THÉORIE DE LA RAMIFICATION

MARTIN DEBAISIEUX

Abstract. Ces notes se proposent d'aborder la ramification des premiers dans les extensions de corps de nombres via une étude locale. Nous commençons par une analyse locale, puis nous montrons comment insérer cette analyse dans le cas global. On applique enfin ces outils afin de démontrer la loi de réciprocité quadratique.

Table des matières

Date: 23 janvier 2023.

Partie I – Ramification locale

Cette première partie est rédigée sur base de [Mil20], [Neu99] et [Ser79] et fait suite à [De22a]. Je recommande de les consulter pour d'éventuels prérequis.

1. Extensions de corps locaux

Nous travaillons exclusivement avec des corps p-adiques dans cette première partie. Soit K un tel corps, nous adoptons les notations fonctorielles en K de v_K, $\mathcal{O}_K$, $\mathfrak{m}_K$ et π_K afin de désigner respectivement la valuation normalisée en K, son anneau des entiers, l'idéal maximal et une uniformisante. Étant donné L une extension finie de K, l'on a

$$\mathfrak{m}_K \mathcal{O}_L = \mathfrak{m}_L^e$$

pour un certain entier $e \geq 1$ que l'on appelle indice de ramification de L/K. Si l'on désigne par k et k_L les corps résiduels respectifs de K et L, le degré de l'extension résiduelle $f = [k_L : k]$ est appelé degré inertiel de L/K. Ces deux invariants forment ensemble

$$[L : K] = e_{L/K}\, f_{L/K}.$$

Cette identité fondamentale est bien connue et fait déjà l'objet d'une section d'un précédent document de l'auteur [De22a].

Proposition 1.1. *Soit $M \supseteq L \supseteq K$ une tour d'extensions finies de corps p-adiques. Alors $f_{M/K} = f_{M/L} f_{L/K}$ et $e_{M/K} = e_{M/L} e_{L/K}$.*

Démonstration. La multiplicativité des degrés inertiels découle simplement de celle des extensions de corps. La multiplicativité des indices de ramification s'ensuit. □

Définition 1.2. Une extension de corps p-adiques L/K est non ramifiée si $e = 1$, est ramifiée sinon. L'extension est dite totalement ramifiée quand $e = [L : K]$.

Alternativement, l'extension n'est pas ramifiée si et seulement si $f = [L : K]$, et est totalement ramifiée si et seulement si $f = 1$.

Remarque 1.3. Toute extension de degré premier est soit non ramifiée, soit totalement ramifiée. Nous construirons plus tard une extension de $\mathbf{Q}_p$ qui est simplement ramifiée.

Afin d'illustrer les prochains résultats et de nous constituer une première batterie d'exemples, nous terminons cette section par l'étude du cas très important des extensions cyclotomiques de $\mathbf{Q}_p$. Pour tout $n \geq 1$, soit ζ_n une racine primitive n-ième de l'unité prise dans une clôture algébrique fixée de $\mathbf{Q}_p$. Suivant la divisibilité de n par p, la nature de l'extension cyclotomique qu'elle engendre sur $\mathbf{Q}_p$ est nettement différente. On y résume ici une partie des informations incontournables dont on se souviendra.

	Ramification	**Degré**	**Groupe de Galois**
$p \nmid n$	non ramifiée	ord p dans $(\mathbf{Z}/n\mathbf{Z})^\times$	$\langle \zeta_n \mapsto \zeta_n^p \rangle$
$n = p^m$	totalement ramifiée	$p^{m-1}(p-1)$	$(\mathbf{Z}/p^m\mathbf{Z})^\times$
Sinon	ramifiée	produit	produit

Considérons d'abord le cas où p ne divise pas n et prenons plus généralement K un corps p-adique, de corps résiduel $k = \mathbf{F}_q$ où q est une puissance de p.

Proposition 1.4. *Soit $L = K(\zeta_n)$ où p ne divise pas n. L'extension L/K n'est pas ramifiée, de degré l'ordre multiplicatif de q* mod n *et de groupe de Galois canoniquement isomorphe à* $\mathrm{Gal}(k_L/k)$*, qui est engendré par $\zeta_n \mapsto \zeta_n^q$.*

Démonstration. Soit $\Phi_n(X) \in K[X]$ le polynôme minimal de ζ_n sur K. Sa réduction modulo $\mathfrak{m}_K$ est celui de $\bar{\zeta}_n$ sur k. En effet, $\overline{\Phi}_n$ divise $X^n - 1$ puisque p ne divise pas n et est donc séparable. Le lemme de Hensel implique qu'il ne peut se factoriser dans k. Puisque Φ et sa réduction sont de même degré,

$$[L : K] = [k(\bar{\zeta}_n) : k] = [k_L : k] = f.$$

Par conséquent L/K n'est pas ramifiée. De plus, $X^n - 1$ se factorise sur L et donc sur k_L, toujours car p ne divise pas n, en facteurs linéaires distincts. Dès lors $k_L = \mathbf{F}_{q^f}$ et ainsi f est le plus petit naturel tel que $\mu_n \subseteq \mathbf{F}_{q^f}^\times$, c'est-à-dire l'ordre multiplicatif de q mod n. □

Considérons désormais le cas où $n = p^m$ est une puissance de p et revenons à la situation où le corps de base est $\mathbf{Q}_p$.

Proposition 1.5. *Soit $L = \mathbf{Q}_p(\zeta_n)$ où $n = p^m$ est une puissance de p. L'extension $L/\mathbf{Q}_p$ est totalement ramifiée, de degré $\varphi(p^m)$ et de groupe de Galois canoniquement isomorphe à $(\mathbf{Z}/p^m\mathbf{Z})^\times$. Une uniformisante pour L est $1 - \zeta_n$.*

Démonstration. L'élément $\xi = \zeta_n^{p^{m-1}}$ est une racine primitive p-ième de l'unité et est donc racine de $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1 \in \mathbf{Q}_p[X]$. Posons

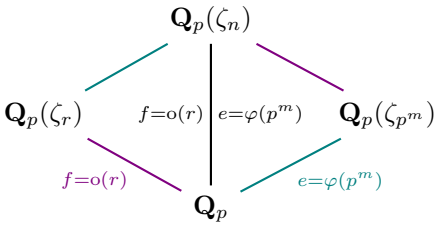
$$P(X) = \Phi_p(X^{p^{m-1}}) = X^{(p-1)p^{m-1}} + X^{(p-2)p^{m-1}} + \cdots + 1.$$

On a clairement que $\zeta_n - 1$ est racine de $P(X + 1)$. Or, ce dernier est d'Eisenstein car il est monique, $P(1) = p$ et $P(X + 1) \equiv X^{(p-1)p^{m-1}} \bmod p$. Dès lors P est le polynôme minimal de ζ_n sur $\mathbf{Q}_p$ et il en découle que $[L : \mathbf{Q}_p] = \varphi(p^m)$. L'injection canonique $\mathrm{Gal}(L/\mathbf{Q}_p) \hookrightarrow (\mathbf{Z}/p^m\mathbf{Z})^\times$ est alors bijective. Finalement,

$$\mathrm{Nm}_{L/\mathbf{Q}_p}(1 - \zeta_n) = P(1) = p.$$

Soit ω_L l'extension de la valuation normalisée v_p de $\mathbf{Q}_p$, alors $\varphi(p^m)\omega_L(1 - \zeta_n) = v_p(p) = 1$. Autrement dit $L/\mathbf{Q}_p$ est totalement ramifiée. □

Considérons finalement la dernière situation, où $n = p^m r$ est divisible par p mais n'en est pas une puissance (autrement dit $m = v_p(n) \neq 0$ et $r \neq 1$). Alors $\zeta_r = \zeta_n^{p^m}$ et $\zeta_{p^m} = \zeta_n^r$ sont des racines primitives respectivement r-ième et p^m-ième de l'unité. De plus, $\mathbf{Q}_p(\zeta_n) = \mathbf{Q}_p(\zeta_r)\mathbf{Q}_p(\zeta_{p^m})$. On se ramène aux cas précédents via le treillis suivant :



où l'on note o(r) l'ordre multiplicatif de p mod r. Dans cette situation, $\mathbf{Q}_p(\zeta_n)/\mathbf{Q}_p$ est (simplement) ramifiée. Son groupe de Galois est le produit direct du groupe de Galois de l'extension non ramifiée par celui de l'extension totalement ramifiée de la décomposition.

2. Extensions non ramifiées

Nous explorons dans cette section la situation des extensions non ramifiées d'un corps p-adique. Nous venons de montrer que $\mathbf{Q}_p$ admet une extension non ramifiée de degré n pour tout $n \geq 1$ réalisée par $\mathbf{Q}_p(\zeta_{p^n-1})$. Nous montrons ici qu'il s'agit de sa seule extension non ramifiée de degré n.

Théorème 2.1. *Soit K un corps p-adique. Les extensions non ramifiées de K sont en bijection avec les extensions de son corps résiduel k.*

Démonstration. Nous montrons que la catégorie des extensions non ramifiées de K est équivalente à celle des extensions de k, où les morphismes sont ceux de corps et où le foncteur est donné par l'association corps à corps résiduel.

(A) Nous commençons par montrer qu'étant donné L une extension non ramifiée de K et M une extension finie de K, l'application $\mathrm{Hom}_K(L,M) \to \mathrm{Hom}_k(k_L,k_M)$ obtenue par restriction à $\mathcal{O}_L$ puis par réduction est bijective. Tout d'abord, elle est bien définie car les morphismes de corps préservent les valuations. Pour montrer la bijectivité, on se donne $\overline{\alpha}$ un élément primitif de k_L/k et $\overline{P}$ son polynôme minimal sur k. Soit $P \in \mathcal{O}_K[X]$ un relèvement monique de $\overline{P}$ et soit $\alpha \in \mathcal{O}_L$ l'unique racine de P se relevant de $\overline{\alpha}$ par Hensel. Comme L/K n'est pas ramifiée, on a

$$[L:K] = [k_L:k] = \deg(\overline{P}) = \deg(P).$$

Mais P doit être irréductible sur K et donc $L = K(\alpha)$. Suite à cela, nous obtenons le diagramme commutatif suivant

$$\begin{array}{ccc} \mathrm{Hom}_K(L,M) & \xrightarrow{\sim} & \{x \in \mathcal{O}_M \mid P(x) = 0\} \\ \downarrow & & \downarrow \text{mod } \mathfrak{m}_M \\ \mathrm{Hom}_k(k_L,k_M) & \xrightarrow{\sim} & \{x \in k_M \mid \overline{P}(x) = 0\}. \end{array}$$

Étant donné que l'application de droite est bijective par le lemme de Hensel, celle de gauche l'est aussi.

(B) Nous montrons désormais que pour toute extension finie λ de k, il existe une unique extension non ramifiée L de K telle que $k_L = \lambda$. Pour cela, on se donne un élément primitif de λ/k. Avec les notations de (A) on construit $L = K(\alpha)$. Puisque k_L comprend une racine de $\overline{P}$, on a $\lambda \subseteq k_L$. Un argument de degré donne l'égalité. L'unicité de L est évidente en appliquant (A). □

Remarque 2.2. Le point (B) de la démonstration précédente est une version forte de l'essentielle surjectivité de l'équivalence de catégories : c'est une surjectivité. On note que L/K est galoisienne si et seulement si l'extension résiduelle k_L/k l'est, le cas échéant $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_L/k)$ canoniquement.

Exemple 2.3. Le corps $\mathbf{Q}_p$ admet donc une unique extension non ramifiée de degré n pour tout $n \geq 1$, donnée par $\mathbf{Q}_p(\zeta_{p^n} - 1)$ et de corps résiduel $\mathbf{F}_{p^n}$. En raison des notations en caractéristique p, il est commun de désigner par $\mathbf{Q}_{p^n}$ et $\mathbf{Z}_{p^n}$ l'extension correspondante et son anneau des entiers. Étant donné que toute extension finie de $\mathbf{F}_p$ est galoisienne, les extensions non ramifiées de $\mathbf{Q}_p$ le sont aussi.

Proposition 2.4. *Soit K un corps p-adique. La classe des extensions non ramifiées de K est distinguée.*

Démonstration. Nous montrons seulement que si L/K n'est pas ramifiée et si M/K est une extension finie, alors LM/M n'est pas ramifiée. En reprenant les notations de la démonstration précédente, on a $LM = M(\alpha)$. Soit $\overline{Q}$ le polynôme minimal de $\overline{\alpha}$ sur k_M. Par Hensel on a alors que $P = QH$ avec Q monique relevant $\overline{Q}$. On en déduit que Q est le polynôme minimal de α sur M et donc

$$[LM:M] = \deg(Q) = \deg(\overline{Q}) \leq [k_{LM}:k_M] \leq [LM:M].$$

Cela combiné à la multiplicativité des degrés inertiels impliquent que le compositum d'extensions non ramifiées est non ramifié. □

Définition 2.5. Étant donné un corps p-adique K, le compositum de ses extensions non ramifiée est noté K^{un} et est appelé l'extension maximale non ramifiée de K. Si L est une extension de K, on note $L_0 = L \cap K^{\mathrm{un}}$ l'extension maximale non ramifiée de K dans L.

Puisque l'on travaille dans un contexte p-adique, le corps résiduel de K^{un} n'est rien d'autre que la clôture algébrique (d'une extension finie) de $\mathbf{F}_p$. Le corps résiduel de L_0 est celui de L.

Exemple 2.6. L'extension maximale non ramifiée de $\mathbf{Q}_p$ est obtenue en adjoignant les racines (p^n-1)-ièmes de l'unité pour tout $n \geq 1$. Comme $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p) \simeq \mathbf{Z}/n\mathbf{Z}$, on en déduit que

$$\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{un}}/\mathbf{Q}_p) \simeq \varprojlim_{n \geq 1} \mathbf{Z}/n\mathbf{Z} = \widehat{\mathbf{Z}}.$$

Remarque 2.7. L'extension maximale non ramifiée de $\mathbf{Q}_p$ n'est pas p-adiquement complète. La démonstration proposée dans [Gou20, Theorem 6.8.4] construit une suite de Cauchy dans $\mathbf{Q}_p^{\mathrm{un}}$ qui ne converge pas dans la clôture algébrique de $\mathbf{Q}_p$. Cette même preuve montre que cette dernière n'est pas non plus complète, justifiant la construction de $\mathbf{C}_p$.

3. Extensions totalement ramifiées

Nous explorons à présent la situation des extensions totalement ramifiées. L'objet principal de cette section est de montrer que ces extensions sont issues d'une racine d'un polynôme d'Eisenstein.

Théorème 3.1. *Soit K un corps p-adique. Une extension finie L/K est totalement ramifiée si et seulement si $L = K(\alpha)$ où α est racine d'un polynôme d'Eisenstein sur K.*

Démonstration. Supposons $L = K(\alpha)$ où α est racine d'un polynôme d'Eisenstein P sur K de degré n. Si ω_L désigne l'extension de valuation normalisée sur K à L, alors $\omega_L(\alpha) = 1/n$. L'indice de ramification de L/K vaut par conséquent au moins n et nécessairement L/K est totalement ramifiée.

Si $\alpha \in L$ est un élément tel que $\omega_L(\alpha) = 1/n$, alors les $1, \alpha, \ldots, \alpha^{n-1}$ représentent des classes distinctes de $v_K(K^\times)$ dans $\omega_L(L^\times)$ et il est donc impossible d'obtenir une relation non triviale

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$$

pour $a_i \in K$ non tous nuls. On en déduit que α est un élément primitif de L/K. On peut donc exprimer α^n selon les autres, ce qui définit un polynôme d'Eisenstein sur K par le principe bien connu [Mil20, 7.11]. □

Remarque 3.2. La démonstration précédente montre que π_L est un élément primitif de L/K. Ainsi, tout élément $x \in L$ peut s'écrire de manière unique sous la forme $x = a_0 + a_1\pi_L + \cdots + a_{n-1}\pi_L^{n-1}$ avec les $a_i \in K$. On a alors $y \in \mathcal{O}_L$ si et seulement si $v_K(a_i) \geq 0$ pour tout i, ou encore si et seulement si $x \in \mathcal{O}_K[\pi_L]$. Par conséquent il est aussi vrai que $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

Exemple 3.3. Étant donné un corps p-adique K, on peut construire une extension totalement ramifiée de degré n pour chaque $n \geq 1$ en lui adjoignant une racine du polynôme d'Eisenstein $X^n - \pi_K$. Elle n'est en général pas unique.

Remarque 3.4. Contrairement à la classe des extensions non ramifiées, celle des extensions totalement ramifiées n'est pas distinguée. Supposons p impair et $n \in \mathbf{Z}$ non divisible par p et n'étant pas un résidu quadratique modulo p. Alors le corps $L = \mathbf{Q}_p(\sqrt{p}, \sqrt{np})$ provient du compositum de deux extensions totalement ramifiées

et pourtant il comprend l'élément $\sqrt{n}$ qui donne lieu à une extension non ramifiée de $\mathbf{Q}_p$. Par conséquent $L/\mathbf{Q}_p$ est simplement ramifiée.

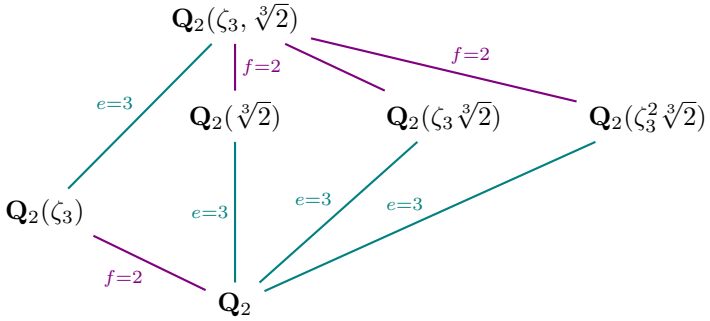
Exemple 3.5. Pour tout $n \geq 1$, l'extension de $\mathbf{Q}_p$ engendrée par ζ_{p^n} est totalement ramifiée de groupe de Galois canoniquement isomorphe à $(\mathbf{Z}/p^n\mathbf{Z})^\times$. En passant à la limite directe sur ces extensions, on définit le corps $\mathbf{Q}_p(\zeta_{p^\infty})$ qui est une extension totalement ramifiée de $\mathbf{Q}_p$ et

$$\mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^\infty})/\mathbf{Q}_p) \simeq \mathbf{Z}_p^\times.$$

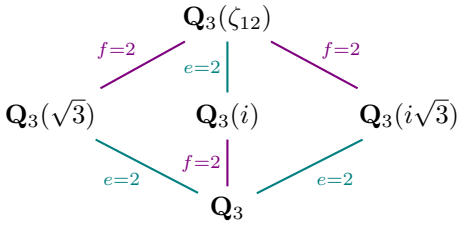
Remarque 3.6. Le théorème de Kronecker-Weber (dans sa version locale) affirme que l'extension abélienne maximale de $\mathbf{Q}_p$ est engendrée par les racines de l'unité. Celle-ci est dès lors composée de l'extension maximale non ramifiée $\mathbf{Q}_p^{\mathrm{un}}$ et de l'extension cyclotomique $\mathbf{Q}_p(\zeta_{p^\infty})$. Puisqu'elles sont linéairement disjointes, on en déduit que

$$\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ab}}/\mathbf{Q}_p) \simeq \widehat{\mathbf{Z}} \times \mathbf{Z}_p^\times.$$

Exemple 3.7. Comme nous l'avons déjà implicitement fait, nous adoptons trois couleurs selon la ramification : **non ramifiée**, simplement **ramifiée** et **totalement ramifiée**. Considérons le corps $\mathbf{Q}_2(\zeta_3, \sqrt[3]{2})$. La théorie de Galois nous apprend que le treillis complet est :



Exemple 3.8. On reprend le même code couleur mais ici l'on s'intéresse au treillis complet de $\mathbf{Q}_3(\zeta_{12})/\mathbf{Q}_3$:



Ces deux exemples ne sont pas justifiés. On laisse le soin au lecteur de calculer les indices de ramification en utilisant les outils précédents.

Proposition 3.9. *Soit K un corps p-adique. À isomorphisme près il n'existe qu'un nombre fini d'extensions totalement ramifiées de K d'un degré fixé.*

Démonstration. Soit $n \geq 2$ un degré fixé, nous montrons qu'il n'y a qu'un nombre fini d'extensions totalement ramifiées de degré au plus n. Chaque point $(a_1, \ldots, a_n)$ de $\mathfrak{m}_K \times \cdots \times \mathfrak{m}_K \times \pi_K \mathcal{O}_K^\times$ définit un polynôme d'Eisenstein de degré n et par conséquent un ensemble fini d'extensions totalement ramifiées de degré n. Selon le lemme de Krasner [Mil20, Proposition 7.63], chaque point du produit possède un voisinage dont tous les points donnent lieu aux mêmes extensions de K. Ce produit étant compact, il suffit d'un nombre fini de ces voisinages pour le recouvrir. □

4. Extensions modérément ramifiées

Nous avons vu à quel point les extensions non ramifiées sont faciles à décrire. La situation avec ramification n'est hélas pas aussi simple. On procède à une nouvelle dichotomie au sein des extensions ramifiées. Suivant la divisibilité par p de l'indice de ramification, il est plus ou moins facile d'étudier ces extensions. On s'intéresse ici au cas le plus simple des deux.

Définition 4.1. Une extension de corps p-adiques L/K est modérément ramifiée si p ne divise pas $e_{L/K}$, est sauvage sinon.

Exemple 4.2. Étant donné K un corps p-adique, les extensions de K de la forme $K(\sqrt[n]{\pi_K})$ avec n non divisible par p sont modérément ramifiées. Si n est un multiple de p, elles sont alors sauvages.

Remarque 4.3. Une extension L/K de corps p-adique est modérée si et seulement si l'est L/L_0. Plus généralement, L/K est modérée si et seulement si $LK^{\mathrm{un}}/K^{\mathrm{un}}$ est modérée. Il faut toutefois être plus prudent car K^{un} n'est pas un corps p-adique mais il est hensélien.

Théorème 4.4. *Soit K un corps p-adique. Si L/K^{un} est une extension modérée ramifiée de degré n, alors $L = K^{un}(\sqrt[n]{\pi_K})$.*

Démonstration. Soit $\alpha \in L$ un élément primitif de L/K^{un}. Puisque cette extension est nécessairement totalement ramifiée de degré n, il en va de même pour $K(\alpha)/E$ avec $E = K(\alpha) \cap K^{\mathrm{un}}$ et donc

$$\pi_K = u\pi_{K(\alpha)}^n$$

pour une unité u de $K(\alpha)$. Nous montrons que π_K est une puissance n-ième dans une extension non ramifiée F/K. La réduction de $X^n - u$ modulo $\mathfrak{m}_{K(\alpha)}$ admet une racine simple dans une extension finie k_F de $k_{K(\alpha)}$ car p ne divise pas n. En appliquant le lemme de Hensel à $X^n - u \in \mathcal{O}_F[X]$ nous obtenons une racine n-ième de u dans $F \subseteq L$. □

Proposition 4.5. *Soit K un corps p-adique. La classe des extensions non ramifiées de K est distinguée.*

Démonstration. Nous montrons que si L/K est modérément ramifiée et si M/K est finie, alors LM/M est modérément ramifiée. Supposons de nouveau $K = K^{\mathrm{un}}$. Comme L/K est modérément ramifiée, on peut écrire $L = K(\sqrt[n]{\pi_K})$ avec n le degré de L/K via le résultat précédent. Alors $LM = M(\sqrt[n]{\pi_K})$ et est donc modérément ramifié sur M. □

Définition 4.6. Étant donné un corps p-adique K, le compositum de ses extensions modérément ramifiées est noté K^{tm} et est appelé l'extension maximale modérément ramifiée de K. Si L est une extension de K, on note l'extension maximale modérément ramifiée de K dans L par $L_1 = L \cap K^{\mathrm{tm}}$.

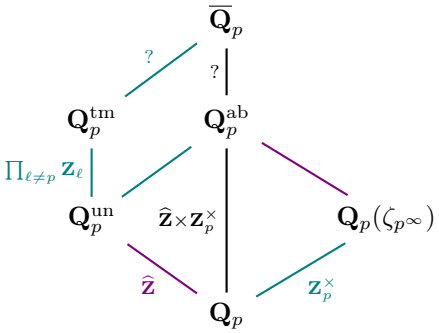
Puisque l'on travaille dans un contexte p-adique, le corps résiduel de K^{tm} est contraint d'être la clôture algébrique (d'une extension finie) de $\mathbf{F}_p$. Celui de L_1 est le corps résiduel associé à L.

Exemple 4.7. On a vu que $\mathbf{Q}_p^{\mathrm{tm}}$ est obtenu en adjoignant à $\mathbf{Q}_p^{\mathrm{un}}$ toutes les racines n-ièmes de p pout tout $n \geq 1$ non divisible par p. Dès lors,

$$\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{tm}}/\mathbf{Q}_p^{\mathrm{un}}) \simeq \prod_{\ell \neq p} \mathbf{Z}_\ell.$$

En effet, $\mathbf{Q}_p^{\mathrm{un}}$ est lui-même obtenu en adjoignant à $\mathbf{Q}_p$ les racines primitives n-ièmes de l'unité pour n non divisible par p, et l'on a $\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{un}}(\sqrt[n]{p})/\mathbf{Q}_p^{\mathrm{un}}) \simeq \mathbf{Z}/n\mathbf{Z}$.

Nous obtenons ce diagramme, dans lequel nous plaçons un condensé des informations apprises jusqu'à présent sur les groupes de Galois :



Exemple 4.8. Chacune des extensions présentes dans les Exemples 3.7 et 3.8 sont modérément ramifiées. Par contre, avec $p = 3$ en 3.7 nous obtenons une toute autre situation :

$\mathbf{Q}_3(\zeta_3, \sqrt[3]{2})$	$\mathbf{Q}_3(\zeta_3)$	$\mathbf{Q}_3(\sqrt[3]{2})$	$\mathbf{Q}_3(\zeta_3\sqrt[3]{2})$	$\mathbf{Q}_3(\zeta_3^2\sqrt[3]{2})$	/
sauvage					$\mathbf{Q}_3(\zeta_3)$
non ramifiée					$\mathbf{Q}_3(\sqrt[3]{2})$
non ramifiée					$\mathbf{Q}_3(\zeta_3\sqrt[3]{2})$
non ramifiée					$\mathbf{Q}_3(\zeta_3^2\sqrt[3]{2})$
sauvage	mod. ramifiée	sauvage	sauvage	sauvage	$\mathbf{Q}_3$

5. Groupes de ramification

Soit L/K une extension galoisienne de corps p-adiques. Dans cette section, nous décomposons le groupe $G = \mathrm{Gal}(L/K)$ en plus petits sous-groupes afin de capturer la ramification de L/K. Notons $|\cdot|_L$ la valeur absolue sur L étendant la p-adique. On définit une filtration exhaustive décroissante de G via

$$G_i = \{\sigma \in G \mid |\sigma(\alpha) - \alpha|_L < |\pi_L|_L^i \text{ pour tout } \alpha \in \mathcal{O}_L\}$$

cela pour tout entier $i \geq 0$. On appelle respectivement G_0, G_1 et tous les autres le groupe d'inertie, le groupe de ramification et les groupes de ramification supérieurs de L/K. De façon équivalente :

$$G_i = \mathrm{Ker}\left(G \to \mathrm{Aut}_{k-\mathrm{alg}}\left(\mathcal{O}_L/\mathfrak{m}_L^{i+1}\right)\right)$$

pour tout $i \geq 0$. Remarquons également que les G_i sont triviaux à partir d'un certain rang. En somme, nous venons de définir une filtration exhaustive décroissante finie de G par des sous-groupes normaux

$$\mathrm{Gal}(L/K) = G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{i\gg 0} = 1.$$

Nous montrons que G est résoluble. Ce résultat met en lumière une contrainte très forte quant aux groupes de Galois d'extensions p-adiques ; en particulier A_5 ne peut être le groupe de Galois d'une telle extension.

Proposition 5.1. *Le sous-corps de L fixe par l'action de G_0 est l'extension maximale non ramifiée L_0 de L/K, avec $G/G_0 \simeq \mathrm{Gal}(L_0/K) \simeq \mathrm{Gal}(k_L/k)$.*

Démonstration. Nous savons que l'application naturelle $\mathrm{Gal}(L_0/K) \to \mathrm{Gal}(k_L/k)$ est un isomorphisme. Toutefois, G_0 est le noyau du morphisme $G \to \mathrm{Gal}(k_L/k)$ qui est surjectif. Le résultat en découle. □

Lemme 5.2. *Pour tout $i \geq 1$, on a $G_i = \{\sigma \in G \mid |\sigma(\pi_L) - \pi_L|_L < |\pi_L|_L^i\}$.*

Démonstration. Soit A l'anneau des entiers de L_0, alors $\mathcal{O}_L = A[\pi_L]$. Il suffit donc de vérifier la condition en π_L. □

Proposition 5.3. *L'application $\rho_0 \colon G_0 \to k_L^\times \colon \sigma \mapsto \sigma(\pi_L)/\pi_L \bmod \mathfrak{m}_L$ est un morphisme de groupes. Son noyau est G_1 et donc G_0/G_1 est abélien.*

Démonstration. Cette application est bien définie et est indépendante du choix de l'uniformisante par définition de G_0. De cela, s'ensuit que ρ_0 est un morphisme de groupes. Finalement, G_1 est son noyau car $\sigma(\pi_L)/\pi_L \equiv 1 \bmod \mathfrak{m}_L$ si et seulement si $\sigma(\pi_L) \equiv \pi_L \bmod \mathfrak{m}_L^2$, ou encore si et seulement si $\sigma \in G_1$ par la reformulation du Lemme 5.2. □

Proposition 5.4. *L'application $\rho_i \colon G_i \to k_L \colon \sigma \mapsto (\sigma(\pi_L) - \pi_L)/\pi_L^{i+1} \bmod \mathfrak{m}_L$ est un morphisme de groupes pour tout $i \geq 1$. Son noyau est G_{i+1} et donc G_i/G_{i+1} est abélien.*

Démonstration. On utilise le Lemme 5.2 pour montrer que les applications ρ_i sont bien définies. Soient σ et $\tau \in G_i$. Pour vérifier que ρ_i est un morphisme, il suffit de montrer que $\sigma(\tau(\pi_L) - \pi_L) \equiv \tau(\pi_L) - \pi_L \bmod \mathfrak{m}_L^{i+2}$. Bien sûr, si π_L est fixe par τ cela est évident. Sinon, on a $\tau(\pi_L) = u\pi_L$ avec $u \in \mathcal{O}_L^\times$ et $u \neq 1$, et la congruence précédente devient

$$\frac{\sigma(u-1)}{(u-1)} \frac{\sigma(\pi_L)}{\pi_L} \equiv 1 \bmod \mathfrak{m}_L$$

ce qui est vrai puisque $\sigma \in G_0$. La détermination du noyau s'effectue comme avant, en utilisant le Lemme 5.2. □

Remarque 5.5. Le groupe $\mathcal{O}_L^\times$ admet une filtration décroissante de sous-groupes $(U^i)_{i\geq 1}$ définis par $U^i = 1 + \mathfrak{m}_L^i$ pour tout entier $i \geq 1$. Par conséquent, les quotients successifs sont $U^i/U^{i+1} \simeq k_L \simeq G_i/G_{i+1}$ pour tout $i \geq 1$.

Théorème 5.6. *Soit L/K une extension galoisienne de corps p-adiques. Alors le groupe $G = \mathrm{Gal}(L/K)$ est résoluble.*

Démonstration. Étant donné que k est un corps fini, le quotient G/G_0 est cyclique et donc abélien par la Proposition 5.1. Les deux propositions précédentes montrent que les autres quotients successifs sont abéliens. □

Proposition 5.7. *Le groupe G_1 est l'unique p-Sylow de G_0. Le sous-corps de L fixe par l'action de G_1 est l'extension maximale modérément ramifiée L_1 de L/K, avec $G/G_1 \simeq \mathrm{Gal}(L_1/K)$.*

Démonstration. Nous savons que les quotients G_i/G_{i+1} se plongent dans k_L pour tout $i \geq 1$ et sont donc des p-groupes. En particulier G_1 l'est aussi car

$$|G_1| = (G_1 : G_2)(G_2 : G_3) \cdots (G_{i-1} : 1) \in p^{\mathbf{N}}.$$

pour un $i \gg 0$. Il s'agit d'un p-Sylow de G_0 car G_0/G_1 se plonge dans $k_L^\times$ d'ordre non divisible par p. L'unicité provient du fait que G_1 est normal dans G_0. L'autre assertion s'ensuit immédiatement. □

Nous obtenons une reformulation des types de ramification en termes de groupes de ramification :

$$\begin{aligned} L/K \text{ est modérément ramifiée} &\Leftrightarrow G_1 = 1. \\ L/K \text{ est non ramifiée} &\Leftrightarrow G_0 = 1. \\ L/K \text{ est totalement ramifiée} &\Leftrightarrow G_0 = G. \end{aligned}$$

Les groupes de ramification supérieurs de L/K apportent plus de finesse dans la partie sauvage, mais cela n'est pas traité dans ces notes.

Exemple 5.8. Prenons $K = \mathbf{Q}_p$ et notons $K_n = \mathbf{Q}_p(\zeta_{p^n})$ pour tout entier $n \geq 1$. Les groupes de ramification de $G = \mathrm{Gal}(K_n/K)$ sont :

$$G_i = \begin{cases} \mathrm{Gal}(K_n/K) & \text{si } i = 0, \\ \mathrm{Gal}(K_n/K_s) & \text{si } p^{s-1} \leq i < p^s \text{ avec } 1 \leq s \leq n-1, \\ 1 & \text{si } i \geq p^{n-1}. \end{cases}$$

Soit $\varepsilon = (1, \zeta_p, \zeta_{p^2}, \cdots) \in \mathbf{Z}_p(1)$ une suite cohérente de racines primitives de l'unité. Étant donné $\sigma \in G$ non trivial, nous posons $a \in \mathbf{Z}$ tel que $\sigma(\zeta_{p^n}) = \zeta_{p^n}^a$, ainsi que $s = v_p(a-1)$ et $c = (a-1)/p^s$. Dès lors,

$$\sigma(\zeta_{p^n}) - \zeta_{p^n} = \zeta_{p^n}(\zeta_{p^{n-s}}^c - 1).$$

Le deuxième facteur est une uniformisante pour K_{n-s} et donc le tout est de valuation $[K_n : K_{n-s}] = p^s$. Du Lemme 5.2 nous avons que $\sigma \in G_{p^s-1}$ et $\sigma \notin G_{p^s}$. D'un autre côté, p^s est la plus grande puissance de p divisant $a-1$, ce qui signifie que $\sigma \in \mathrm{Gal}(K_n/K_s)$ et $\sigma \notin \mathrm{Gal}(K_n/K_{s+1})$.

Remarque 5.9. Le fichier `ramification_groups.py` joint dans le délivrable imprime les groupes de ramification d'une extension cyclotomique totalement ramifiée de $\mathbf{Q}_p$. Pour l'employer, on entre `python3 ramification_groups.py p n` en spécialisant `p` et `n` selon les conventions de l'exemple précédent.

Partie II – Ramification globale

Cette seconde partie est principalement rédigée sur base de [Mil20], en supposant que le lecteur a pris connaissance de [De22a] et [De22b].

6. Places d'un corps de nombres

Nous nous intéressons maintenant à la situation des corps de nombres, un cas particulier des corps globaux. Étant donné une extension finie de corps de nombres et une valeur absolue sur le corps de base, nous cherchons tout d'abord à caractériser toutes les extensions de cette dernière.

Théorème 6.1. *Soit $(K, |\cdot|)$ un corps de nombres valué et soit $L = K(\alpha)$ une extension finie de K. Les extensions de $|\cdot|$ à L sont en correspondance avec les facteurs irréductibles moniques du polynôme minimal de α sur K dans $\widehat{K}[X]$.*

Démonstration. Soit $P \in K[X]$ le polynôme minimal de α sur K. Si l'on se donne une extension de $|\cdot|$ à L, on peut compléter L et l'on a $\widehat{L} = \widehat{K}(\alpha)$. Notons Q le polynôme minimal de α sur $\widehat{K}$, alors Q divise P dans $\widehat{K}[X]$. Nous obtenons donc pour chaque extension de $|\cdot|$ un facteur irréductible de P dans $\widehat{K}[X]$. Réciproquement, si Q est un facteur irréductible monique de P dans $\widehat{K}[X]$, alors L se plonge dans $\widehat{K}(x) = \widehat{K}[X]/(g(X))$ via $\alpha \mapsto x$. La valeur absolue sur $\widehat{K}$ s'étend de manière unique à $\widehat{K}(x)$ et cela induit une valeur absolue sur L. Ces opérations sont inverses l'une de l'autre. □

L'on retrouve bien entendu le fait que pour un corps valué complet, les extensions de sa valeur absolue sont uniques. Nous l'avons d'ailleurs utilisé afin de prouver le théorème précédent.

Corollaire 6.2. *Soit $(K, |\cdot|)$ un corps de nombres valué et soit L/K une extension finie. Soient $L_1, \ldots, L_g$ les complétions de L selon les différentes valeurs absolues étendant $|\cdot|$. Alors $L \otimes_K \widehat{K} \simeq L_1 \cdots L_g$.*

Démonstration. Soit α un élément primitif de L/K de polynôme minimal P. En particulier $L = K(\alpha) = K[X]/(P(X))$. Notons $P = P_1 \cdots P_g$ la décomposition en facteurs irréductibles moniques dans $\widehat{K}[X]$. D'après le théorème des restes chinois, l'on a

$$L \otimes_K \widehat{K} = \widehat{K}[X]/(P(X)) \simeq \prod_{i=1}^{g} \widehat{K}[X]/(P_i(X))$$

et le résultat découle du Théorème 6.1. □

Corollaire 6.3. *Soit $(K, |\cdot|)$ un corps de nombres valué et soit L/K une extension finie. Soient $L_1, \ldots, L_g$ les complétions de L selon les différentes valeurs absolues étendant $|\cdot|$. Alors $\mathrm{Nm}_{L/K} = \prod_{i=1}^{g} \mathrm{Nm}_{L_i/\widehat{K}}$ et $\mathrm{Tr}_{L/K} = \sum_{i=1}^{g} \mathrm{Tr}_{L_i/\widehat{K}}$.*

Démonstration. La norme d'un élément $x \in L$ est le déterminant de l'application K-linéaire de multiplication par x. Celle-ci est invariante par tensorisation avec $\widehat{K}$. On voit aisément que la norme dans le produit se décompose en un produit. Il en va de même pour la trace. □

Remarque 6.4. Supposons que L/K est une extension de corps de nombres telle que $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Munissons K d'une valeur absolue $\mathfrak{p}$-adique pour un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$. En reprenant les notations précédentes, comme les P_i sont irréductibles dans $\widehat{K}[X]$, le lemme de Hensel montre que P_i est une puissance e_i d'un polynôme irréductible $Q_i \in \mathcal{O}_L[X]$. Par [Mil20, Theorem 3.41] l'on a

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} (\mathfrak{p}, Q_i(\alpha))^{e_i}.$$

Ainsi, les valeurs absolues sur L étendant la $\mathfrak{p}$-adique fixée correspondent aux idéaux premiers $(\mathfrak{p}, Q_i(\alpha))$.

Définition 6.5. Une place d'un corps de nombres K est une classe d'équivalence de valeurs absolues non triviales sur K. L'ensemble des places sur K est $S(K)$.

Exemple 6.6. Les places sur $\mathbf{Q}$ sont les premiers naturels et ce que l'on note infini, donnant respectivement lieu aux valeurs absolues p-adiques et à la valeur absolue archimédienne.

Compte tenu de la première partie de cette section, nous disons qu'une place w de L une extension finie d'un corps de nombres K divise une place v de K si les valeurs absolues de w étendent celles de v. Nous allons généraliser la formule bien connue du produit. Rappelons qu'une valeur absolue est normalisée s'il s'agit de la valeur absolue usuelle[1] sur $\mathbf{R}$, le carré de l'usuelle sur $\mathbf{C}$ et $(\mathcal{O}_K : \mathfrak{p})^{-v_{\mathfrak{p}}(\cdot)}$ si elle est définie en un premier $\mathfrak{p}$.

Lemme 6.7. *Soit L/K une extension de corps de nombres. Pour tout $v \in S(K)$, l'on a $\prod_{w|v} |\cdot|_w = |\mathrm{Nm}_{L/K}(\cdot)|_v$ où les valeurs absolues sont normalisées.*

Démonstration. Découle du Corollaire 6.3 et de l'extension de valeurs absolues sur des corps complets. □

Théorème 6.8 (Formule du produit)**.** *Soit K un corps de nombres. En prenant les valeurs absolues normalisées, l'on a $\prod_{w \in S(K)} |x|_w = 1$ pour tout $x \in K^\times$.*

Démonstration. On se ramène à la formule du produit sur $\mathbf{Q}$ via le Lemme 6.7 et l'on a

$$\prod_{w \in S(K)} |x|_w = \prod_{v \in S(\mathbf{Q})} \left(\prod_{w|v} |x|_w \right) = \prod_{v \in S(\mathbf{Q})} |\mathrm{Nm}_{K/\mathbf{Q}}(x)|_v = 1.$$

□

[1] Celle-ci n'est pas une valeur absolue. Il existe divers moyens de contourner ce problème mais le mieux pour ce document est de simplement l'ignorer.

Nota Bene 6.9. Artin et Whaples ont donné une caractérisation des corps globaux dans [AW45] dans le language des places. Soit K est un corps muni d'un ensemble S de places satisfaisant les points :

(A1) Il existe un ensemble de représentants v des places tel que pour tout $x \in K^\times$ l'on ait $|x|_v \neq 1$ en un nombre fini de places et $\prod_{v\in S} |x|_v = 1$;
(A2) Il existe au moins une place v telle que K_v est un corps local.

Alors K est un corps global et S est l'ensemble de ses places. Réciproquement, tout corps global satisfait (A1) et (A2).

7. Groupes de décomposition

Étudier le groupe de Galois d'une extension de $\mathbf{Q}$ peut être une tâche ardue. À ce jour, on ne sait pas encore décrire le groupe de Galois absolu de $\mathbf{Q}$. La multitude de premiers et *a fortiori* la ramification n'arrange en rien cette étude. Pour faciliter un peu cela, on décompose le groupe en chaque premier, permettant après complétion de travailler localement.

Définition 7.1. Soit L un corps de nombres galoisien sur $\mathbf{Q}$ et soit $\mathfrak{p}$ un premier de $\mathcal{O}_L$ étendant un premier $p \in \mathbf{Z}$ fixé. Le groupe de décomposition de $G = \mathrm{Gal}(L/\mathbf{Q})$ en $\mathfrak{p}$ est $D_\mathfrak{p} = \{\sigma \in G \mid \sigma\mathfrak{p} = \mathfrak{p}\}$.

Afin de garder la définition concise, nous n'avons pas déterminé la nature de cet objet. Le groupe G agit sur le spectre de $\mathcal{O}_L$ et cette action est transitive lorsqu'elle est restreinte à $S_p(L)$ les premiers divisant p [Mil20, Theorem 3.34]. Le groupe $D_\mathfrak{p}$ est le stabilisateur de $\mathfrak{p}$ pour cette action. Ces deux sections finales se généralisent naturellement de $\mathbf{Q}$ à un corps de nombres quelconque simplement en adaptant les notations.

Lemme 7.2. *Soient L et $\mathfrak{p}$ comme avant. Si $\mathfrak{q} \in S_p(L)$ est un autre premier, alors $D_\mathfrak{p}$ et $D_\mathfrak{q}$ sont conjugués via n'importe quel automorphisme de L envoyant $\mathfrak{p}$ sur $\mathfrak{q}$.*

L'action de G sur $S_p(L)$ étant transitive, tous les groupes de décomposition des premiers de $\mathcal{O}_L$ divisant p sont conjugués. Combiné au fait que l'ensemble $S_p(L)$ est de cardinalité $g = (G : D_\mathfrak{p})$ par le théorème de l'orbite-stabilisateur, nous obtenons le résultat suivant.

Théorème 7.3. *Soient L et $\mathfrak{p}$ comme avant. L'extension $L_\mathfrak{p}/\mathbf{Q}_p$ des complétés est galoisienne, de groupe de Galois $\mathrm{Gal}(L_\mathfrak{p}/\mathbf{Q}_p) \simeq D_\mathfrak{p}$.*

Démonstration. Tout élément $\sigma \in D_\mathfrak{p}$ s'étend par continuité de manière unique en un automorphisme $\mathbf{Q}_p$-linéaire de $L_\mathfrak{p}$. Dès lors $|D_\mathfrak{p}| \leq [L_\mathfrak{p} : \mathbf{Q}_p]$. Toutefois l'on sait que $|D_\mathfrak{p}| = |D_{\tau\mathfrak{p}}|$ pour tout $\tau \in G$ par le Lemme 7.2. De cette façon, nous obtenons que

$$|G| = (G : D_\mathfrak{p}) \cdot |D_\mathfrak{p}| \leq \sum_{\tau \in G/D_\mathfrak{p}} [L_{\tau\mathfrak{p}} : \mathbf{Q}_p] = [L : \mathbf{Q}] = |G|$$

où l'avant-dernière égalité provient du Corollaire 6.2. Nous en déduisons que $|D_\mathfrak{p}| = [L_\mathfrak{p} : \mathbf{Q}_p] = |\mathrm{Gal}(L_\mathfrak{p}/\mathbf{Q}_p)|$ et donc l'assertion. □

Définition 7.4. Soient L et $\mathfrak{p}$ comme avant. Le groupe d'inertie $I_\mathfrak{p}$ de G en $\mathfrak{p}$ est le noyau du morphisme $D_\mathfrak{p} \to \mathrm{Gal}(k_{L_\mathfrak{p}}/\mathbf{F}_p)$ résultant du Théorème 7.3.

La flèche précédente est surjective, on a alors une suite exacte. Le rôle du groupe de décomposition est d'isoler l'extension $L/L^{D_\mathfrak{p}}$ des autres premiers divisant p, alors que celui de l'inertie est d'isoler la ramification dans cette extension. Cette découpe est fondamentale et permet d'amener l'étude locale. Nous en sommes donc au point culminant de cette seconde partie, où toutes les informations sont comprises dans la Figure 1.

Proposition 7.5. *Les indices de ramification, ainsi que les degrés inertiels de la tour d'extensions $L \supseteq L^{I_\mathfrak{p}} \supseteq L^{D_\mathfrak{p}} \supseteq \mathbf{Q}$ sont donnés par la Figure 1.*

Démonstration. Nous commençons par montrer que $[L^{D_\mathfrak{p}} : \mathbf{Q}] = g$. Par la théorie de Galois, on sait que ce degré vaut $(G : D_\mathfrak{p})$ et cette quantité est égale à g. Au vu des contraintes sur les indices et degrés, on en déduit les annotations de l'étage du bas de chaque tour. De nouveau, la théorie de Galois nous apprend que $|D_\mathfrak{p}| = ef$ et donc la suite exacte donne $|I_\mathfrak{p}| = e$. Les deux autres étages s'ensuivent. □

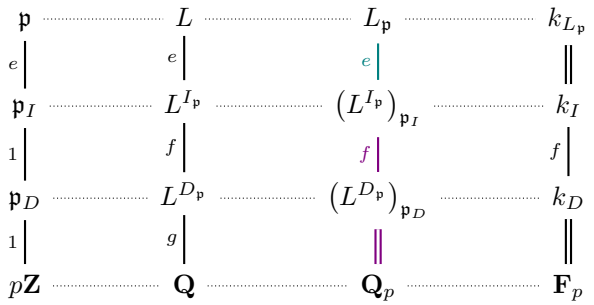


FIGURE 1. Étude locale-globale d'une extension finie et galoisienne de $\mathbf{Q}$ en un premier $\mathfrak{p}$ étendant p.

Remarque 7.6. Il est donc possible de construire une tour d'extensions telle que toute la ramification de $\mathfrak{p}$ sur p prend place au sommet et toutes les extensions de corps résiduels au milieu.

Remarque 7.7. Combinons des extensions de corps de nombres. Soit $M \supseteq L \supseteq \mathbf{Q}$ une telle tour avec $M/\mathbf{Q}$ et $L/\mathbf{Q}$ galoisiennes. Notons $G = \mathrm{Gal}(M/\mathbf{Q})$ et faisons de même avec $H = \mathrm{Gal}(M/L)$. Soient $\mathfrak{P}$ un premier de $\mathcal{O}_M$ divisant un premier $\mathfrak{p}$ de $\mathcal{O}_L$ lui-même divisant p. On peut facilement montrer que le groupe de décomposition de H en $\mathfrak{P}$ est $D_\mathfrak{P}(L) = H \cap D_\mathfrak{P}$ qui est l'image de $D_\mathfrak{P}$ dans G/H.

Exemple 7.8. Soit L/K une extension quadratique de corps de nombres. Selon la ramification, la table suivante détermine les groupes de décompositions et d'inertie de $\mathrm{Gal}(L/K)$:

Ramification	**Groupes de décomposition**	**Groupes d'inertie**
$g = 2$	deux, égaux à $\mathrm{Gal}(L/K)$	deux, égaux à $\mathrm{Gal}(L/K)$
$f = 2$	un seul, égal à $\mathrm{Gal}(L/K)$	un seul, trivial
$e = 2$	un seul, trivial	un seul, trivial

Remarque 7.9. Soit $L = \mathbf{Q}(\sqrt{d})$ avec $d \in \mathbf{Z}$ sans facteur carré, $K = \mathbf{Q}$ et p un premier impair. Rappelons que $g = 2$ si et seulement si d est un carré modulo p, que $f = 2$ si et seulement si d n'est pas un, et que $e = 2$ si et seulement si p divise le discriminant de $\mathcal{O}_L/\mathbf{Z}$.

Exemple 7.10. Prenons $L = \mathbf{Q}(\zeta_n)$ où $\zeta_n \in \mathbf{C}$ est une racine primitive n-ième de l'unité. Soit $p \in \mathbf{Z}$ un premier ne divisant pas n et soit $\mathfrak{p} \in S_p(L)$. Dès lors, p ne se ramifie pas dans $\mathcal{O}_L$ et donc $I_\mathfrak{p}$ est trivial. Par conséquent,

$$D_\mathfrak{p} \simeq \mathrm{Gal}(\mathbf{Q}_p(\zeta_n)/\mathbf{Q}_p) \simeq \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$$

où $q = p^f$ avec f l'ordre multiplicatif de p mod $n\mathbf{Z}$. Ainsi $D_\mathfrak{p}$ est cyclique, engendré par l'opérateur de Frobenius $\zeta_n \to \zeta_n^p$.

8. L'opérateur de Frobenius

Définition 8.1. Soit L un corps de nombres galoisien sur $\mathbf{Q}$ et non ramifié en un premier $p \in \mathbf{Z}$. L'opérateur de Frobenius de $\mathrm{Gal}(L/\mathbf{Q})$ en un $\mathfrak{p} \in S_p(L)$ est l'unique $\sigma_\mathfrak{p} \in D_\mathfrak{p}$ vérifiant $\sigma_\mathfrak{p}(x) \equiv x^p \bmod \mathfrak{p}$ en tout $x \in \mathcal{O}_L$.

Compte tenu du Lemme 7.2 et du fait que les indices de ramification des premiers intervenant dans une décomposition sont égaux lorsque l'extension est galoisienne, les opérateurs de Frobenius entre tels premiers sont conjugués. Nous n'allons nous intéresser qu'à des extensions abéliennes dans cette section, où donc les Frobenius sont égaux. Pour cette raison, nous abandonnons la dépendance en le premier dans nos notations.

Exemple 8.2. Avec $L = \mathbf{Q}(\zeta_n)$ et p ne divisant pas n, l'opérateur de Frobenius σ est donné par $\sigma(\zeta_n) = \zeta_n^p$.

Exemple 8.3. Soit $L = \mathbf{Q}(\sqrt{d})$ avec $d \in \mathbf{Z}$ sans facteur carré et soit $p \in \mathbf{Z}$ un premier non ramifié dans L. Identifions $\mathrm{Gal}(L/\mathbf{Q}) \simeq \{1, -1\}$. Dès lors, l'opérateur de Frobenius σ vaut 1 ou -1 selon que p se décompose ou non dans L, autrement dit selon que d est un carré ou non modulo p.

Sur base de la théorie de Galois et des exemples précédents, nous donnons une démonstration selon Milne de la loi de réciprocité quadratique.

Proposition 8.4. *Soit $p \in \mathbf{Z}$ un nombre premier impair. Alors -1 est un carré modulo p si et seulement si $p \equiv 1 \bmod 4\mathbf{Z}$. En d'autres symboles :*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Démonstration. Si $-1 \equiv x^2 \bmod p\mathbf{Z}$, alors x est d'ordre 4 et il suit du théorème de Lagrange que 4 divise $p-1$. Réciproquement, $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $p-1$, il admet un générateur a et ainsi $a^{(p-1)/2} = -1 \bmod p\mathbf{Z}$. □

Théorème 8.5. *Soient p et $q \in \mathbf{Z}$ deux premiers impairs distincts. Alors on a la relation :*

$$\left(\frac{q}{p}\right) = (-1)^{(q-1)(p-1)/4} \left(\frac{p}{q}\right).$$

Démonstration. Soit $L = \mathbf{Q}(\zeta_p)$. Comme le groupe de Galois de $L/\mathbf{Q}$ est cyclique d'ordre $p-1$, il contient un unique sous-groupe d'indice 2 et de suite L contient une unique extension quadratique F de $\mathbf{Q}$. Puisque p est l'unique premier de $\mathbf{Z}$ se ramifiant dans L, il doit se ramifier dans F sinon un autre le fera [Mil20, Theorem 4.9]. Si $p \equiv 1 \bmod 4\mathbf{Z}$, alors p est le seul premier se ramifiant dans $\mathbf{Q}(\sqrt{p})$ et ce corps est la seule extension quadratique de $\mathbf{Q}$ où cela est vrai. Sinon $-p \equiv 1 \bmod 4\mathbf{Z}$ et cette fois c'est $\mathbf{Q}(\sqrt{-p})$ que l'on considère. Ainsi, $F = \mathbf{Q}(\sqrt{d})$ avec

$$d = (-1)^{(p-1)/2} p.$$

D'un autre côté, l'opérateur de Frobenius σ pour q dans l'extension $L/\mathbf{Q}$ est donné par $\sigma(\zeta_p) = \zeta_p^q$. Toutefois, on a que σ est l'identité sur F si et seulement si q est un carré modulo p. En d'autres mots,

$$\sigma\,|_F = \left(\frac{q}{p}\right).$$

Mais notre étude des extensions quadratiques nous apprend aussi que cette restriction est

$$\left(\frac{q}{p}\right) = \left(\frac{d}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right)$$

d'où l'assertion. □

Théorème 8.6. *Soit p un premier impair. Alors 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \bmod 8\mathbf{Z}$. En d'autres symboles :*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Démonstration. Soit ζ_8 une racine primitive huitième de l'unité dans une clôture algébrique fixée de $\mathbf{F}_p$ et posons $a = \zeta_8 + \zeta_8^{-1}$. Puisque $\zeta_8^4 = -1$, nous constatons que

$$X^4 + 1 = (X^2 - \zeta_8^2)(X^2 - \zeta_8^{-2}) \in \overline{\mathbf{F}}_p[X]$$

puisque les racines des deux polynômes sont $\pm\zeta_8$ et $\pm\zeta_8^{-1}$. Par conséquent nous en déduisons que $\zeta_8^2 + \zeta_8^{-2} = 0$ et donc que $a^2 = 2$. Si on suppose $p \equiv 1 \bmod 8\mathbf{Z}$, alors $a^p = a$ et ainsi

$$1 = a^{p-1} = 2^{(p-1)/2} = \left(\frac{2}{p}\right).$$

Si maintenant on suppose $p \equiv \pm 5 \bmod 8\mathbf{Z}$, alors $a^p = -a$ et on trouve une égalité similaire, achevant la démonstration. □

Références

[AW45] Emil Artin et George Whaples – *Axiomatic characterization of fields by the product formula for valuations*, Bulletin of the American Mathematical Society **51** (1945).

[Con] Brian Conrad – *Higher ramification groups*, Math **248A**, disponible sur `http://virtualmath1.stanford.edu/~conrad/248APage/handouts/ramgroup.pdf`.

[De22a] Martin Debaisieux – *Théorie algébrique des nombres*, Projet de Master, Université de Mons, disponible sur `https://martindbx.github.io/notes/ant.pdf` (2022).

[De22b] ——— – *Initiation analytique aux corps ultramétriques*, Projet de Master, Université de Mons, disponible sur `https://martindbx.github.io/notes/ultrametric-fields.pdf` (2022).

[Gou20] Fernando Gouvêa – *p-adic Numbers*, An introduction, Universitext, Third edition, Springer (2020).

[Mar77] Daniel Marcus – *Number Fields*, Graduate Texts in Mathematics **50**, Springer (1977).

[Mil] Alison Miller – *Algebraic Number Theory* (notes), Math **223A**, disponible sur `http://www-personal.umich.edu/~alimil/223anotes.pdf`.

[Mil20] James Milne – *Algebraic Number Theory* (v3.08), disponible sur `https://www.jmilne.org/math/CourseNotes/ANT.pdf` (2020).

[Neu99] Jürgen Neukirch – *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften **322**, Springer (1999).

[Ser79] Jean-Pierre Serre – *Local fields*, Graduate Texts in Mathematics **67**, Springer (1979).

[Sha] Romyar Sharifi – *Algebraic Number Theory*, disponible sur `https://www.math.ucla.edu/~sharifi/algnum.pdfhttps://www.math.ucla.edu/~sharifi/algnum.pdf`.

[You] Alex Youcis – *Galois groups of local and global fields*, disponible sur `https://alex-youcis.github.io/localglobalgalois.pdf`.

Email address: `martin.debaisieux@umons.ac.be`

Department of Mathematics, University of Mons
15 Avenue Victor Maistriau, De Vinci building
Mons B-7000