathcal{P} = \{x \in K : v(x) > 0\}$$

est le seul idéal maximal de $\mathcal{O}$. En fait, si $\pi \in \mathcal{P}$ vérifie $v(\pi) = 1$, alors tout idéal non nul de $\mathcal{O}$ est de la forme $\mathcal{P}^n = \pi^n \mathcal{O}$ avec $n \geq 1$.

En particulier, tout élément de $\mathcal{O} \setminus \mathcal{P}$ est inversible dans $\mathcal{O}$.

Démonstration. Il est clair par les propriétés des valuations discrètes que $\mathcal{O}$ est un sous-anneau de K et que $\mathcal{P}$ est un idéal de $\mathcal{O}$. De plus, on vérifie aisément que tout élement dans $\mathcal{O} \setminus \mathcal{P}$ est inversible dans $\mathcal{O}$: si $v(x) = 0$, alors $v(x^{-1}) = -v(x) = 0$ et donc $x^{-1} \in \mathcal{O}$.

Soit I un idéal non nul de $\mathcal{O}$, en considérant l'ensemble $\{v(x) : x \in I\}$, on choisit $a \in I$ avec $n = v(a)$ minimal. On affirme que $I = a\mathcal{O} = \pi^n(a\pi^{-n})\mathcal{O} = \pi^n\mathcal{O}$ (notons que $v(a\pi^{-n}) = 0$). Soit $x \in I$, alors $v(x) \geq v(a)$ donc $v(xa^{-1}) \geq 0$ et $xa^{-1} \in \mathcal{O}$, i.e. $x \in a\mathcal{O}$. □

Définition 1.4. On appelle $\mathcal{O}$ l'*anneau de valuation* de (K,v)et $\mathcal{P}$ l'*idéal de valuation*. Si π est un générateur de $\mathcal{P}$, on dit que π est une *uniformisante* de K. Le corps $\kappa = \mathcal{O}/\mathcal{P}$ est appelé le *corps résiduel* de (K,v).

Corollaire 1.5. *Pour tout $n \in \mathbb{N}$, on a $\mathcal{P}^n/\mathcal{P}^{n+1} \simeq \kappa$ (en les regardant comme des groupes additifs).*

Démonstration. D'après la proposition précédente, on sait que $\mathcal{P}^n = \pi^n\mathcal{O}$ et par conséquent,

$$\mathcal{P}^n/\mathcal{P}^{n+1} \to \mathcal{O}/\mathcal{P}, \quad x\pi^n \mapsto x \mod \mathcal{P}$$

est l'isomorphisme voulu. □

Corollaire 1.6. *On a l'égalité :*

$$K^* = \pi^{\mathbb{Z}}\mathcal{O}^*,$$

où $\mathcal{O}^* = \mathcal{O} \setminus \mathcal{P}$ est le groupe des unités de $\mathcal{O}$.

Démonstration. Soit $x \in K^*$ et $v(x) = n$ alors $v(x\pi^{-n}) = 0$. Donc $x\pi^{-n} \in \mathcal{O}^*$, i.e. $x \in \pi^n\mathcal{O}^*$. L'unicité de cette écriture est évidente. □

1.2 Valeurs absolues

Définition 1.7. Soit K un corps. Une *valeur absolue* définie sur K est une fonction

$$|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$$

qui satisfait :

i) $|x| = 0$ si et seulement si $x = 0$;

ii) $|xy| = |x||y| \quad \forall x, y \in K$;

iii) $|x + y| \leq |x| + |y| \quad \forall x, y \in K$.

Le couple $(K, |\cdot|)$ est appelé un *corps valué*.

Une valeur absolue est dite *triviale* si pour tout $x \in K^*$, $|x| = 1$. On considérera uniquement des valeurs absolues non triviales.

On dira que la valeur absolue est *ultramétrique* si en plus

iv) $|x + y| \leq \max\{|x|, |y|\} \quad \forall x, y \in K$ (inégalité triangulaire forte ou *ultramétrique*).

On dira que la valeur absolue est *discrète* si en plus

v) $|K^*| = \{|x| : x \in K^*\}$ est un sous-groupe discret de $(R_{>0}, \cdot)$, i.e. $|K^*| = r^{\mathbb{Z}}$ pour certain $r > 1$.

Proposition 1.8. *Soit v une valuation discrète sur K et $r > 1$. Alors la fonction*

$$|x| = r^{-v(x)}$$

définit une valeur absolue discrète et ultramétrique sur K (avec la convention $|0| = r^{-\infty} = 0$). Récriproquement, si $|\cdot|$ est une valeur absolue discrète et ultramétrique sur K et $|K^*| = r^{\mathbb{Z}}$, alors l'application

$$v : K^* \to \mathbb{Z}, \quad x \mapsto -\log_r |x|$$

définit une valuation discrète sur K.

Démonstration. La mulitiplicativité de $|\cdot|$ vient de la propriété i) de la Définition 1.1. L'inégalité triangulaire forte découle du fait que

$$v(x + y) \geq \min\{v(x), v(y)\}.$$

Pour la réciproque, c'est la multiplicativité de $|\cdot|$ qui nous donne la propriété i). Pour la propriété ii) on note que, comme $|\cdot|$ est ultramétrique et $|x| = r^{-v(x)}$, on a

$$r^{-v(x+y)} \leq \max\{r^{-v(x)}, r^{-v(y)}\}$$

d'où l'inégalité $v(x + y) \geq \min\{v(x), v(y)\}$. □

On appelle valeur absolue *p-adique* sur $\mathbb{Q}$ la valeur absolue définie par

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

Notons que les valeurs absolues donnent aux corps une structure d'espace métrique (avec la distance $d(x, y) = |x - y|$). Si la valeur absolue est ultramétrique, on dit que la distance est *ultramétrique* et $(K, |\cdot|)$ est un espace *ultramétrique*.

Remarque 1.9. Soit $(K, |\cdot|)$ un corps valué avec $|\cdot|$ induite par une valuation discrète v. Alors $\mathcal{O} = \overline{B}(0,1) = \{x \in K : |x| \leq 1\}$ et $\mathscr{P} = B(0,1) = \{x \in K : |x| < 1\}$. On note que $\{\mathscr{P}^n : n \in \mathbb{N}\}$ est un système fondamental de voisinages de 0.

Définition 1.10. On dit que deux valeurs absolues sur un corps K sont *équivalentes* si elles définissent la même topologie sur K.

Proposition 1.11. *Soient $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur K. Les affirmations suivantes sont équivalentes.*

i) $|\cdot|_1$ *et* $|\cdot|_2$ *sont équivalentes ;*

ii) $\forall x \in K$, $|x|_1 < 1$ *si et seulement si* $|x|_2 < 1$ *;*

iii) Il existe $\alpha > 0$ *tel que* $\forall x \in K$, $|x|_1 = |x|_2^\alpha$.

Démonstration. i)⇒ii) : si $|\cdot|_1$ et $|\cdot|_2$ définissent la même topologie dans K et $(x_n)_{n\in\mathbb{N}}$ est une suite dans K, on a que $(x_n)_{n\in\mathbb{N}}$ converge pour $|\cdot|_1$ si et seulement si elle converge pour $|\cdot|_2$. Or, la suite $(x^n)_{n\in\mathbb{N}}$ converge vers 0 dans $|\cdot|_1$ si et seulement si $|x|_1 < 1$, et de même dans $|\cdot|_2$, d'où le résultat en découle.

ii)⇒iii) : en prenant x^{-1} à la place de x dans la propriété ii), on voit que $|x|_1 > 1 \Leftrightarrow |x|_2 > 1$ et donc $|x|_1 = 1 \Leftrightarrow |x|_2 = 1$. Soit alors $x_0 \in K^*$ avec $|x_0|_1 \neq 1$ et $\alpha > 0$ tel que $|x_0|_1 = |x_0|_2^\alpha$. En prenant x_0^{-1} si nécéssaire, on peut supposer que $|x_0|_1 > 1$. On veut montrer que α est le nombre souhaité. Pour $|x|_1 = 1$, le résultat est vérifié. Soient alors $x \in K^*$ avec $|x|_1 \neq 1$, $\beta > 0$ tel que $|x|_1 = |x|_2^\beta$ et $\gamma \in \mathbb{R}$ tel que $|x|_1 = |x_0|_1^\gamma$. On doit montrer que $\beta = \alpha$. Pour $n \in \mathbb{N}$, soit $m = m(n) \in \mathbb{Z}$ le seul entier tel que $\frac{m}{n} \leq \gamma < \frac{m+1}{n}$. On a alors l'inégalité

$$|x_0|_1^{\frac{m}{n}} \leq |x|_1 < |x_0|_1^{\frac{m+1}{n}}$$

et en utilisant les définitions de α et β on obtient

$$|x_0|_2^{\alpha\frac{m}{n}} \leq |x|_2^\beta < |x_0|_2^{\alpha\frac{m+1}{n}}. \tag{1}$$

Or, la première equation, peut se récrire de la façon suivante

$$\left|\frac{x_0^m}{x^n}\right|_1 \leq 1 < \left|\frac{x_0^{m+1}}{x^n}\right|_1.$$

Et par hypothèse on a

$$\left|\frac{x_0^m}{x^n}\right|_2 \leq 1 < \left|\frac{x_0^{m+1}}{x^n}\right|_2$$

et finalement

$$|x_0|_2^{\frac{m}{n}} \leq |x|_2 < |x_0|_2^{\frac{m+1}{n}}$$

$$|x_0|_2^{\alpha\frac{m}{n}} \leq |x|_2^\alpha < |x_0|_2^{\alpha\frac{m+1}{n}}. \tag{2}$$

En faisant $n \to \infty$ dans les équations (1) et (2) on trouve

$$|x|_2^\beta = |x_0|_2^{\gamma\alpha} = |x|_2^\alpha,$$

et alors $\beta = \alpha$, ce qui conclut.

iii)⇒i) Les boules sont les mêmes. □

Avec cette proposition, on peut classifier les valeurs absolues sur $\mathbb{Q}$ à équivalence près.

Théorème 1.12 (Ostrowski)**.** *Si on appelle $|\cdot|_\infty$ la valeur absolue classique, toute valeur absolue non-triviale sur $\mathbb{Q}$ est équivalente à l'une des valeurs absolues $|\cdot|_p$ où p est un nombre premier ou ∞.*

Démonstration. Supposons d'abord que $|n| \leq 1$ pour tout $n \in \mathbb{N}$. Comme $|\cdot|$ est non-trivial, il existe $p \in \mathbb{N}$ premier tel que $|p| < 1$, car si $n = ab$ et $|n| < 1$, alors $|a| < 1$ ou $|b| < 1$. Supposons qu'il existe un autre nombre premier q tel que $|q| < 1$. Prenons donc $m \in \mathbb{N}$ tel que $|p^m| < 1/2$ et $|q^m| < 1/2$. Comme $\text{pgcd}(p^m, q^m) = 1$, il existent $a, b \in \mathbb{Z}$ tels que $ap^m + bq^m = 1$, et on trouve la contradiction

$$1 = |1| = |ap^m + bq^m| \leq |a||p^m| + |b||q^m| \leq |p^m| + |q^m| < \frac{1}{2} + \frac{1}{2} = 1.$$

Donc $|p| = |p|_p^\alpha$ pour certain $\alpha > 0$ et $|q| = 1$ pour tout q premier différent de p. Le théorème fondamental de l'arithmétique nous dit alors que $|n| = |n|_p^\alpha$ pour tout $n \in \mathbb{N}$ et par conséquent, $|x| = |x|_p^\alpha$ pour tout $x \in \mathbb{Q}$.

Supposons maintenant qu'il existe $n \in \mathbb{N}$ tel que $|n| > 1$. Soit $\alpha > 0$ tel que $|n| = n^\alpha$. Pour $m \in \mathbb{N}$ on regarde son écriture en base n. C'est-à-dire, $m = \sum_{i=0}^k m_i n^i$ avec $0 \leq m_i < n$ et $m_k \neq 0$. Notons que l'inégalité triangulaire nous dit que $|m| = |1 + 1 + \cdots + 1| \leq 1 + 1 + \cdots + 1 = m$ pour tout entier positif m. Alors

$$\begin{aligned} |m| = \left|\sum_{i=0}^k m_i n^i\right| &\leq \sum_{i=0}^k |m_i||n^i| \leq \sum_{i=0}^k (n-1)n^{\alpha i} \leq (n-1)n^{\alpha k} \sum_{i=0}^k n^{-\alpha i} \\ &\leq (n-1)n^{\alpha k} \sum_{i=0}^\infty n^{-\alpha i} \leq n^{\alpha k} \frac{(n-1)n^\alpha}{n^\alpha - 1} \leq m^\alpha \frac{(n-1)n^\alpha}{n^\alpha - 1}, \end{aligned}$$

où la dernière inégalité vient du fait que $m \geq n^k$. Alors, si on pose $C = \frac{(n-1)n^\alpha}{n^\alpha - 1}$ on a $|m| \leq Cm^\alpha$ pour tout entier positif m. En particulier, pour tout $N \in \mathbb{N}$,

$$\begin{aligned} |m^N| &\leq Cm^{N\alpha}, \\ |m| &\leq \sqrt[N]{C} m^\alpha. \end{aligned}$$

En faisant $N \to \infty$ on a $\sqrt[N]{C} \to 1$ et on trouve finalement, pour tout $m \in \mathbb{N}$

$$|m| \leq m^\alpha.$$

Pour l'autre direction, on pose $a = n^{k+1} - m$, alors $0 < a \leq n^{k+1} - n^k$. En utilisant ce qu'on vient de montrer,

$$|a| \leq a^\alpha \leq (n^{k+1} - n^k)^\alpha.$$

Donc, par l'inégalité triangulaire,

$$\begin{aligned} |m| &\geq |n^{k+1}| - |a| \\ &\geq n^{(k+1)\alpha} - (n^{k+1} - n^k)^\alpha \\ &\geq n^{(k+1)\alpha} \left[1 - \left(1 - \frac{1}{n}\right)^\alpha\right] \\ &\geq C' n^{(k+1)\alpha} \\ &\geq C' m^\alpha, \end{aligned}$$

où $C' = 1-(1-1/n)^\alpha$ ne dépend que de n. Alors par le même raisonnement qu'avant, on trouve, pour tout $m \in \mathbb{N}$

$$|m| \geq m^\alpha.$$

Donc on a finalement, pour tout $m \in \mathbb{N}$

$$|m| = m^\alpha = |m|_\infty^\alpha$$

d'où on tire le résultat pour tout $x \in \mathbb{Q}$ par multiplicativité. □

1.3 Complétion

On a parlé des corps valués en général. Les corps qu'on veut étudier, les corps $\mathbb{Q}_p$, ne sont rien de plus que la complétion de $\mathbb{Q}$ par rapport à la distance induite par la valeur absolue $|\cdot|_p$. On montre alors la procédure de complétion d'un corps valué. Pour des démonstrations des lemmes qu'on ne montre pas, voir [6], chapitre II-3.

Définition 1.13. Un homomorphisme de corps $\sigma : K \to L$ est appelé un *homomorphisme de corps valués* entre $(K, |\cdot|)$ et $(L, |\cdot|')$ si pour tout $x \in K$, $|\sigma(x)|' = |x|$.

Théorème 1.14. *Soit $(K, |\cdot|)$ un corps valué. Il existe $(\hat{K}, \|\cdot\|)$ corps valué complet et $\sigma : (K, |\cdot|) \to (\hat{K}, \|\cdot\|)$ homomorphisme de corps valués avec les propriétés suivantes :*

i) $\sigma(K)$ est dense dans $\hat{K}$;

ii) Si $(L, |\cdot|')$ est un corps valué complet et $\tau : (K, |\cdot|) \to (L, |\cdot|')$ un homomorphisme de corps valués, alors il existe un unique homomorphisme de corps valués $\tau' : (\hat{K}, \|\cdot\|) \to (L, |\cdot|')$ tel que $\tau = \tau' \circ \sigma$.

Le couple $((\hat{K}, \|\cdot\|), \sigma)$ est unique à isomorphisme de corps valués près. On l'appelle le complété de K.

Démonstration. On suit la complétion standard d'un corps, en identifiant suites de Cauchy équivalentes. Soient

$$\mathscr{C} = \{\text{suites de Cauchy dans K}\},$$

$$\mathscr{N} = \{\text{suites de Cauchy convergeant vers 0, i.e. suites } (a_n) \text{ avec } a_n \to 0\},$$

et définissons la somme et la multiplication des suites terme à terme

$$(a_n) + (b_n) = (a_n + b_n),$$

$$(a_n)(b_n) = (a_n b_n).$$

Tout d'abord, on note que

Lemme 1.15. *$\mathscr{C}$ est un anneau et $\mathscr{N}$ est un idéal maximal de $\mathscr{C}$.*

On définit $\hat{K} = \mathscr{C}/\mathscr{N}$, qui est bien un corps par le dernier lemme. Alors σ est défini de façon naturelle :

$$\begin{aligned} \sigma : \ & K \to \hat{K} \\ & a \to (a) \mod \mathscr{N} \end{aligned}$$

où (a) dénote la suite avec terme constante a. Alors σ est bien un homomorphisme de corps, injectif car $\sigma(1_K) = 1_{\hat{K}}$. On identifie K avec son image $\sigma(K)$ dans $\hat{K}$ et notera $\{a_n\} = (a_n) \mod \mathscr{N}$ un élément de $\hat{K}$.

Lemme 1.16. *L'application*

$$\|\cdot\| : \hat{K} \to \mathbb{R}_{>0}, \|\{a_n\}\| = \lim_{n\to\infty} |a_n|$$

définit une valeur absolue sur $\hat{K}$ dont la réstriction à K coïncide avec $|\cdot|$.

Lemme 1.17. *$\hat{K}$ est complet par rapport à $\|\cdot\|$.*

On a alors que $(\hat{K}, \|\cdot\|)$ est un corps valué et $\sigma : (K, |\cdot|) \to (\hat{K}, \|\cdot\|)$ est un homomorphisme de corps valués.

Maintenant, la propriété i) découle du lemme suivant :

Lemme 1.18. *Tout élément de $\hat{K}$ est la limite d'une suite dans $\sigma(K)$. Donc $\sigma(K)$ est dense dans $\hat{K}$.*

Démonstration. Pour $\{a_n\} \in \hat{K}$ on a

$$\{a_n\} = \lim_{n\to\infty} \sigma(a_n)$$

En fait, on voit que pour $n \in \mathbb{N}$ tel que $|a_m - a_n| < \varepsilon$ si $m \geq n$ on a

$$\|\{a_n\} - \sigma(a_n)\| = \lim_{m\to\infty} |a_m - a_n| \leq \sup_{m\geq n} |a_m - a_n| \leq \varepsilon.$$

□

Ensuite, pour montrer la propriété ii), on se donne un corps $(L, |\cdot|')$ valué et complet, et $\tau : (K, |\cdot|) \to (L, |\cdot|')$ homomorphisme de corps valués. On définit $\tau' : (\hat{K}, \|\cdot\|) \to (L, |\cdot|')$ comme

$$\tau'(\{a_n\}) = \lim_{n\to\infty} \tau(a_n).$$

On vérifie que ceci est bien défini : si (a_n) est une suite de Cauchy pour $|\cdot|$, alors $|\tau(a_n)|' = |a_n|$ implique que $(\tau(a_n))$ est une suite de Cauchy pour $|\cdot|'$, ce qui donne l'existence de la limite. On vérifie aussi que $\tau = \tau' \circ \sigma$.

Pour l'unicité de τ', soit τ'' un homomorphisme de corps valués satisfaisant $\tau'' \circ \sigma = \tau$. Alors par le Lemme 1.18, pour tout $\{a_n\} = \lim_{n\to\infty} \sigma(a_n)$ on a

$$\tau''(\{a_n\}) = \lim_{n\to\infty} \tau''(\sigma(a_n)) = \lim_{n\to\infty} \tau(a_n) = \tau'(\{a_n\}).$$

Donc $\tau'' = \tau'$.

Finalement, si $(\hat{K}', \|\cdot\|')$ est un corps valué complet et $\sigma' : (K, |\cdot|) \to (\hat{K}', \|\cdot\|')$ est un homomorphisme de corps qui satisfait la propiété ii), alors par hypothèse, il existe des homomorphismes de corps valués

$$\upsilon : (\hat{K}, \|\cdot\|) \to (\hat{K}', \|\cdot\|')$$
$$\upsilon' : (\hat{K}', \|\cdot\|') \to (\hat{K}, \|\cdot\|)$$

tels que $\upsilon \circ \sigma = \sigma'$ et $\upsilon' \circ \sigma' = \sigma$. Alors $\upsilon' \circ \upsilon \circ \sigma = \sigma$ et $\upsilon \circ \upsilon' \circ \sigma' = \sigma'$ et par la propriété d'unicité on a $\upsilon' \circ \upsilon = id_{\hat{K}}$ et $\upsilon \circ \upsilon' = id_{\hat{K}'}$. Donc $(\hat{K}, \|\cdot\|)$ et $(\hat{K}', \|\cdot\|')$ sont isomorphes.

□

Remarque 1.19. Si $|\cdot|$ sur K est discrète et ultramétrique ou, de façon équivalente, $|\cdot|$ est induite par une valuation discrète v, alors $\|\cdot\|$ est discrète sur $\hat{K}$ et $\|\hat{K}^*\| = |K^*|$, car les suites convergentes dans un espace discret ce sont les suites constantes à partir d'un certain rang. Alors, d'après la Proposition 1.8 et la continuité du logarithme, v s'étend uniquement sur $\hat{K}$ de la façon suivante :

$$\hat{v}(\{a_n\}) = \lim_{n\to\infty} v(a_n).$$

On notera abusivement $\|\cdot\| = |\cdot|$ et $\hat{v} = v$.

On a tout maintenant pour présenter le protagoniste de cette histoire.

Définition 1.20. On appelle $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ par rapport à la valeur absolue $|\cdot|_p$. On note $\mathbb{Z}_p$ l'anneau de valuation de $\mathbb{Q}_p$ et on l'appelle *l'anneau des entiers p-adiques*.

On note que p est une uniformisante de $\mathbb{Q}_p$.

Remarque 1.21. On note que le théoreme 1.12 nous dit que les seuls complétés de $\mathbb{Q}$ par rapport à une valeur absolue sont, à isomorphisme près, $\mathbb{R}$ et $\mathbb{Q}_p$ pour p premier. On voit que ces corps ne sont pas isomorphes entre eux, car une tel isomorphisme devrait fixer $\mathbb{Z}$ et les images de $\mathbb{Z}$ par $|\cdot|_p$ sont clairement différentes pour chaque p premier ou ∞.

2 Corps locaux

Ayant défini les corps $\mathbb{Q}_p$, on voudrait commencer à regarder ses propriétes. On sait déjà qu'il s'agit d'un corps valué et on a donné quelques propriétés. Mais on veut aller plus loin. Pour cela, nous étudierons un type un peu plus général de corps, ce qui nous permettra de comprendre plus aisément les extensions de $\mathbb{Q}_p$.

2.1 Définition et propriétés

Définition 2.1. Soit $(K, |\cdot|)$ complet par rapport à la valeur absolue $|\cdot|$ induite par une valuation discrète v. On dit que K est un *corps local* si son corps résiduel κ est fini.

Soit K un corps local et $(x_k)_{k\geq N}$ une suite dans K. On note $\sum_{k=N}^{\infty} x_k$ la limite de la suite convergente $s_n = \sum_{k=N}^{n} x_k$, ce qui équivaut par le *critère de Cauchy* à $x_k \to 0$ lorsque $n \to \infty$, car l'inégalite triangulaire forte nous dit

$$|s_{n+m} - s_n| \leq \max\{|x_{n+1}|, \cdots, |x_{n+m}|\}.$$

Théorème 2.2 (Théorème de Représentation)**.** *Soit K un corps local, π une uniformisante de K et soit R un système de représentants de κ contenant 0. Alors tout $x \in K^*$ s'écrit de façon unique comme une somme*

$$x = \sum_{k\geq n} \lambda_k \pi^k \qquad \lambda_k \in R, \lambda_n \neq 0, n = v(x).$$

En particulier, $n \geq 0$ ssi $x \in \mathcal{O}$.

Démonstration. Prenons $x \in \mathcal{O}^*$. On sait qu'il existe un unique $\lambda_0 \in R$ non nul tel que

$$x = \lambda_0 + \pi x_1$$

avec $x_1 \in \mathcal{O}$. En itérant cette procédure pour x_1, on obtient par récurrence

$$x = \lambda_0 + \lambda_1 \pi + \cdots + \lambda_{k-1}\pi^{k-1} + x_k \pi^k$$

avec $\lambda_0, \ldots, \lambda_{k-1} \in R$ et $x \in \mathcal{O}$. On peut écrire alors $x = s_k + x_k \pi^k$ où s_k est la somme partielle $\sum_{i=0}^{k-1} \lambda_i \pi^i$. Or, comme $|\pi| < 1$, il est clair que $|x_k \pi^k| \leq |\pi|^k \to 0$ et alors la suite (s_k) converge

vers x lorsque k tend vers l'infini. Et en notant que la somme commence en $n = 0 = v(x)$, on a le résultat pour $x \in \mathcal{O}^*$.

Maintenant, si $x \in K$, il suffit de noter qu'il existe un unique $n = v(x) \in \mathbb{Z}$ tel que $v(\pi^{-n}x) = 0$, donc $\pi^{-n}x \in \mathcal{O}^*$. Par ce qu'on vient de montrer, on voit immédiatement qu'on obtient une série pour x commençant à l'indice $k = n$. □

On donne maintenant une propriété topologique très forte des corps locaux qui nous sera utile plus tard.

Proposition 2.3. *Soit K un corps local et $\mathcal{O}$ son anneau de valuation. Alors $\mathcal{O}$ est compact et K est localement compact.*

Démonstration. Soit q le cardinal du corps residuel κ. On sait alors que $\mathcal{P}^n/\mathcal{P}^{n+1} \simeq \kappa$ est finie pour tout $n \in \mathbb{N}$. On en déduit que $\mathrm{Card}(\mathcal{O}/\mathcal{P}^n) = q^n$.

Or, comme K est complet et $\mathcal{O}$ est un fermé de K par la Remarque 1.9, il est aussi complet. Donc pour montrer la compacité de $\mathcal{O}$, il suffit de montrer que l'on peut le récouvrir avec un nombre finie de boules de rayon ϵ pour tout $\epsilon > 0$. Pour cela, soit $n \in \mathbb{N}$ tel que $r^{-n} < \epsilon$ où $|K^*| = r^{\mathbb{Z}}$ avec $r > 1$. Soient $x_1, \cdots, x_m$ des représentants des classes de $\mathcal{O}/\mathcal{P}^n$. Pour tout $x \in \mathcal{O}$, il existe $i \in \{1, \cdots, m\}$ tel que $x \equiv x_i \mod \mathcal{P}^n$ et donc $|x - x_i| \leq r^{-n} < \epsilon$, i.e. $x \in B(x_i, \epsilon)$. Alors les boules de centre x_i pour $i \in \{1, \cdots, m\}$ et rayon ϵ recouvrent $\mathcal{O}$, donc $\mathcal{O}$ est bien compact.

Finalement, K est localement compact car $\mathcal{O}$ est un voisinage compact de 0. □

Et pour terminer cette partie, on donne un résultat qui nous montre qu'en général $\mathcal{O}$ et κ sont fortement liés : On peut touours descendre de $\mathcal{O}$ à κ à travers de la restriction. Mais on peut aussi remonter de κ à $\mathcal{O}$.

Théorème 2.4 (Lemme de Hensel)**.** *Soit $f(x)$ un polynôme dans $\mathcal{O}[x]$. Si f admet une factorisation modulo $\mathcal{P}$*

$$f(x) \equiv \bar{g}(x)\bar{h}(x) \mod \mathcal{P}$$

avec $\bar{g}$ et $\bar{h}$ premiers entre eux dans $\kappa[x]$ et g unitaire, alors f admet une factorisation

$$f(x) = g(x)h(x)$$

avec g et h dans $\mathcal{O}[x]$ et g étant un "relèvement" de $\bar{g}$. C'est-à-dire, $\deg g = \deg \bar{g}$ *et* $g(x) \equiv \bar{g}(x) \mod \mathcal{P}$.

Démonstration. On construit des suites de Cauchy (g_n) et (h_n) (où on regarde la convergence coefficient par coefficient) vérifiant les propriétés

i) g_n est unitaire et $\deg g_n = \deg \bar{g}$;
ii) $g_{n+1} \equiv g_n \mod \mathcal{P}^n$ et $h_{n+1} \equiv h_n \mod \mathcal{P}^n$;
iii) $f(x) \equiv g_n(x)h_n(x) \mod \mathcal{P}^n$.

L'hypothèse du théorème nous permet de choisir $g_1 \equiv \bar{g} \mod \mathcal{P}$ et $h_1 \equiv \bar{h} \mod \mathcal{P}$. Alors, supposons qu'on a des polynômes g_n et h_n vérifiant ces propriétés. Maintenant, la propriété ii) nous oblige à poser

$$g_{n+1}(x) = g_n(x) + \pi^n r(x) \quad \text{et} \quad h_{n+1}(x) = h_n(x) + \pi^n s(x)$$

avec $r(x), s(x) \in \mathcal{O}[x]$ et π une uniformisante de K. Or, pour la propriété iii) on doit avoir

$$f(x) \equiv g_{n+1}(x)h_{n+1}(x) \mod \mathcal{P}^{n+1},$$

$$f(x) \equiv g_n(x)h_n(x) + \pi^n r(x)h_n(x) + \pi^n s(x)g_n(x) \mod \mathscr{P}^{n+1}.$$

Par hypothèse on a $f(x) - g_n(x)h_n(x) = \pi^n t(x)$ pour certain $t(x) \in \mathscr{O}[x]$. Alors

$$\pi^n t(x) \equiv \pi^n r(x)h_n(x) + \pi^n s(x)g_n(x) \mod \mathscr{P}^{n+1},$$

$$t(x) \equiv r(x)h_n(x) + s(x)g_n(x) \mod \mathscr{P}.$$

On remarque que comme $g_n \equiv \bar{g} \mod \mathscr{P}$ et $h_n \equiv \bar{h} \mod \mathscr{P}$ et $\bar{g}, \bar{h}$ sont premiers entre eux, on a que g_n et h_n le sont aussi modulo $\mathscr{P}$. Donc on sait qu'il existent des polinômes $a(x), b(x) \in \mathscr{O}[x]$ tels que

$$a(x)g_n(x) + b(x)h_n(x) \equiv 1 \mod \mathscr{P}.$$

Alors, en posant $r'(x) = b(x)t(x)$ et $s'(x) = a(x)t(x)$ on voit que $g_n(x) + \pi^n r'(x)$ et $h_n(x) + \pi^n s'(x)$ vérifient les propriétés ii) et iii).

Il nous manque encore le fait que g_{n+1} soit unitaire et de même degré que $\bar{g}$. Pour cela, il suffit que $\deg r < \deg g_n$. On définit alors $r(x) \in \mathscr{O}[x]$ comme le reste de la division euclidienne de $r'(x)$ par $g_n(x)$. C'est-à-dire

$$r'(x) = q(x)g_n(x) + r(x)$$

avec $q(x) \in \mathscr{O}[x]$. On pose finalement $s(x) = s'(x) + h_n(x)q(x)$ et on vérifie aisément qu'on a

$$r(x)h_n(x) + s(x)g_n(x) \equiv r'(x)h_n(x) + s'(x)g_n(x) \equiv t(x) \mod \mathscr{P}$$

avec $\deg r < \deg g_n$, ce qui nous permet de conclure.

Ayant les suites (g_n) et (h_n) on appelle g et h ses limites. Par la propriété iii) on a $f(x) \equiv gh \mod \mathscr{P}^n$ pour tout $n \geq 1$, et donc $f(x) = g(x)h(x)$. □

On trouve immédiatement une application pour ce théorème.

Corollaire 2.5. *Soit $f(x) = a_n x^n + \cdots + a_0$ un polynôme irréductible dans $K[x]$. Alors*

$$|f| := \max_{0 \leq i \leq n} |a_i| = \max\{|a_0|, |a_n|\}.$$

En particulier, si $a_n = 1$ et $a_0 \in \mathscr{O}$, alors $f \in \mathscr{O}[x]$.

Démonstration. Soit $m = \min_{0 \leq i \leq n} v(a_i)$. En multipliant f par π^{-m} on peut supposer que $m = 0$ (i.e. $|f| = 1$). Alors, si $r = \min\{i : |a_i| = 1\}$, on voit que

$$f(x) \equiv a_n x^n + \cdots a_r x^r \mod \mathscr{P}$$

avec $a_r \not\equiv 0 \mod \mathscr{P}$. Et alors

$$f(x) \equiv x^r(a_n x^{n-r} + \cdots a_r) \mod \mathscr{P}.$$

Donc si $r \notin \{1, n\}$, le Lemme de Hensel nous dit que f admet une factorisation non triviale dans $K[x]$, ce qui contredit l'irréducibilité de f. □

2.2 Les corps locaux $\mathbb{Q}_p$

On fait maintenant une petite parenthèse pour appliquer tous ces résultats à $\mathbb{Q}_p$.

Proposition 2.6. *On a l'égalité*

$$\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p.$$

Par conséquent, $\mathbb{Q}_p$ est un corps local.

Démonstration. Notons que si $x, y \in \{0, \cdots, p-1\}$ avec $x > y$, alors $x - y \in \{1, \cdots, p-1\}$ et donc $x - y \notin p\mathbb{Z}_p$, ce qui nous dit que les classes de ces éléments sont différentes deux à deux. Il suffit donc de montrer que pour tout élément $x \in \mathbb{Z}_p$ on peut trouver $\lambda \in \{0, \cdots, p-1\}$ tel que $\lambda - x \in p\mathbb{Z}_p$. Pour cela, on utilise le fait que $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$ (voir le Théorème 1.14). Il existe alors $a/b \in \mathbb{Q}$ avec $\text{pgcd}(a, b) = 1$ tel que

$$\left|\frac{a}{b} - x\right|_p \leq \frac{1}{p}.$$

Et en notant que $|x|_p \leq 1$, l'inégalité triangulaire forte nous dit que $|a/b|_p \leq 1$. Alors $a/b \in \mathbb{Z}_p$ et par la définition de $|\cdot|_p$, on voit que $p \nmid b$. Soient b', λ des éléments de $\{0, \cdots p-1\}$ tels que $bb' \equiv 1 \mod p$ et $\lambda \equiv ab' \mod p$. Alors

$$\lambda b \equiv a \mod p\mathbb{Z}_p,$$
$$\lambda \equiv a/b \mod p\mathbb{Z}_p.$$

Donc

$$\left|\lambda - \frac{a}{b}\right|_p \leq \frac{1}{p}.$$

En utilisant encore une fois l'inégalité triangulaire forte et les deux inégalites que nous avons, on voit que

$$|\lambda - x|_p \leq \frac{1}{p}$$

Et alors $\lambda - x \in p\mathbb{Z}_p$ comme on voulait. □

Corollaire 2.7. *On a*

$$\mathbb{Z}_p = \left\{ \sum_{k=0}^{\infty} \lambda_k p^k | \lambda_k \in \{0, \cdots, p-1\} \right\}.$$

En particulier, $\mathbb{Z}_p$ est l'adhérence de $\mathbb{Z}$ dans $\mathbb{Q}_p$.

Démonstration. Le premier énoncé est clair d'apres le Théorème de Représentation. Par la Proposition 2.3, on sait que $\mathbb{Z}_p$ est compact donc fermé dans $\mathbb{Q}_p$.

D'autre part, $\mathbb{Z} \subset \mathbb{Z}_p$, car pour $n \in \mathbb{Z}$ on a bien $v_p(n) \geq 0$. Et comme tout élement de $\mathbb{Z}_p$ est la limite de ses sommes partielles qui sont dans $\mathbb{Z}$, on voit que $\mathbb{Z}_p$ est l'adhérence de $\mathbb{Z}$ dans $\mathbb{Q}_p$. □

Proposition 2.8. *Pour chaque $n \in \mathbb{N}^*$, on note ζ_n une racine primitive n-ième de l'unité. Soit $\mu_{(p)} = \{\zeta_n \in \mathbb{Q}_p : (p, n) = 1\}$. Alors $\zeta_n \in \mu_{(p)}$ si et seulment si $n|p-1$. Autrement dit, $\mu_{(p)} = \{\zeta_{p-1}^k : k = 1, \cdots, p-1\}$.*

Démonstration. Comme $P(x) = x^{p-1} - 1$ est scindé et séparable sur $\mathbb{F}_p$, le Lemme de Hensel nous dit alors que chaque racine de P dans $\mathbb{F}_p$ se relève en une racine de P dans $\mathbb{Q}_p$. En particulier, P a $p-1$ racines deux à deux distinctes dans $\mathbb{Q}_p$. Par conséquent, $\mathbb{Q}_p$ contient ζ_{p-1}.

D'autre part, la projection canonique de $\mathbb{Z}_p$ vers $\mathbb{F}_p$ nous donne un morphisme de groupes $\rho : \mu_{(p)} \to \mathbb{F}_p^*$. Supposons qu'il existe $n > 1$ premier à p tel que $\rho(\zeta_n) = 1$. Alors,

$$x^n - 1 = (x - \zeta_n)(x-1)Q(x) \equiv (x-1)^2 Q(x) \mod p\mathbb{Z}_p$$

ce qui contredit la séparabilité de $x^n - 1$ sur $\mathbb{F}_p$ car $\text{pgcd}(p, n) = 1$. Alors, le morphisme est injectif, ce qui nous dit que $|\mu_{(p)}| \leq |\mathbb{F}_p^*|$.

Donc forcément on a $\mu_{(p)} = \{\zeta_{p-1}^k : k = 1, \cdots, p-1\}$. □

Remarque 2.9. Dans le Théorème de Représentation, on peut également choisir comme système de représentants pour $\mathbb{Q}_p$ l'ensemble $\mu_{(p)} \cup \{0\}$. C'est la *représentation de Teichmüller*.

2.3 Extensions des corps locaux

Maintenant qu'on connaît quelques propriétés des corps locaux, on voudrait regarder ses extensions en souhaitant qu'elles aient encore ces propriétés. Heureusement, on trouve que la valeur absolue s'étend de façon naturelle aux extensions finies, et de plus, de façon unique.

On rappelle quelques résultats sur les espaces vecotriels normés de dimension finie. Pour plus de détails, voir [2], chapitre II-3.

Définition 2.10. Deux normes $\|\cdot\|, \|\cdot\|'$ dans un K-espace vectoriel V sont *équivalentes* s'il existe $c, C > 0$ tels que, pour tout $x \in V$

$$c\|x\|' \leq \|x\| \leq C\|x\|'.$$

Proposition 2.11. *Soit K un corps complet par rapport à sa valeur absolue $|\cdot|$ et V un K-espace vectoriel de dimension finie. Alors toutes les normes sur V sont équivalentes.*

En fait, si $\dim_K(V) = n$ et $\{v_1, \cdots, v_n\}$ est une base de V, toute norme $\|\cdot\|$ est équivalente à la norme définie par

$$\|x\|' = \left\| \sum_{i=1}^n \lambda_i v_i \right\|' = \max_{1 \leq i \leq n} |\lambda_i|.$$

En particulier, $(V, \|\cdot\|)$ est homéomorphe à K^n muni de la topologie produit.

Corollaire 2.12. *Avec les mêmes notations, $(V, \|\cdot\|)$ est complet. Si de plus, K est localement compact, $(V, \|\cdot\|)$ l'est.*

On rappelle (voir [3], chapitre VI-5) que si $K \subset L$ une extension finie de degré n, la *norme* de L sur K est l'application

$$N_{L/K} : L \longrightarrow K$$

qui à $\alpha \in L$ associe le déterminant de l'application K-linéaire $\ell_\alpha : L \to L$ définie par $\ell_\alpha(x) = \alpha x$, c'est-à-dire

$$N_{L/K}(\alpha) = \det(\ell_\alpha).$$

Notons maintenant que, pour $\alpha, \beta \in K$ on a $\ell_{\alpha\beta} = \ell_\alpha \circ \ell_\beta$. Alors, par la propriété multiplicative du déterminant, on trouve que $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$. Aussi on note que si $\alpha \neq 0$, alors ℓ_α est inversible d'inverse $\ell_{\alpha^{-1}}$. Cela nous dit que $N_{L/K}(\alpha) = \det(\ell_\alpha) \neq 0$.

Soit $F(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in K[x]$ le polynôme caractéristique de ℓ_α. On a alors $N_{L/K}(\alpha) = (-1)^n b_0 \in K$. Et dans le même contexte, on sait que $F(x) = f_1(x)\cdots f_s(x)$ avec $f_i \in K[x]$ et $f_1|f_2|\cdots|f_s$ et $f_s(x) = f(x)$ le polynôme minimal de ℓ_α (donc de α). Comme f est irréductible, on trouve que $f_1 = \cdots = f_s = f$ et alors $F = f^s$. Donc, si on note $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ on a que $n = sm$ et alors $N_{L/K}(\alpha) = (-1)^n a_0^s$.

En particulier, si L/K est séparable et $\sigma_1, \cdots, \sigma_n$ sont les K-plongement de L dans $\bar{K}$, une clôture algébrique de K, alors

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

On montre maintenant le résultat mentioné au debut de cette section.

Théorème 2.13. *Soit K un corps local avec valeur absolue $|\cdot|$ induite par la valuation discrète v et $K \subset L$ une extension finie de degré n. Alors $|\cdot|$ s'étend de façon unique à L, i.e. il existe une valeur absolue sur L, notée abusivement $|\cdot|$, telle que sa restriction à K coïncide avec la valeur absolue sur K. Cette extension est donnée par la formule*

$$|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}.$$

En plus, on peut définir une valuation discrète w sur L qui munit L d'une structure de corps local.

Démonstration. Existence : D'abord, comme pour $\alpha \in K$ on a $N_{L/K}(\alpha) = \alpha^n$, la formule donnée coïncide avec la valeur originale. Ensuite, montrons que

$$\alpha \mapsto \sqrt[n]{|N_{L/K}(\alpha)|}$$

est bien une valeur absolue sur L. Il est clair que $\sqrt[n]{|N_{L/K}(\alpha)|} = 0$ ssi $\alpha = 0$. La propriété mulitplicative découle de la multiplicativité de la norme dont on a déjà parlé. Pour l'inégalité triangulaire forte, on montre le résultat suivant.

Lemme 2.14. *Soit $\mathcal{Q} = \{\alpha \in L$: le polynôme minimal de α sur K est dans $\mathcal{O}[x]\}$. Alors*

$$\mathcal{Q} = \{\alpha \in L : N_{L/K}(\alpha) \in \mathcal{O}\} = \{\alpha \in L : \sqrt[n]{|N_{L/K}(\alpha)|} \leq 1\}.$$

Démonstration. Soit $\alpha \in L$ et $f(x) = x^m + a_{m-1}x^{m-1}\cdots + a_0 \in K[x]$ son polynôme minimal. Si $\alpha \in \mathcal{Q}$, alors $f \in \mathcal{O}[x]$ et on a vu déjà que $N_{L/K}(\alpha) = \pm a_0^{n/m} \in \mathcal{O}$ puisque $m|n$. Réciproquement, si $\alpha \in L^*$ avec $N_{L/K}(\alpha) \in \mathcal{O}$, on a $|a_0^{n/m}| \leq 1$, alors $|a_0| \leq 1$ ou bien $a_0 \in \mathcal{O}$. Par le Corollaire 2.5, on trouve que $f \in \mathcal{O}[x]$, donc $\alpha \in \mathcal{Q}$. □

Pour montrer l'inégalité triangulaire forte, il suffit de montrer que $|\alpha + 1| \leq \max\{|\alpha|, 1\}$. Quitte à remplacer α par α^{-1}, on voudrait montrer $|\alpha| \leq 1 \Rightarrow |\alpha + 1| \leq 1$. Or, par le dernier lemme, cette dernière affirmation est équivalente à dire que $\alpha \in \mathcal{Q} \Rightarrow \alpha + 1 \in \mathcal{Q}$, ce qui est clairement vérifié.

Unicité : Soient $|\cdot|$ et $|\cdot|'$ deux valeurs absolues sur L étendant la valeur absolue de K. En particulier ce sont des normes sur le K-espace vectoriel L. Alors, par la Proposition 2.11, il existe des constantes $c, C > 0$ telles que, pour tout $x \in L$

$$c|x| \leq |x|' \leq C|x|.$$

En particulier, pour tout $n \in \mathbb{N}$,

$$c|x^n| \leq |x^n|' \leq C|x^n|,$$
$$c^{1/n}|x| \leq |x|' \leq C^{1/n}|x|,$$

et en faisant n tendre vers l'infini, on trouve que $|x| = |x|'$ pour tout $x \in L$. Donc les valeurs sont bien égales.

Il nous reste à montrer que L est aussi un corps local. Pour cela, notons que $|L^*| \subset \{\sqrt[n]{|\alpha|} : \alpha \in K\} = (r^{1/n})^{\mathbb{Z}}$, donc $|L^*|$ est bien discret. D'après la Proposition 1.8 , on note que cela suffit pour munir L d'une valuation discrète w. En regardant l'énoncé du Lemme 2.14 et la Remarque 1.9, on voit que $\mathcal{Q} = \mathcal{O}_L$, l'anneau de valuation de L.

Il nous reste à montrer que son corps residuel κ_L est fini. Or, la Proposition 2.3 et Corollaire 2.12 nous disent que L est localement compact, car L est un K-espace vectoriel de dimension finie. En particulier, $\mathcal{O}_L = \mathcal{Q} = \{\alpha \in L : |\alpha| \leq 1\}$ est un compact de L. Si on appelle $\mathcal{P}_L$ son idéal de valuation, on voit que $\kappa_L = \mathcal{O}_L/\mathcal{P}_L$ correspond à un recouvrement de $\mathcal{O}_L$ avec des ouverts disjoints ($\mathcal{P}_L$ est ouvert par la Remarque 1.9), donc il doit être forcément fini. On conclut que L est bien un corps local. □

Corollaire 2.15. *Si $K \subset L$ est une extension finie de corps locaux, alors pour tout $\sigma \in Gal(L/K)$ et tout $\alpha \in L$ on a $|\sigma(\alpha)| = |\alpha|$.*

Démonstration. Il suffit de noter que si $|\cdot|$ est un valeur absolue sur L étendant celle de K, alors l'application

$$\alpha \mapsto |\sigma(\alpha)|$$

définit une autre valeur absolue sur L qui coincide avec $|\cdot|$ sur K. Alors par l'unicité des valeurs absolues, on a l'égalité désirée. □

Notation Dorénavant, pour K un corps local, on notera $\mathcal{O}_K, \mathcal{P}_K$ son anneau et son idéal de valuation respectivement et κ_K son corps résiduel.

Notons maintenant que l'inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induit une inclusion

$$\mathcal{O}_K/(\mathcal{O}_K \cap \mathcal{P}_L) \hookrightarrow \mathcal{O}_L/\mathcal{P}_L = \kappa_L$$

Or, $\mathcal{O}_K \cap \mathcal{P}_L$ est un idéal premier de $\mathcal{O}_K$. En fait, si $\alpha_1, \alpha_2 \in \mathcal{O}_K \subset \mathcal{O}_L$ et $\alpha_1\alpha_2 \in \mathcal{P}_L$, comme $\mathcal{P}_L$ est un idéal premier de $\mathcal{O}_L$, on a bien que l'un des α_i est dans $\mathcal{P}_L$, donc dans $\mathcal{O}_K \cap \mathcal{P}_L$. Mais comme $\mathcal{O}_K$ n'a qu'un seule idéal premier propre $\mathcal{P}_K$ et $1 \notin \mathcal{O}_K \cap \mathcal{P}_K$, on trouve que $\kappa_K = \mathcal{O}_K/\mathcal{P}_K = \mathcal{O}_K/(\mathcal{O}_K \cap \mathcal{P}_L)$. Et alors on a l'inclusion, ou plus précisement, l'extension de corps

$$\kappa_K \hookrightarrow \kappa_L.$$

Et κ_L étant fini, on trouve que cette extension est finie.

On définit alors deux indices que nous aideront à comprendre les extensions finies de corps locaux.

Définition 2.16. Soit $K \subset L$ une extension finie de corps locaux.
Le degré $f = [\kappa_L : \kappa_K]$ de l'extension de corps induite $\kappa_K \subset \kappa_L$ est appelé le *degré résiduel* de l'extension.
L'indice $e = |L^*|/|K^*|$ (l'indice de $|K^*|$ comme sous-groupe de $|L^*|$) est appelé *l'indice de ramification* de l'extension.

Remarque 2.17. Avec les notations du Théorème 2.13, on voit que pour $\alpha \in K$, $w(\alpha) = e \cdot v(\alpha)$.

Théorème 2.18. *Avec les mêmes notations, si $K \subset L$ est une extension finie de corps locaux de degré n, alors $n = ef$.*

Démonstration. Soit $(\tilde{s}_n)_{1\le i\le f}$ une base de κ_L sur κ_K et $(s_n)_{1\le i\le f}$ une famille de représentants des éléments de cette base dans $\mathcal{O}_L$. On note qu'ils se trouvent forcément dans $\mathcal{O}_L^*$. Soit Π une unformisante de L. On montre d'abord que les éléments

$$\{s_i\Pi^j\}_{1\le i\le f,\,0\le j<e} \tag{*}$$

sont linéairement indépendants sur K. Pour cela, supposons

$$\sum_{i=1}^{f}\sum_{j=0}^{e-1}\lambda_{i,j}s_i\Pi^j = 0 \quad \lambda_{i,j}\in K$$

En posant $\gamma_j = \sum_i \lambda_{i,j}s_i$ on a

$$\sum_{j=0}^{e-1}\gamma_j\Pi^j = 0.$$

Choisissons pour chaque j un coefficient $\ell = \ell(j)$ tel que $|\lambda_{\ell,j}| = \max_i|\lambda_{i,j}|$. On affirme que $|\gamma_j| = |\lambda_{\ell,j}|$. Si $\lambda_{\ell,j} = 0$ c'est vrai. Sinon, on regarde $\gamma_j/\lambda_{\ell,j} \in \mathcal{O}_K$ et on voit que

$$\frac{\gamma_j}{\lambda_{\ell,j}} \equiv \sum_{i=1}^{f}\frac{\lambda_{i,j}}{\lambda_{\ell,j}}\tilde{s}_i \mod \mathcal{P}_L.$$

Comme les $\tilde{s}_i$ forment une base de κ_L et le coefficient de $\tilde{s}_\ell$ est 1, on voit que $\gamma_j/\lambda_{\ell,j} \not\equiv 0 \mod \mathcal{P}_L$, ce qui implique que $|\gamma_j/\lambda_{\ell,j}| = 1$. Alors, $|\gamma_j| \in r^{\mathbb{Z}} = |K^*|$.

D'autre part, par définition de e, on voit que $|L^*| = r^{(1/e)\mathbb{Z}}$. En particulier, $|\Pi| = r^{1/e}$. Donc

$$|\gamma_j\Pi^j| \equiv r^{j/e} \mod r^{\mathbb{Z}}.$$

Et alors $|\gamma_{j_1}\Pi^{j_1}| \neq |\gamma_{j_2}\Pi^{j_2}|$ si $j_1 \neq j_2$. Donc par l'inégalité triangulaire forte, on trouve que $0 = |\sum_j \gamma_j\Pi^j| = \max_j|\gamma_j\Pi^j|$, d'où on trouve que $\gamma_j = 0$ pour tout $0 \le j \le e-1$. Alors $|\lambda_{i,j}| \le |\lambda_{\ell,j}| = |\gamma_j| = 0$ pour tous i, j. Donc les éléments de (*) sont bien linéairement indépendants.

Maintenant il faut montrer que (*) engendre L. Pour cela, notons que $\kappa_L = \{\sum_{i=1}^f t_i\tilde{s}_i : t_i \in \kappa_K\}$ et alors, si R est un système de représentants des éléments de κ_K dans K comprenant 0, on a que $\{\sum_{i=1}^f t_i s_i : t_i \in R\}$ est un système de représentants de κ_L dans L. Alors le théorème de représentation nous dit que tout élément $\alpha \in \mathcal{O}_L$ peut s'écrire sous la forme

$$\alpha = \sum_{j\ge 0}\sum_{i=1}^{f} t_{i,j}s_i\Pi^j, \quad t_{i,j}\in R,$$

ce qui nous dit que, si π est un uniformisante de K, pour tout élément $\overline{\alpha} \in \mathcal{O}_L/\pi\mathcal{O}_L = \mathcal{O}_L/\Pi^e\mathcal{O}_L$ on a

$$\overline{\alpha} \equiv \sum_{j=0}^{e-1}\sum_{i=1}^{f} t_{i,j}s_i\Pi^j \mod \pi, \quad t_{i,j}\in R.$$

Alors, si $\alpha \in L$, quitte à multiplier α par une puissance de π convenable, on peut supposer que $\alpha \in \mathcal{O}_L$. Il existe donc $\alpha_1 \in \mathcal{O}_L$ tel que

$$\alpha = \sum_{j=0}^{e-1}\sum_{i=1}^{f} t_{0,i,j}s_i\Pi^j + \pi\alpha_1.$$

En itérant la procédure, par récurrence on voit que α s'écrit comme

$$\begin{aligned}\alpha &= \sum_{j=0}^{e-1}\sum_{i=1}^{f} t_{0,i,j}s_i\Pi^j + \pi\sum_{j=0}^{e-1}\sum_{i=1}^{f} t_{1,i,j}s_i\Pi^j + \pi^2\sum_{j=0}^{e-1}\sum_{i=1}^{f} t_{2,i,j}s_i\Pi^j + \cdots \\ &= \sum_{m\geq 0}\pi^m\sum_{j=0}^{e-1}\sum_{i=1}^{f} t_{m,i,j}s_i\Pi^j = \sum_{j=0}^{e-1}\sum_{i=1}^{f}\left(\sum_{m\geq 0}\pi^m t_{m,i,j}\right)s_i\Pi^j,\end{aligned}$$

car les séries sont toutes convergentes. Et comme $\sum_m \pi^m t_{m,i,j} \in \mathcal{O}_K$, on a bien que L est engendré par les $\{s_i\Pi^j\}$, ce qui conclut. □

Définition 2.19. On dit qu'une extension finie de corps locaux $K \subset L$ est
- *non-ramifiée* si $e = 1$, ou de façon équivalente, si $[L : K] = f$
- *totalement ramifiée* si $f = 1$, ou de façon équivalente, si $[L : K] = e$
- *modérément ramifiée* si elle est totalement ramifiée et $\text{pgcd}(e, p) = 1$
- *sauvagement ramifiée* si elle est totalement ramifiée et $e = p^k$ pour certain $k \geq 1$.

En se souvenant du théorème de la base téléscopique, on voudrait que cette multiplicativité reste vraie pour notre décomposition des degrés des extensions. Ceci est en fait vrai et facile à voir.

Proposition 2.20. *Si $K \subset L \subset M$ sont des extensions finies des corps locaux de degrés $[L : K] = n_{L/K} = e_{L/K}f_{L/K}$ et $[M : L] = n_{M/L} = e_{M/L}f_{M/L}$. Alors $[M : K] = n_{M/K} = e_{M/K}f_{M/K}$ avec*

$$e_{M/K} = e_{L/K}e_{M/L}, \quad f_{M/K} = f_{L/K}f_{M/L}.$$

Démonstration. Il suffit d'appliquer le théorème de la base téléscopique aux corps $\kappa_K, \kappa_L, \kappa_M$ pour trouver $f_{M/K} = f_{L/K}f_{M/L}$. En divisant la relation $n_{M/K} = n_{L/K}n_{M/L}$ par cette dernière égalité, on obitient $e_{M/K} = e_{L/K}e_{M/L}$. □

3 Le chemin vers la preuve

Ayant fait déjà une analyse générale des corps locaux (et ayant démontré que $\mathbb{Q}_p$ est bien un corps local), on donne dans cette section quelques résultats qui nous seront utiles pour montrer le théorème final. Dans toute cette section on note, comme précédemment, ζ_n une racine primitive n-ième de l'unité, p la caractéristique des corps résiduels dont on parle et $\overline{\mathbb{Q}_p}$ une clôture algébrique de $\mathbb{Q}_p$.

3.1 Extensions non-ramifiées et totalement ramifiées

On commence par un résultat qui nous donne tout de ce que nous aurons besoin sur les extensions non-ramifiées.

Théorème 3.1. *Soit $K \subset L$ une extension finie non-ramifiée de corps locaux. Alors*

i) $L = K(\zeta_n)$ pour certain n avec $pgcd(p, n) = 1$;

ii) $K \subset L$ est cyclique, i.e. galoisienne avec $Gal(L/K)$ cyclique.

En plus, pour K fixé et pour tout $f \geq 1$ il existe une unique extension non-ramifiée L de K de degré f (et elle sera clairement cyclique).

Démonstration. On sait que κ_L est le corps de décomposition de $P(x) = x^n - 1$ sur κ_K pour certain n avec $\text{pgcd}(p, n) = 1$. En particulier, P est séparable. Le Lemme de Hensel nous dit alors que toutes les racines de P (vu comme un polynôme dans $K[x]$) sont dans L. En fait, si on note $\overline{\alpha}$ la classe de α modulo $\mathscr{P}_L$, alors pour chaque racine α_0 dans κ_L, on trouve un racine α dans $\mathscr{O}_L$ tel que $\overline{\alpha} = \alpha_0$. On voit alors que P est séparable sur K et scindé dans L. Donc, comme ζ_n est une racine de P, on voit que $\zeta_n \in L$ et $K(\zeta_n) \subset L$.

On voit aussi que $\overline{\zeta_n^k} \neq \overline{\zeta_n^\ell}$ si $k \not\equiv \ell \mod n$. Donc on a que $\overline{\zeta_n}$ est une racine primitive n-ième de l'unité dans κ_L, ce qui nous dit $\kappa_L = \kappa_K(\overline{\zeta_n})$.

Soit Q le polynôme minimal de ζ_n dans $K[x]$. D'après le lemme de Gauss, $Q \in \mathscr{O}[x]$. Supposons que sa restriction modulo $\mathscr{P}_K$, $\overline{Q}$, soit réductible. Alors, comme P est séparable sur κ_K et $\overline{Q} \mid P$, le Lemme de Hensel nous donnerait une factorisation non-triviale de Q sur K, ce qui contredit son irréductibilité. Par conséquent, $\overline{Q}$ est irréductible dans $\kappa_K[x]$ et, comme $\overline{\zeta_n}$ est une racine de $\overline{Q}$,

$$[K(\zeta_n) : K] = \deg Q = \deg \overline{Q} = [\kappa_K(\overline{\zeta_n}) : \kappa_K] = [\kappa_L : \kappa_K] = f = [L : K].$$

D'où l'égalité $L = K(\zeta_n)$.

Pour la partie ii) on affirme que

$$\text{Gal}(L/K) \simeq \text{Gal}(\kappa_L/\kappa_K)$$

d'où on obtient immédiatement le résultat, car toute extension finie de corps finis est cyclique. Pour montrer cela, on définit le morphisme de groupes $\rho : \text{Gal}(L/K) \to \text{Gal}(\kappa_L/\kappa_K)$ par

$$\rho(\sigma)(\overline{\alpha}) = \overline{\sigma(\alpha)}, \quad \alpha \in \mathscr{O}_L.$$

Ceci est bien définie, car si $\overline{\alpha} = \overline{\beta}$ alors $\alpha - \beta \in \mathscr{P}_L$. Et comme σ préserve la valeur absolue (par le Corollaire 2.15), on a $\sigma(\alpha - \beta) \in \mathscr{P}_L$ et alors $\overline{\sigma(\alpha)} - \overline{\sigma(\beta)} = \overline{\sigma(\alpha - \beta)} = 0$. On vérifie sans problèmes aussi que ρ est un morphisme. Donc il suffit de montrer qu'il est injectif, car $[L : K] = f = [\kappa_L : \kappa_K]$ implique $|\text{Gal}(L/K)| = |\text{Gal}(\kappa_L/\kappa_K)|$, d'où on obtient la surjectivité.

Supposons donc $\rho(\sigma)(\overline{\zeta_n}) = \overline{\zeta_n}$. Alors $\sigma(\zeta_n) = \zeta_n$ car on a vu déjà que les racines de P dans L sont différents modulo $\mathscr{P}_L$ (donc σ ne peut pas envoyer ζ_n sur une autre racine de P). On a alors que ρ est injectif.

Finalement, pour la dernière affirmation il suffit de trouver ζ_ℓ avec $(p, \ell) = 1$ tel que $f = [\kappa_K(\overline{\zeta_\ell}) : \kappa_K]$. Par exemple, si $|\kappa_K| = q$, on peut prendre $\ell = q^f - 1$. Alors l'extension $K \subset K(\zeta_\ell)$ est non-ramifiée. Pour verifier cela, on raisonne comme d'avant pour trouver que $[K(\zeta_\ell) : K] = [\kappa_K(\overline{\zeta_\ell}) : \kappa_K] = f$. Sachant que l'extension est non-ramifiée, on voit immédiatement qu'elle est cyclique et de degré f. S'il y avait deux telles extensions, leur composée serait aussi non-ramifiée (il suffit de noter que $K(\zeta_i)K(\zeta_j) = K(\zeta_k)$ avec $k = \text{ppcm}(i, j)$), donc cyclique. Alors elles seront forcément égales, car un groupe cyclique ne peut pas avoir deux quotients différents de même indice. □

Maintenant qu'on a vu que la réduction ζ_n modulo $\mathscr{P}$ est encore une racine de l'unité, on ne fera plus la différence entre ζ_n et $\overline{\zeta_n}$. On notera toujours ζ_n.

Corollaire 3.2. *Soit $K \subset L$ une extension finie de corps locaux. Alors il existe une unique sous-extension non-ramifiée maximale $K \subset K^{nr}$ incluse dans L. En particulier, l'extension $K^{nr} \subset L$ est totalement ramifiée.*

Démonstration. Soit $n = ef$ le degré de l'extension $K \subset L$. Si on pose $\kappa_K = \mathbb{F}_q$, on sait que $\kappa_L = \kappa_K(\zeta_{q^f-1})$. Et si K' est une sous-extension non-ramifiée, on voit que $K' = K(\zeta_m)$ avec $(p,m) = 1$ et donc $\kappa_{K'} = \kappa_K(\zeta_m)$. Comme $\kappa_{K'} \subset \kappa_L$, on en déduit que $m|q^f - 1$. Alors $K^{\mathrm{nr}} = K(\zeta_{q^f-1})$ est une sous-extension non-ramifiée maximale de degré f. L'unicité découle du dernier résultat. Finalement, la proposition 2.20 nous dit que, comme $f_{K^{\mathrm{nr}}/K} = f_{L/K}$, on a que $f_{L/K^{\mathrm{nr}}} = 1$, donc $K^{\mathrm{nr}} \subset L$ est totalement ramifiéee. □

On continue maintenant avec les extensions totalement ramifiées.

Théorème 3.3. *Soit $K \subset L$ une extension finie moderément ramifiée. Alors il existe π une uniformisante de K tel que $L = K(\pi^{1/e})$.*

Démonstration. Choisissons Π une uniformisante de L et π_0 un autre dans K. Alors $|\Pi^e| = |\pi_0|$, ou bien

$$\Pi^e = u\pi_0 \qquad u \in \mathscr{O}_L^*.$$

Or, comme l'extension est totalement ramifiée, on a $\kappa_L = \kappa_K$. Donc il existe $u_0 \in \mathscr{O}_K^*$ tel que $u \equiv u_0 \mod \mathscr{P}_L$. C'est-à-dire,

$$u = u_0 + \alpha \qquad \alpha \in \mathscr{P}_L.$$

On pose $\pi = \pi_0 u_0$, alors

$$\Pi^e = \pi_0 u_0 + \pi_0 \alpha = \pi + \pi_0 \alpha,$$

et $\alpha \in \mathscr{P}_L$ implique en particulier que $|\alpha| < 1$, donc

$$|\Pi^e - \pi| = |\pi_0 \alpha| < |\pi_0| = |\pi|.$$

Regardons le polynôme $P(x) = x^e - \pi$. Il est irréductible dans K par le critère d'Eisenstein appliqué sur $\mathscr{O}_K$ et il est séparable car on est en caractéristique 0. Soient $\alpha_1, \ldots, \alpha_e$ les racines de P dans M, son corps de décomposition sur K. Comme les α_i sont conjuguées, on voit, grâce au Corollaire 2.15, que $|\alpha_i| = |\alpha_j|$. Alors par l'inégalité triangulaire forte on a que, pour i fixé, $|\alpha_i - \alpha_j| \leq \max\{|\alpha_i|, |\alpha_j|\} = |\alpha_i|$. Mais on a aussi

$$\prod_{j \neq i} |\alpha_i - \alpha_j| = |P'(\alpha_i)| = |e\alpha_i^{e-1}| = |\alpha_i|^{e-1}$$

et on trouve alors qu'on a en fait l'égalité $|\alpha_i - \alpha_j| = |\alpha_i|$ pour $j \neq i$.

D'autre part, comme

$$\prod_{1 \leq i \leq e} |\Pi - \alpha_i| = |P(\Pi)| = |\Pi^e - \pi| < |\pi| = \prod_{1 \leq i \leq e} |\alpha_i|,$$

on voit que pour certain i on a forcément $|\Pi - \alpha_i| < |\alpha_i|$. Et alors $|\Pi - \alpha_i| < |\alpha_i - \alpha_j|$ pour $j \neq i$. L'inégalité triangulaire forte nous dit alors que pour $j \neq i$,

$$|\Pi - \alpha_j| = |\alpha_i - \alpha_j| > |\Pi - \alpha_i|.$$

Supposons que $\alpha_i \notin L$. Comme ML est le corps de décomposition de P sur L, on sait que ML/L est galoisienne. Prenons donc $\sigma \in \mathrm{Gal}(ML/L)$ tel que $\sigma(\alpha_i) \neq \alpha_i$. Alors $\sigma(\alpha_i) = \alpha_k$ pour certain $k \neq i$. On voit par le Corollaire 2.15 que

$$|\Pi - \alpha_i| = |\sigma(\Pi - \alpha_i)| = |\Pi - \alpha_k|$$

ce qui donne une contradiction. Donc $\alpha_i \in L$ et $K(\alpha_i) \subset L$. Et en notant que $[K(\alpha_i) : K] = deg(P) = e = [L : K]$, on voit que $L = K(\alpha_i) = K(\pi^{1/e})$. □

3.2 Extensions de $\mathbb{Q}_p$

Maintenant on laisse un peu de côté les généralités pour regarder les extensions de $\mathbb{Q}_p$. D'abord, en regardant le Théorème 3.1, on voit que pour $(p,n)=1$, l'extension $\mathbb{Q}_p(\zeta_n)$ est non-ramifiée. Pour avoir une analyse complète des extensions cyclotomiques de $\mathbb{Q}_p$, il faut se demander maintenant ce qui se passe avec ζ_{p^m}. On trouve le résultat suivante.

Proposition 3.4. *L'extension $\mathbb{Q}_p(\zeta_{p^m})$ est totalement ramifiée de degré $p^{m-1}(p-1)$.*

Démonstration. On sait que

$$\Phi_{p^m}(x)=\frac{x^{p^m}-1}{x^{p^{m-1}}-1}=x^{p^{m-1}(p-1)}+x^{p^{m-1}(p-2)}+\dots x^{p^{m-1}}+1=\prod_{\substack{1\le k\le p^m-1\\(p,k)=1}}(x-\zeta_{p^m}^k). \tag{3}$$

D'autre part, soit $k\in\mathbb{Z}$ tel que $\mathrm{pgcd}(k,p)=1$. On sait qu'il existe $\ell\in\mathbb{Z}$ tel que $k\ell\equiv 1 \mod p^m$. Alors, par l'inégalité triangulaire forte et le fait que $|\zeta_{p^m}|^{p^m}=|1|=1\Rightarrow|\zeta_{p^m}|=1$ on a

$$\left|\frac{1-\zeta_{p^m}^k}{1-\zeta_{p^m}}\right|=|1+\zeta_{p^m}+\dots+\zeta_{p^m}^{k-1}|\le 1$$

$$\left|\frac{1-\zeta_{p^m}}{1-\zeta_{p^m}^k}\right|=\left|\frac{1-\zeta_{p^m}^{k\ell}}{1-\zeta_{p^m}^k}\right|=|1+\zeta_{p^m}^k+\dots+\zeta_{p^m}^{k(\ell-1)}|\le 1.$$

On voit alors que pour tout k premier à p on a $|1-\zeta_{p^m}|=|1-\zeta_{p^m}^k|$. Et donc, de l'équation (3) on obtient

$$|\Phi_{p^m}(1)|=|p|=\prod_{\substack{1\le k\le p^m-1\\(p,k)=1}}|1-\zeta_{p^m}^k|=|1-\zeta_{p^m}|^{\varphi(p^m)}.$$

Alors $p^{(1/\varphi(p^m))\mathbb{Z}}\subset|\mathbb{Q}_p(\zeta_{p^m})|$, ce qui entraîne $e\ge\varphi(p^m)=p^{m-1}(p-1)$. Mais d'autre part on a que $e\le n=[\mathbb{Q}_p(\zeta_{p^m}):\mathbb{Q}_p]\le\deg\Phi_{p^m}=p^{m-1}(p-1)$. Alors on a $n=e=p^{m-1}(p-1)$ et l'extension est totalement ramifiée. □

Notons qu'il existe un morphisme injectif canonique

$$\rho:\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)\to(\mathbb{Z}/p^m\mathbb{Z})^*,\sigma\mapsto n(\sigma),$$

où $\sigma(\zeta_{p^m})=\zeta_{p^m}^{n(\sigma)}$. Et comme les deux groupes ont le même cardinal, ρ est un isomorphisme. On obtient comme conséquence immédiate que $\mathbb{Q}_p\subset\mathbb{Q}_p(\zeta_{p^m})$ est galoisienne (ce qu'on aurait pu montrer en notant que Φ_{p^m} est irréductible dans $\mathbb{Q}_p$ et $\mathbb{Q}_p(\zeta_{p^m})$ est son corps de décomposition). On trouve alors que pour $p\neq 2$

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)\simeq(\mathbb{Z}/p^m\mathbb{Z})^*\simeq\mathbb{Z}/(p-1)\mathbb{Z}\times\mathbb{Z}/p^{m-1}\mathbb{Z}.$$

Et pour $p=2$ (et $m\ge 2$)

$$\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^m})/\mathbb{Q}_2)\simeq(\mathbb{Z}/2^m\mathbb{Z})^*\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{m-2}\mathbb{Z}.$$

Ceci nous permet de voir que dans tous les cas, $\mathbb{Q}_p\subset\mathbb{Q}_p(\zeta_{p^m})$ est abélienne (et en particulier cyclique pour $p\neq 2$).

Ayant les extensions de $\mathbb{Q}_p$ du type $\mathbb{Q}_p(\zeta_n)$ pour $(p,n)=1$ et $n=p^m$, il suffit de les mélanger pour obtenir toutes les extensions. Pour cela on montre le théorème suivant.

Théorème 3.5. *Soient K,L des extensions finies galoisiennes de $\mathbb{Q}_p$. Alors $KL/\mathbb{Q}_p$ est aussi galoisienne et on a l'isomorphisme de groupes*

$$Gal(KL/\mathbb{Q}_p) \simeq \{(\sigma,\tau) \in Gal(K/\mathbb{Q}_p) \times Gal(L/\mathbb{Q}_p) : \sigma|_{K\cap L} = \tau|_{K\cap L}\}.$$

Démonstration. D'abord, comme K et L sont des extensions galoisiennes, on sait qu'elles sont des corps de décomposition de certains polynômes sur $\mathbb{Q}_p$. Alors, leur composée est clairement le corps de décomposition du produit de ces polynômes sur $\mathbb{Q}_p$. D'où on tire que cette extension est normale, donc galoisienne car $\mathbb{Q}_p$ est de caractéristique 0.

Maintenant, soit $G = \mathrm{Gal}(KL/\mathbb{Q}_p)$ et $H = \{(\sigma,\tau) : \sigma|_{K\cap L} = \tau|_{K\cap L}\}$. On définit le morphisme de groupes

$$\rho : G \to H, \quad \sigma \mapsto (\sigma|_K, \sigma|_L).$$

Il est bien défini, car K et L étant des extensions galoisiennes, on a que pour tout $\sigma \in G$, $\sigma(K) = K$ et $\sigma(L) = L$. Il est en plus clairement injectif, car $\sigma \in G$ est défini par son action sur K et sur L. Il suffit alors de montrer que $|G| = |H|$.

Soit alors $F = K \cap L$ et soient $m = [F : \mathbb{Q}_p]$, $k = [KL : K]$ et $l = [KL : L]$. On voit que $A = \mathrm{Gal}(KL/K)$ et $B = \mathrm{Gal}(KL/L)$ sont des sous-groupes distingués de G car $\mathbb{Q}_p \subset K$ et $\mathbb{Q}_p \subset L$ sont des extensions galoisiennes. En plus, il est clair que $A \cap B = \{1\}$ puisque fixer K et L révient à fixer KL et aussi que le corps fixé par le sous-groupe AB est F. Alors on a que

$$[KL : F] = |AB| = \frac{|A||B|}{|A \cap B|} = kl.$$

Donc $[K : F] = l$ et $[L : F] = k$, et on a $|G| = [KL : K][K : F][F : \mathbb{Q}_p] = klm$.

D'autre part, chaque $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ induit un morphisme $\sigma|_F \in \mathrm{Hom}(F, \overline{\mathbb{Q}_p})$. Et on sait que

$$|\{\tau \in \mathrm{Hom}(L, \overline{\mathbb{Q}_p}) : \tau|_F = \sigma|_F\}| = [L : F]_s = [L : F] = k,$$

car toutes nos extensions sont séparables. Or, comme $\mathbb{Q}_p \subset L$ est galoisienne, on a que $\mathrm{Hom}(L, \overline{\mathbb{Q}_p}) = \mathrm{Gal}(L/\mathbb{Q}_p)$. Alors, pour chaque $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ il y a k éléments dans $\mathrm{Gal}(L/\mathbb{Q}_p)$ avec la même restriction à F. Donc on trouve que $|H| = k|\mathrm{Gal}(K/\mathbb{Q}_p)| = k[K : \mathbb{Q}_p] = klm$. □

Corollaire 3.6. *Si $\mathbb{Q}_p \subset K$ et $\mathbb{Q}_p \subset L$ sont des extensions finies abéliennes, alors $\mathbb{Q}_p \subset KL$ l'est aussi. En particulier, toute extension cyclotomique de $\mathbb{Q}_p$ est abélienne.*

On donne finalement un petit lemme qui nous sera utile dans la preuve finale.

Lemme 3.7. $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$

Démonstration. Notons $K = \mathbb{Q}_p(\zeta_p)$. Par la Proposition 3.4, on voit que $[K : \mathbb{Q}_p] = p-1$. D'autre part, le polynôme $x^{p-1} + p$ est irréductible dans $\mathbb{Q}_p$ par le critère de Eisenstein appliqué sur $\mathbb{Z}_p$. Alors $[\mathbb{Q}_p((-p)^{1/(p-1)}) : \mathbb{Q}_p] = p-1$. Donc il suffit de montrer que $(-p)^{1/(p-1)}$ appartient à K. Soit

$$f(x) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \cdots + p$$

On voit que

$$f(\zeta_p - 1) = 0 \equiv (\zeta_p - 1)^{p-1} + p \mod p(\zeta_p - 1)$$

En divisant par p on obtient

$$u := \frac{(\zeta_p - 1)^{p-1}}{-p} \equiv 1 \mod (\zeta_p - 1)$$

Ou de façon équivalente, $u \equiv 1 \mod \mathscr{P}_K$ (par la Proposition 3.4, on voit que $(\zeta_p - 1)$ est une uniformisante de K). Donc, si on pose $g(x) = x^{p-1} - u$, on voit que la réduction de g modulo

$\mathscr{P}_K$ est séparable et admet 1 comme racine. Alors le Lemme de Hensel nous dit qu'il existe une racine de g dans K, i.e. il existe $\alpha \in K$ tel que $\alpha^{p-1} = u$. Et alors

$$(-p)^{1/(p-1)} = \frac{\zeta_p - 1}{\alpha} \in K$$

ce qui conclut. □

3.3 Théorie de Kummer

Dans cette partie, nous donnons quelques résultats de la théorie de Kummer qui nous seront utiles dans la partie technique de la preuve. Pour éviter des problèmes, tous les corps dont on parle dans cette partie sont supposés de caractéristique 0. On note μ_n l'ensemble des racines n-ièmes de l'unité.

Définition 3.8. Soit $K \subset L$ une extension galoisienne de groupe G. On dit que l'extension est *d'exposant n* si $\sigma^n = 1$ pour tout $\sigma \in G$. On dit que l'extension est *abélienne* si G est abélien.

Définition 3.9. Soit K un corps contenant μ_n et B un sous-groupe de K^* contenant $K^{*n} = \{\alpha^n : \alpha \in K^*\}$. On appelle *extension de Kummer d'exposant n* et on note $K(B^{1/n}) = K_B$ la composée de toutes les extensions $K(a^{1/n})$ avec $a \in B$.

Notons que comme $\mu_n \subset K$, $K(a^{1/n})$ est indépendant du choix de la racine de a. Cette extension est galoisienne, car pour tout $a \in B$ le polynôme $x^n - a$ est scindé sur K_B.

Soit maintenant $a \in B$, α une racine n-ième de a et $\sigma \in G = \mathrm{Gal}(K_B/K)$. Alors $\sigma(\alpha) = \omega_{a,\sigma}\alpha$ pour une certaine racine n-ième de l'unité $\omega_{a,\sigma}$. On a alors un morphisme de groupes

$$G \to \mu_n, \quad \sigma \mapsto \omega_{a,\sigma}$$

où on note que

$$\tau(\sigma(\alpha)) = \omega_{a,\tau}\omega_{a,\sigma}\alpha = \omega_{a,\sigma}\omega_{a,\tau}\alpha = \sigma(\tau(\alpha)).$$

Notons maintenant que $\omega_{a,\sigma}$ ne dépend pas du choix de la racine n-ième de a. En fait, si α' est une autre racine, on sait que $\alpha' = \zeta\alpha$ pour certain $\zeta \in \mu_n$, et alors

$$\omega_{a,\sigma} = \frac{\sigma(\alpha)}{\alpha} = \frac{\zeta\sigma(\alpha)}{\zeta\alpha} = \frac{\sigma(\alpha')}{\alpha'}.$$

On définit alors l'accouplement

$$\langle\cdot,\cdot\rangle : G \times B \to \mu_n, \quad (\sigma, a) \mapsto \langle\sigma, a\rangle = \omega_{a,\sigma}.$$

Si $a, b \in B$ et $\alpha, \beta \in K_B$ tels que $\alpha^n = a$ et $\beta^n = b$, on a clairement $(\alpha\beta)^n = ab$ et

$$\frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma(\alpha)}{\alpha}\frac{\sigma(\beta)}{\beta},$$

donc $\langle\cdot,\cdot\rangle$ est bilinéaire. En plus, on voit que si $a \in K^{*m}$, alors $\langle\sigma, a\rangle = 1$.

Théorème 3.10. *Soit $K \subset K_B$ une extension de Kummer d'exposant n. Alors cette extension est abélienne d'exposant n. Si G est son groupe de Galois, $\langle\cdot,\cdot\rangle : G \times B \to \mu_n$ a $\{1\}$ comme noyau à gauche et K^{*n} comme noyau à droite. L'extension est finie si et seulement si $|B/K^{*n}|$ est fini et dans ce cas*

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

et en particulier, $[K_B : K] = |B/K^{*n}|$.

Démonstration. Supposons $\langle \sigma, a\rangle = 1$ pour tout $a \in B$. Alors, pour tout $\alpha \in B^{1/n}$ on a $\sigma(\alpha) = \alpha$, et comme ces éléments engendrent K_B, on trouve que σ est l'identité. Supposons maintenant que $\langle \sigma, a\rangle = 1$ pour tout $\sigma \in G$. Alors G fixe le sous-corps $K(a^{1/n})$. Donc $K(a^{1/n}) \subset K$ et $a \in K^{*n}$.

Pour montrer que $K \subset K_B$ est abélienne et d'exposant n, il suffit de noter que pour tout $\sigma, \tau \in G$, on a $\tau(\sigma(\alpha)) = \sigma(\tau(\alpha))$ et $\sigma^n(\alpha) = \langle \sigma, \alpha^n\rangle^n \alpha = \alpha$ pour tout $\alpha \in B^{1/n}$, donc pour tout $\alpha \in K_B$.

Pour montrer ce qu'il nous manque, nous avons besoin d'un petit lemme.

Lemme 3.11. *Soit G un groupe abélien fini. Alors $G \simeq Hom(G, \mathbb{C}^*)$.*

Démonstration. D'abord, c'est clair que si $G = H_1 \times H_2$, alors

$$\mathrm{Hom}(G, \mathbb{C}^*) = \mathrm{Hom}(H_1, \mathbb{C}^*) \times \mathrm{Hom}(H_2, \mathbb{C}^*).$$

Or, on sait que tout groupe abélien est le produit de ses sous-groupes cycliques maximaux. Alors il suffit de montrer le résultat pour G cyclique. Et dans ce cas, si α engendre G et $|\alpha| = n$, alors pour tout $\sigma \in \mathrm{Hom}(G, \mathbb{C}^*)$ on a $\sigma(\alpha)^n = 1$, donc $\sigma(\alpha) \in \mu_n$. On définit alors $\rho : G \to \mathrm{Hom}(G, \mathbb{C}^*)$ comme $\rho(\alpha^m) = \sigma_m$ où $\sigma_m(\alpha) = \zeta_n^m$. Ce morphisme est clairement injective et il est surjective par ce qu'on vient de noter, donc c'est un isomorphisme. □

Sachant que les noyaux de $\langle \cdot, \cdot \rangle$ sont $\{1\}$ et K^{*n}, on trouve des injections

$$B/K^{*n} \hookrightarrow \mathrm{Hom}(G, \mu_n), \qquad G \hookrightarrow \mathrm{Hom}(B/K^{*n}, \mu_n). \tag{4}$$

Notons que comme G est d'exposant n, alors $\mathrm{Hom}(G, \mathbb{C}^*) = \mathrm{Hom}(G, \mu_n)$ et de même pour B/K^{*n}. Alors en utilisant le lemme et (4), on voit que

$$B/K^{*n} \hookrightarrow \mathrm{Hom}(G, \mu_n) \simeq G \hookrightarrow \mathrm{Hom}(B/K^{*n}, \mu_n) \simeq B/K^{*n}.$$

Donc les applications (4) sont des isomorphismes, ce qui nous donne $B/K^{*n} \simeq \mathrm{Hom}(G, \mu_n)$ et $[K_B : K] = |G| = |B/K^{*n}|$, ce qui conclut. □

Théorème 3.12. *Les extensions abéliennes d'exposant n d'un corps K contenant μ_n sont en correspondance bijective avec les sous-groupes B de K^* contenant K^{*n}.*

Démonstration. Montrons d'abord que l'application $B \mapsto K_B$ est injective. Supposons que $K_{B_1} \subset K_{B_2}$. On veut montrer alors que $B_1 \subset B_2$. Soit $a \in B_1$. On a clairement $K(a^{1/n}) \subset K_{B_2}$ et en particulier $K(a^{1/n})$ est contenu dans une sous-extension finiment engendrée de K_{B_2}. On peut donc supposer que B_2/K^{*n} est fini. On pose B_3 le sous-groupe de K^* engendré par B_2 et a. C'est clair que $K_{B_2} = K_{B_3}$ et par le Théorème 3.10 on voit que

$$|B_2/K^{*n}| = [K_{B_2} : K] = [K_{B_3} : K] = |B_3/K^{*n}|.$$

Donc forcément $B_2 = B_3$, et $a \in B_2$, ce qui implique $B_1 \subset B_2$.

Soit maintenant L une extension abélienne de K d'exposant n. Elle est la composée de ses sous-extensions finies (et elles sont toutes d'exposant n). Et toute sous-extension abélienne finie d'exposant n est la composée de ses sous-extensions cycliques aussi d'exposant n. Supposons que chacune de ces extensions est engendrée par une racine n-ième d'un élément de K. Alors L est engendré par une famille de racines n-ièmes, disons les racines n-ièmes des $\{a_i\}_{i\in I}$ avec $a_i \in K^*$. En posant B comme le groupe engendré par $\{a_i\}_{i\in I}$ et par K^{*n}, on voit que $L = K(B^{1/n})$.

Le lemme suivante nous permet alors de conclure.

Lemme 3.13. *Soit K un corps contenant les racines n-ièmes de l'unité et $K \subset L$ une extension cyclique de degré n. Alors il existe $a \in K$ tel que $L = K(a^{1/n})$.*

Démonstration. Soit σ un générateur de $G = \mathrm{Gal}(L/K)$ et ζ un racine primitive n-ième de l'unité dans K. On considère le morphisme

$$\mathrm{id} + \zeta\sigma + \zeta\sigma(\zeta)\sigma^2 + \cdots + \left[\prod_{i=0}^{n-2} \sigma^i(\zeta)\right] \sigma^{n-1}.$$

Par le Théorème d'indépendance des caractères, on sait que ce morphisme n'est pas identiquement 0. Donc il existe $\beta \in L$ tel que l'élément

$$\alpha = \beta + \zeta\sigma(\beta) + \zeta\sigma(\zeta)\sigma^2(\beta) + \cdots + \left[\prod_{i=0}^{n-2} \sigma^i(\zeta)\right] \sigma^{n-1}(\beta)$$

soit non nul. Alors, comme $N_{L/K}(\zeta) = 1$ et $G = \{\sigma^i : 1 \leq i \leq n\}$, on voit que $\zeta\sigma(\alpha) = \alpha$, et donc $\sigma(\alpha) = \zeta^{-1}\alpha$. Alors pour tout $1 \leq i \leq n$ on a $\sigma^i(\alpha) = \zeta^{-i}\alpha$. Donc les $\zeta^i\alpha$ sont des conjugués différents de α sur K, ce qui entraîne $[K(\alpha) : K] \geq n$. Mais $[L : K] = n$, donc on a forcément $L = K(\alpha)$. Et en notant que

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta^{-1}\alpha)^n = \alpha^n,$$

on voit que $a = \alpha^n \in K$, et donc $L = K(a^{1/n})$. □

□

4 Le théorème de Kronecker-Weber local

On peut désormais prouver le résultat souhaité.

Théorème 4.1 (Théorème de Kronecker-Weber local)**.** *Soit $\mathbb{Q}_p \subset K$ une extension finie et abélienne. Alors il existe $n \in \mathbb{N}$ tel que $K \subset \mathbb{Q}_p(\zeta_n)$.*

Démonstration. On sait que tout groupe abélien est un produit des groupes cycliques d'ordre une puissance d'un nombre premier. Alors, le Théorème 3.5 nous dit une extension abélienne $\mathbb{Q}_p \subset K$ est la composée de ses sous-extensions cycliques. En plus, la composée d'extensions cyclotomiques est encore cyclotomique. Cela nous permet de nous ramèner au cas où $\mathrm{Gal}(K/\mathbb{Q}_p) = \mathbb{Z}/q^m\mathbb{Z}$ avec q premier et $m \geq 1$.

On verra trois cas : $p \neq q$, $p = q \neq 2$ et $p = q = 2$.

Cas 1 : $p \neq q$. Soit L la sous-extension non-ramifiée maximale de K. Le Théorème 3.1 et son corollaire nous disent alors que $L = \mathbb{Q}_p(\zeta_n)$ pour certain $n \geq 1$ et $L \subset K$ est totalement ramifiée de degré e. Comme $e|q^m$ et $q \neq p$, on voit que $L \subset K$ est modérément ramifiée. Alors le Théorème 3.3 s'applique et on obtient $K = L(\pi^{1/e})$ pour π une certain uniformisante de L.

Or, comme $\mathbb{Q}_p \subset L$ est non-ramifié, on voit que $|\pi| = |p|$, ou bien

$$\pi = -up$$

pour certain $u \in \mathcal{O}_L^*$. Or, $u \not\equiv 0 \mod \mathcal{P}_L$ implique que la restriction de $x^e - u$ dans $\kappa_L[x]$ est séparable. Donc, si P est le polynôme minimal de $u^{1/e}$ sur L, sa restriction dans $\kappa_L[x]$ est aussi séparable et irréductible par le Lemme de Hensel. Alors

$$[\kappa_{L(u^{1/e})} : \kappa_L] = [\kappa_L(\overline{u}^{1/e}) : \kappa_L] = [L(u^{1/e}) : L]$$

ce qui nous dit que $L \subset L(u^{1/e})$ est non-ramifié. Donc, encore par le Théorème 3.1,

$$L(u^{1/e}) = L(\zeta_\ell) \subset \mathbb{Q}_p(\zeta_{n\ell})$$

pour certain $\ell \geq 1$. En particulier $\mathbb{Q}_p(u^{1/e}) \subset \mathbb{Q}_p(\zeta_{n\ell})$, donc l'extension $\mathbb{Q}_p \subset \mathbb{Q}_p(u^{1/e})$ est abélienne. D'autre part, comme $\mathbb{Q}_p \subset K$ est abélienne, on voit que $\mathbb{Q}_p \subset \mathbb{Q}_p(\pi^{1/e})$ l'est aussi. En utilisant le Théorème 3.5, on en déduit que $\mathbb{Q}_p \subset \mathbb{Q}_p((-p)^{1/e})$ est aussi une extension abélienne, donc galoisienne. Alors le polynôme $Q(x) = x^e + p$ est scindé dans $\mathbb{Q}_p((-p)^{1/e})$, d'où on obtient que $\zeta_e(-p)^{1/e} \in \mathbb{Q}_p((-p)^{1/e})$ et donc $\zeta_e \in \mathbb{Q}_p((-p)^{1/e})$.

En plus, en notant que $p^{(1/e)\mathbb{Z}} \subset |\mathbb{Q}_p((-p)^{1/e})|$ et $[\mathbb{Q}_p((-p)^{1/e}) : \mathbb{Q}_p] \leq \deg Q = e$, on voit que $\mathbb{Q}_p \subset \mathbb{Q}_p((-p)^{1/e})$ est totalement ramifié. Cela nous dit que $\mathbb{Q}_p \subset \mathbb{Q}_p(\zeta_e)$ est totalement ramifié. Mais $p \nmid e$, donc l'extension est aussi non-ramifié, donc triviale. Alors $\zeta_e \in \mathbb{Q}_p$ et la Proposition 2.8 nous dit donc que $e|p-1$. Alors, par le Lemme 3.7, on voit que

$$\mathbb{Q}_p((-p)^{1/e}) \subset \mathbb{Q}_p((-p)^{1/p-1}) = \mathbb{Q}_p(\zeta_p).$$

Et finalement on a

$$K = L(\pi^{1/e}) \subset L(u^{1/e}, (-p)^{1/e}) \subset \mathbb{Q}_p(\zeta_{n\ell p}).$$

Cas 2 : $p = q \neq 2$ Soit $\mathbb{Q}_p \subset K$ une extension cyclique de degré p^m. Il existe une sous-extension cyclique totalement ramifiée $\mathbb{Q}_p \subset K^{\mathrm{tr}}$ de degré p^m contenue dans $\mathbb{Q}_p(\zeta_{p^{m+1}})$ (il suffit de prendre le corps fixé par le sous-groupe d'ordre $p-1$ dans le groupe de Galois). On a aussi une extension non-ramifié $\mathbb{Q}_p \subset K^{\mathrm{nr}}$ grâce au Théorème 3.1 qui est égale à $\mathbb{Q}_p(\zeta_n)$ pour certain $n \geq 1$. Comme $K^{\mathrm{tr}} \cap K^{\mathrm{nr}} = \mathbb{Q}_p$, on a que

$$\mathrm{Gal}(K^{\mathrm{tr}}K^{\mathrm{nr}}/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^m\mathbb{Z})^2.$$

Supposons par l'absurde que $K \not\subset \mathbb{Q}_p(\zeta_{p^{m+1}n})$. Alors

$$\mathrm{Gal}(K(\zeta_{p^{m+1}n})/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^m\mathbb{Z})^2 \times \mathbb{Z}/p^{m'}\mathbb{Z}$$

pour certain $m' \geq 1$. Comme $(\mathbb{Z}/p\mathbb{Z})^3$ est un quotient de ce groupe, on voit qu'il existe un corps L tel que $\mathrm{Gal}(L/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$.

La proposition suivante nous donne une contradiction qui termine le cas 2.

Proposition 4.2. *Soit $p \neq 2$. Alors il n'existe pas d'extension $\mathbb{Q}_p \subset L$ tel que $Gal(L/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$.*

Démonstration. Supposons qu'il existe une telle L. Alors $\mathbb{Q}_p \subset L(\zeta_p)$ est abélienne comme la composée de $\mathbb{Q}_p(\zeta_p)$ et L abéliennes et

$$\mathrm{Gal}(L(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \simeq (\mathbb{Z}/p\mathbb{Z})^3.$$

Cette extension est une extension de Kummer d'exposant p, donc il existe un sous-groupe $B \subset \mathbb{Q}_p(\zeta_p)^*$ contenant $\mathbb{Q}_p(\zeta_p)^{*p}$ avec

$$B' = B/(\mathbb{Q}_p(\zeta_p)^*)^p \simeq (\mathbb{Z}/p\mathbb{Z})^3 \quad \text{et} \quad \mathbb{Q}_p(\zeta_p)(B^{1/p}) = L(\zeta_p).$$

Soit $a \in B$ et $M = \mathbb{Q}_p(\zeta_p, a^{1/p})$. Alors $\mathbb{Q}_p \subset M$ est abélienne.

Soit τ un générateur du groupe $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ et $\omega \in \mathbb{Z}$ tel que $\tau(\zeta_p) = \zeta_p^\omega$.

Lemme 4.3. *On a l'égalité*

$$\tau(a) \equiv a^\omega \mod (\mathbb{Q}_p(\zeta_p)^*)^p.$$

Démonstration. Soit A le sous-groupe de B' engendré par a. La théorie de Kummer nous donne le morphisme non-dégénéré

$$\mathrm{Gal}(M/\mathbb{Q}_p(\zeta_p)) \times A \to \mu_p, \quad (\sigma, a) \mapsto \langle \sigma, a \rangle = \frac{\sigma(a^{1/p})}{a^{1/p}}.$$

Comme $\tau(\zeta_p) = \zeta_p^{\omega}$, on a $\tau(\zeta) = \zeta^{\omega}$ pour tout $\zeta \in \mu_p$. On en déduit alors

$$\tau(\langle \sigma, a \rangle) = \langle \sigma, a \rangle^{\omega} = \langle \sigma, a^{\omega} \rangle.$$

Or, pour une extension de τ à $\mathrm{Gal}(M/\mathbb{Q}_p)$ et $\sigma \in \mathrm{Gal}(M/\mathbb{Q}_p(\zeta_p))$, on a bien $\tau\sigma\tau^{-1} = \sigma$, car l'extension $\mathbb{Q}_p \subset M$ est abélienne. Alors

$$\tau(\langle \sigma, a \rangle) = \frac{\tau(\sigma(a^{1/p}))}{\tau(a^{1/p})} = \frac{(\tau\sigma\tau^{-1})(\tau(a^{1/p}))}{\tau(a^{1/p})} = \frac{\sigma(\tau(a^{1/p}))}{\tau(a^{1/p})} = \langle \sigma, \tau(a) \rangle,$$

car $\tau(a^{1/p})$ est un racine p-ième de $\tau(a)$ et on a vu dans la section 3.3 que $\langle \sigma, \tau(a) \rangle$ est indépendant du choix de la racine de $\tau(a)$. Donc on a

$$\langle \sigma, \tau(a) \rangle = \langle \sigma, a^{\omega} \rangle \quad \forall \sigma \in \mathrm{Gal}(M/\mathbb{Q}_p(\zeta_p)).$$

Et comme $\langle \cdot, \cdot \rangle$ est non-dégénéré, on a, par le Théorème 3.10, $\tau(a) \equiv a^{\omega} \mod (\mathbb{Q}_p(\zeta_p)^*)^p$. □

Donc, si v est la valuation sur $\mathbb{Q}_p(\zeta_p)$,

$$v(a) = v(\tau(a)) \equiv \omega v(a) \mod p.$$

Mais comme τ engendre $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$, on a $\omega \not\equiv 1 \mod p$. Et alors $v(a) \equiv 0 \mod p$.

Maintenant, par la Remarque 2.9 et le fait que $\mathbb{Q}_p(\zeta_p)$ est totalement ramifié, on voit que

$$\mathbb{Q}_p(\zeta_p)^* = (\zeta_p - 1)^{\mathbb{Z}} \times \mu_{p-1} \times U,$$

où $U = \{u \in \mathbb{Q}_p(\zeta_p) : u \equiv 1 \mod (\zeta_p - 1)\}$. Alors, en notant que $\mu_{p-1}^p = \mu_{p-1}$, on peut toujours multiplier a par une puissance p-ième et supposer $a \in U$. Donc on a

$$B' \subset U/U^p.$$

Lemme 4.4. *Notons $\pi = \zeta_p - 1$. Alors*

$$U^p = \{u \in \mathbb{Q}_p(\zeta_p) : u \equiv 1 \mod \pi^{p+1}\}.$$

Démonstration. Soit $u \in U$ et $b \in \mathbb{Z}$ tel que $u \equiv 1 + b\pi \mod \pi^2$ (on rappelle que comme $\mathbb{Q}_p \subset \mathbb{Q}_p(\zeta_p)$ est totalement ramifiée, il suffit de prendre $b \in \mathbb{Z}$ car le corps résiduel est $\mathbb{F}_p$). Comme

$$\zeta_p^b \equiv 1 + b\pi \mod \pi^2,$$

on voit que $u_1 = \zeta_p^{-b} u \equiv 1 \mod \pi^2$. Et en rappelant que $p \equiv 0 \mod \pi^{p-1}$ on trouve

$$u^p = u_1^p \equiv 1 \mod \pi^{p+1}.$$

D'autre part, soit $u_2 \equiv 1 \mod \pi^{p+1}$. On sait que dans $\mathbb{Q}_p[[x]]$ on a

$$\left(\sum_{n=0}^{\infty} \binom{1/p}{n} x^n \right)^p = 1 + x.$$

Alors, si $u_2 = 1 + d\pi^{p+1}$ avec $|d| \leq 1$, montrons que

$$\sum_{n=0}^{\infty} \binom{1/p}{n} (u_2 - 1)^n = \sum_{n=0}^{\infty} \left[\frac{1}{n!} \prod_{k=0}^{n-1} \left(\frac{1}{p} - k \right) \right] (d\pi^{p+1})^n \tag{5}$$

est convergente, ce qui nous donnera l'existence d'une racine p-ième de u_2. Pour montrer cela, soit v la valuation sur $\mathbb{Q}_p(\zeta_p)$ et v_p celle de $\mathbb{Q}_p$. Alors, on voit que $v(d^n \pi^{n(p+1)})) \geq n(p+1)$, et

$$v(n!) = (p-1)v_p(n!) = (p-1) \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor < (p-1) \sum_{i \geq 1} \frac{n}{p^i} = n$$

et

$$v\left(\prod_{k=0}^{n-1} \left(\frac{1}{p} - k \right) \right) = \sum_{k=0}^{n-1} v\left(\frac{1}{p} - k \right) = (p-1) \sum_{k=0}^{n-1} v_p\left(\frac{pk-1}{p} \right) = -n(p-1).$$

Donc si on appelle α_n le terme général de la série (5), on voit que

$$v(\alpha_n) > n(p+1) - n(p-1) - n = n,$$

ce qui montre que la série est bien convergente et alors $u_2^{1/p}$ existe dans $\mathbb{Q}_p(\zeta_p)$ et il est clairement dans U (le premier terme de la série est 1), donc $u_2 \in U^p$, ce qui conclut le lemme. □

Posons encore $u \in B$, et $u = \zeta_p^b u_1$ avec $u_1 \equiv 1 \mod \pi^2$ comme dans le lemme. Le Lemme 4.3 nous dit

$$\tau(u) \equiv u^\omega \mod U^p.$$

Et comme ζ_p vérifie aussi cette rélation, on voit que u_1 la vérifie aussi. Posons $u_1 = 1 + c\pi^d + \cdots$ avec $c \in \mathbb{Z}$, $(p, c) = 1$ et $d \geq 2$. En notant que

$$\frac{\tau(\pi)}{\pi} = \frac{1 - \zeta_p^\omega}{1 - \zeta_p} = 1 + \zeta_p + \cdots + \zeta_p^{\omega - 1} \equiv \omega \mod \pi,$$

on voit que

$$\tau(u_1) = 1 + c\omega^d \pi^d \mod \pi^{d+1}.$$

Mais d'autre part,

$$u_1^\omega = 1 + c\omega\pi^d \mod \pi^{d+1}.$$

Alors la rélation $\tau(u_1) \equiv u_1^\omega \mod U^p$ nous dit que, soit $d \geq p+1$, ou $d \leq p$ et $d \equiv 1 \mod p-1$, car ω est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Dans le premier cas, on trouve $u_1 \in U^p$ et dans l'autre on trouve $d = p$. Comme $1 + \pi^p$ engendre modulo U^p le sous-groupe de $u_1 \equiv 1 \mod \pi^p$, si on appelle $< \zeta_p, 1 + \pi^p > \subset U/U^p$ le sous-groupe engendré par ζ_p et $1 + \pi^p$, on a montré que

$$B' \subset < \zeta_p, 1 + \pi^p > \subset U/U^p,$$

Mais $B' \simeq (\mathbb{Z}/p\mathbb{Z})^3$ ne peut pas être engendré par deux éléments, donc on a une contradiction, ce qui termine la preuve. □

Cas 3 : $p = q = 2$ Soit $\mathbb{Q}_2 \subset K$ une extension cyclique de degré 2^m. On a déjà une extension totalement ramifié $K^{\mathrm{tr}} = \mathbb{Q}_2(\zeta_{2^{m+2}})$ avec

$$\mathrm{Gal}(K^{\mathrm{tr}}/\mathbb{Q}_2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}.$$

On a aussi l'extension non-ramifié $K^{\mathrm{nr}} = \mathbb{Q}_2(\zeta_n)$ pour certain $n \geq 1$ avec

$$\mathrm{Gal}(K^{\mathrm{nr}}/\mathbb{Q}_2) \simeq \mathbb{Z}/2^m\mathbb{Z}.$$

Et comme $K^{\mathrm{tr}} \cap K^{\mathrm{nr}} = \mathbb{Q}_2$, on a

$$\mathrm{Gal}(K^{\mathrm{tr}}K^{\mathrm{nr}}/\mathbb{Q}_2) \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^m\mathbb{Z})^2.$$

Supposons par l'absurde que $K \not\subset K^{\mathrm{tr}}K^{\mathrm{nr}}$. Alors, par le Théorème 3.5, $\mathrm{Gal}(KK^{\mathrm{tr}}K^{\mathrm{nr}}/\mathbb{Q}_2)$ est d'exposant 2^m, il a au plus 4 générateurs, dont un est d'ordre 2, et il a $\mathrm{Gal}(K^{\mathrm{tr}}K^{\mathrm{nr}}/\mathbb{Q}_2)$ comme quotient par un sous-groupe non trivial. Donc,

$$\mathrm{Gal}(KK^{\mathrm{tr}}K^{\mathrm{nr}}/\mathbb{Q}_2) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^m\mathbb{Z})^2 \times \mathbb{Z}/2^\ell\mathbb{Z} & \text{avec } \ell \geq 1, \\ \text{ou} \\ (\mathbb{Z}/2^m\mathbb{Z})^2 \times \mathbb{Z}/2^\ell\mathbb{Z} & \text{avec } m \geq \ell \geq 2. \end{cases}$$

Alors, il existe un sous-corps L de $\mathbb{Q}_2 \subset KK^{\mathrm{tr}}K^{\mathrm{nr}}$ tel que

$$\mathrm{Gal}(L/\mathbb{Q}_2) \simeq \begin{cases} (\mathbb{Z}/2\mathbb{Z})^4 \\ \text{ou} \\ (\mathbb{Z}/4\mathbb{Z})^3. \end{cases}$$

Encore une fois, on montrera que ceci est impossible.

Supposons $\mathrm{Gal}(L/\mathbb{Q}_2) \simeq (\mathbb{Z}/2\mathbb{Z})^4$. Alors $\mathbb{Q}_2 \subset L$ est une extension de Kummer d'exposant 2. Donc il existe un sous groupe $B \subset (\mathbb{Q}_2)^*$ contenant $\mathbb{Q}_2^{*2}$ avec

$$B' = B/\mathbb{Q}_2^{*2} \simeq (\mathbb{Z}/2\mathbb{Z})^4 \quad \text{et} \quad L = \mathbb{Q}_2(B^{1/2}).$$

Or, on sait que

$$\mathbb{Q}_2^* \simeq 2^{\mathbb{Z}} \times \{\pm 1\} \times U,$$

où $U = \{u \in \mathbb{Q}_2 : u \equiv 1 \mod 4\}$ (notons que $\{\pm 1\} \times U = \{u \in \mathbb{Q}_2 : u \equiv 1 \mod 2\} = \mathbb{Z}_2^*$). Alors

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \{\pm 1\} \times U/U^2.$$

On affirme que $U^2 = \{u \in \mathbb{Q}_2 : u \equiv 1 \mod 8\}$. L'une des inclusions est évidente, et pour l'autre, il suffit de changer p et π par 2 dans la deuxième partie de la preuve du Lemme 4.4 (où on remarque que $\mathbb{Q}_2(\zeta_2) = \mathbb{Q}_2(-1) = \mathbb{Q}_2$) et de noter que la śerie obtenue a comme premiers termes 1 et $4d$ avec $|d| \leq 1$. Alors on a que $U/U^2 \simeq \mathbb{Z}/2\mathbb{Z}$, et par conséquent,

$$B' \subset \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq (\mathbb{Z}/2\mathbb{Z})^3,$$

ce qui est une contradiction et élimine le premier cas.

Supposons maintenant que $\mathrm{Gal}(L/\mathbb{Q}_2) \simeq (\mathbb{Z}/4\mathbb{Z})^3$. On a alors que $i = \sqrt{-1} \in L$. Sinon, $\mathrm{Gal}(L(i)/\mathbb{Q}_2)$ aurait comme quotient le groupe $(\mathbb{Z}/2\mathbb{Z})^4$, ce qui est impossible par ce que l'on vient de montrer. Alors, comme $\mathrm{Gal}(L/\mathbb{Q}_2(i))$ est d'ordre 32 et tout sous-groupe d'ordre 32 de $(\mathbb{Z}/4\mathbb{Z})^3$ contient un sous-groupe de la forme $(\mathbb{Z}/4\mathbb{Z})^2$, en prenant M le corps fixé par ce sous-groupe on trouve que

$$\mathbb{Q}_2(i) \subset M \subset L \quad \text{et} \quad \mathrm{Gal}(M/\mathbb{Q}_2) \simeq \mathbb{Z}/4\mathbb{Z}.$$

Soit σ un générateur de $\mathrm{Gal}(M/\mathbb{Q}_2)$. Alors σ^2 engendre $\mathrm{Gal}(M/\mathbb{Q}_2(i))$ et $\sigma(i) = -i$. On peut écrire

$$M = \mathbb{Q}_2(i, \alpha),$$

pour certain $\alpha \in M$ avec $\alpha^2 \in \mathbb{Q}_2(i)$ et $\sigma^2(\alpha) = -\alpha$. Or,

$$\sigma^2(\sigma(\alpha)) = \sigma(\sigma^2(\alpha)) = \sigma(-\alpha) = -\sigma(\alpha),$$

et alors σ^2 fixe l'élément $\sigma(\alpha)/\alpha$, ce qui implique

$$\frac{\sigma(\alpha)}{\alpha} = A + Bi \in \mathbb{Q}_2(i),$$

avec $A, B \in \mathbb{Q}_2$, et donc

$$\frac{\sigma^2(\alpha)}{\sigma(\alpha)} = \sigma(A + Bi) = A - Bi.$$

On obtient finalement

$$A^2 + B^2 = \frac{\sigma(\alpha)}{\alpha}\frac{\sigma^2(\alpha)}{\sigma(\alpha)} = \frac{\sigma^2(\alpha)}{\alpha} = -1.$$

Le lemme suivante nous permet de conclure.

Lemme 4.5.

$$A^2 + B^2 + 1 = 0$$

n'a pas de solutions dans $\mathbb{Q}_2$.

Démonstration. En multipliant l'équation par une puissance de 2 appropriée, on se ramène au cas

$$A^2 + B^2 + C^2 = 0$$

avec $A, B, C \in \mathbb{Z}_2$ et 2 ne divisant pas l'une des variables. Supposons $2 \nmid A$. Alors, en regardant la restriction modulo 8,

$$1 + B^2 + C^2 \equiv 0 \mod 8,$$

ce qui n'a pas de solutions, car les carrés modulo 8 sont $0, 1$ et 4. □

Ceci conclut la preuve du Théorème 4.1. ◡̈ ◡̈ ◡̈

□

Références

[1] J.P. Serre, *Local Fields*, Springer, GTM 67, 1980

[2] Alain M. Robert, *A Course in p-adic Analysis* 2nd edition, Springer, GTM 198, 2000

[3] Serge Lang, *Algebra* 3rd Edition, Springer, GTM 211, 2002

[4] Lawrence C. Washington, *Introduction to cyclotomic fields* 2nd Edition, Springer, GTM 83, 1997

[5] Fernando Q. Gouvêa, *p-adic numbers : an introduction* 2nd Edition, Springer, 2000

[6] A. Frölich & M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, Cambridge Studies in Advanced Mathematics 27, 1991