Une étude locale de la ramification dans les extensions de corps de nombres

Martin Debaisieux

Dernière compilation le 5 novembre 2024

Nous abordons 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 l'insérer dans le cas global. On applique ces outils afin de démontrer la loi de réciprocité quadratique.

Table des matières

Des extensions de corps p-adiques **1**
1.1 Décomposition du degré de l'extension 1
1.2 Extensions non ramifiées 3
1.3 Extensions totalement ramifiées 4
1.4 Extensions modérément ramifiées 5
1.5 Groupes de ramification 7
Vers les extensions de corps de nombres **8**
2.1 Extensions de valeurs absolues et places 8
2.2 Groupes de décomposition 10
2.3 L'opérateur de Frobenius 12

❖ Des extensions de corps p-adiques

Dans ce premier chapitre, p est un nombre premier fixé et K est un corps p-adique (une extension finie de $\mathbf{Q}_p$) pris dans une clôture algébrique fixée. Si $L/\mathbf{Q}_p$ est finie, nous notons v_L sa valuation normalisée sur L et $\mathcal{O}_L$ l'anneau de ses entiers, d'idéal maximal $\mathfrak{m}_L$ dont une uniformisante est π_L.

1.1 Décomposition du degré de l'extension

Étant donné une extension finie L/K, on a que $\mathfrak{m}_K\mathcal{O}_L = \mathfrak{m}_L^e$ pour un certain entier $e \geqslant 1$ appelé indice de ramification de L/K. Si l'on note 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 résiduel de L/K et l'on a :

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

car il n'y a qu'un seul premier dans L. Cette identité fondamentale est bien connue et fait déjà l'objet d'une section d'un précédent document [De22a, §2.6].

Proposition 1.1. Soit $M \supseteq L \supseteq K$ une tour d'extensions finies, 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 résiduels découle simplement de celle des extensions de corps ; celle 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 est non 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 $K = \mathbf{Q}_p$ qui est (simplement) ramifiée.

Pour nous constituer une liste d'exemples, nous terminons cette section par l'analyse du cas très important des extensions cyclotomiques de $\mathbf{Q}_p$. Pour tout $n \geqslant 1$, nous notons par ζ_n une racine primitive n-ième de l'unité. Selon la divisibilité de n par p, la nature de l'extension cyclotomique qu'elle engendre diffère. On y résume ici une partie des informations dont on se souviendra.

	Ramification	**Degré**	**Groupe de Galois**
$p \nmid n$	non ramifiée	ordre 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

Table 1 – Récapitulatif sur la ramification des extensions cyclotomiques de $\mathbf{Q}_p$.

Considérons dans un premier temps le cas où p ne divise pas n et travaillons sur K, où l'on note le corps résiduel $\mathbf{F}_q := k$ avec q une puissance de p.

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

Démonstration. Soit Φ_n le polynôme minimal de ζ_n sur K. Sa réduction modulo π_K est celui de ζ_n mod $\mathfrak{m}_K$ sur k. En effet, $\Phi_n(X)$ mod $\pi_K K[X]$ 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 $k[X]$. Puisque Φ_n et sa réduction sont de même degré, on a

$$[L : K] = [k(\zeta_n \bmod \mathfrak{m}_K) : k] = [k_L : k].$$

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

Considérons désormais le cas où $n = p^m$ est une puissance $m \geqslant 1$ de p et revenons à la situation où $K = \mathbf{Q}_p$.

Proposition 1.5. Soit $L = \mathbf{Q}_p(\zeta_n)$ avec $n = p^m$, alors $L/\mathbf{Q}_p$ 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. Soit $P(X) = \Phi_p\left(X^{p^{m-1}}\right)$ avec $\Phi_p(X) := (X^p - 1)/(X - 1)$, alors on vérifie aisément que P est le polynôme minimal de ζ_n sur $\mathbf{Q}_p$ et donc 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 dès lors bijective. D'un autre côté, on a $\mathrm{Nm}_{L/\mathbf{Q}_p}(1 - \zeta_n) = P(1) = p$, ainsi on trouve que $\varphi(p^m)v_p(1 - \zeta_n) = v_p(p) = 1$ et donc que l'extension en question est totalement ramifiée. □

Nota bene 1.6. Lorsque $n = p^m r$ est divisible par p mais n'en est pas une puissance (autrement dit $m = v_p(n) \geqslant 1$ et $r \neq 1$), on peut décomposer $\mathbf{Q}_p(\zeta_n)$ en deux parties non triviales via

$$\zeta_r := \zeta_n^{p^m} \in \mu_r \quad \text{et} \quad \zeta_{p^m} := \zeta_n^r \in \mu_{p^m}$$

de sorte que $\mathbf{Q}_p(\zeta_n) = \mathbf{Q}_p(\zeta_r, \zeta_{p^m})$ est le compositum d'une extension non ramifiée par une extension totalement ramifiée de $\mathbf{Q}_p$. Dans ce cas, ζ_n engendre une extension (simplement) ramifiée de $\mathbf{Q}_p$ de degré résiduel l'ordre multiplicatif de p mod $r\mathbf{Z}$ et d'indice de ramification $\varphi(p^m)$.

1.2 Extensions non ramifiées

Nous nous concentrons maintenant sur le cas 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 chaque $n \geqslant 1$, engendrée par une racine primitive $(p^n - 1)$-ième de l'unité. Il s'agit en réalité de sa seule extension non ramifiée de degré n. L'étude non ramifiée est bien connue.

Théorème 1.7. Les extension non ramifiées de K sont en bijection avec les extensions de son corps résiduel k via l'association $L \rightsquigarrow k_L := \mathcal{O}_L/\mathfrak{m}_L$.

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. Pour cela, nous montrons que le foncteur donné est pleinement fidèle et essentiellement surjectif.

(A) Nous commençons par montrer qu'étant donné L/K non ramifiée et M/K finie, 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. Cette application est bien définie car les morphismes préservent les valuations. Pour montrer la bijectivité, on se donne a un élément primitif de k_L/k et P_a son polynôme minimal sur k. Soit $P \in \mathcal{O}_K[X]$ un relèvement monique de P_a et soit $\alpha \in \mathcal{O}_L$ l'unique racine de P se relevant de a par le lemme de Hensel. Puisque L/K n'est pas ramifiée,

$$[L : K] = [k_L : k] = \deg(P) = \deg(P_a).$$

Mais P doit être irréductible dans $K[X]$ et donc $L = K(\alpha)$. De cela, on obtient le diagramme commutatif suivant :

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

L'application de droite étant bijective par le lemme de Hensel, nous déduisons ce que nous avons annoncé.

(B) Nous montrons finalement que pour toute extension finie F/k, il existe une unique extension non ramifiée L/K telle que $F = k_L$. Pour cela, nous nous donnons un élément primitif de F/k et, avec les notations de (A), nous construisons $L := K(\alpha)$. Comme k_L comprend une racine de P_a, on a $F \subseteq k_L$. Un argument de degré donne l'égalité. L'unicité de L est évidente en appliquant (A). □

Corollaire 1.8. Les extensions non ramifiées L de K sont galoisiennes, de groupe de Galois canoniquement isomorphe à $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_L/k)$.

Exemple 1.9. Le corps $\mathbf{Q}_p$ admet une unique extension non ramifiée de degré n pour tout $n \geqslant 1$, engendrée par une racine primitive $(p^n - 1)$-ième de l'unité et de corps résiduel $\mathbf{F}_{p^n}$. Cette extension est galoisienne.

Proposition 1.10. La classe des extensions non ramifiées de K est distinguée.

Démonstration. Nous montrons seulement que si L/K est non ramifiée et si M/K est finie, alors LM/M est non ramifiée. Le reste est laissé en exercice. En reprenant les notations de la démonstration du Théorème 1.7, on a $LM = M(\alpha)$. Considérons Q_a le polynôme minimal de a sur k_M, par le lemme de Hensel on a $P = QH$ où Q est un relèvement monique de Q_a. On en déduit que Q est le polynôme minimal de α sur M et donc

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

Cela, combiné à la multiplicativité des degrés résiduels, implique que le compositum d'extensions non ramifiées est une extension non ramifiée. □

Définition 1.11. Le compositum des extensions non ramifiées de K est une extension non ramifiée K^{nr} de K, appelée extension maximale non ramifiée de K. Si L est une extension de K, l'extension maximale non ramifiée de K dans L est $L_0 = L \cap K^{\mathrm{nr}}$.

Puisque nous travaillons avec des corps p-adiques, le corps résiduel de K^{nr} n'est autre que la clôture algébrique de $\mathbf{F}_p$ déterminée par notre choix de clôture algébrique de $\mathbf{Q}_p$. Le corps résiduel de L_0 est celui de L.

Exemple 1.12. L'extension maximale non ramifiée de $\mathbf{Q}_p$ est obtenue en adjoignant une racine primitive $(p^n - 1)$-ième de l'unité pour tout $n \geqslant 1$. Comme $\mathbf{F}_{p^n}/\mathbf{F}_p$ est une extension cyclique de degré n, on a

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

Remarque 1.13. Le corps $\mathbf{Q}_p^{\mathrm{nr}}$ n'est pas p-adiquement complet. La preuve proposée dans [Gou20, Theorem 6.8.4] construit une suite de Cauchy dans $\mathbf{Q}_p^{\mathrm{nr}}$ qui ne converge pas dans la clôture algébrique de $\mathbf{Q}_p$. Cette même démonstration montre que cette dernière n'est pas complète, justifiant la construction de $\mathbf{C}_p$.

1.3 Extensions totalement ramifiées

Nous explorons désormais le cas des extensions totalement ramifiées d'un corps p-adique. Ces extensions sont moins maniables que les non ramifiées et leur classe n'est pas distinguée. L'objet principal de cette section est de montrer comment l'on peut construire de telles extensions.

Théorème 1.14. Une extension finie L/K est totalement ramifiée si et seulement si $L = K(\alpha)$ où $\alpha \in L$ est racine d'un polynôme d'Eisenstein sur K.

Démonstration. Si L est engendré sur K par une racine $\alpha \in L$ d'un polynôme d'Eisenstein sur K, alors $v_K(\alpha) = 1/n$ et ainsi $e = n$. Réciproquement, si $\alpha \in L$ est tel que $v_K(\alpha) = 1/n$, alors les $1, \alpha, \ldots, \alpha^{n-1}$ représentent des classes distinctes de $v_K(K^\times)$ dans $v_K(L^\times)$ et il est donc impossible d'obtenir une relation non triviale

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$$

pour des $b_i \in K$ non tous nuls. Nous en déduisons que α est un élément primitif de L/K. On peut donc exprimer α^n selon les autres, et cela donne lieu à un polynôme d'Eisenstein sur K par le principe [Mil20, 7.11]. □

Remarque 1.15. La démonstration précédente montre que π_L peut être choisi comme élément primitif de L/K. Ainsi, tout élément $x \in L$ s'écrit de manière unique sous la forme

$$x = b_0 + b_1\pi_L + \cdots + b_{n-1}\pi_L^{n-1}$$

avec les $b_i \in K$. Par conséquent, x est entier si et seulement si on a $v_K(b_i) \geqslant 0$ pour tout $i \in \{0, \ldots, n-1\}$, ou encore si et seulement si $x \in O_K[\pi_L]$. Par suite, il est aussi vrai de dire que $O_L = O_K[\pi_L]$.

Exemple 1.16. On peut construire une extension totalement ramifiée de K de degré n pour chaque $n \geqslant 1$ en lui adjoignant une racine du polynôme d'Eisenstein $X^n - \pi_K$. Cette extension de degré n n'est en général pas la seule à être totalement ramifiée.

Exemple 1.17. Soit p impair et soit $n \in \mathbf{Z}$ un entier n'étant pas un résidu quadratique modulo $p\mathbf{Z}$. Le corps $L = \mathbf{Q}_p(\sqrt{p}, \sqrt{np})$ est alors le compositum de deux extensions totalement ramifiées de $\mathbf{Q}_p$ et pourtant il comprend l'élément $\sqrt{n}$ donnant lieu à une extension non ramifiée de $\mathbf{Q}_p$. Par conséquent, $L/\mathbf{Q}_p$ est (simplement) ramifiée et *a fortiori* la classe des extensions totalement ramifiées d'un corps p-adique n'est pas distinguée.

Exemple 1.18. Pour tout $n \geqslant 1$, 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 inductive sur ces extensions, on définit le corps $\mathbf{Q}_p(\zeta_{p^\infty})$ qui est une extension totalement ramifiée de $\mathbf{Q}_p$ telle que

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

Le théorème de Kronecker-Weber (dans sa version locale) nous apprend que l'extension abélienne maximale de $\mathbf{Q}_p$ est engendrée par les racines de l'unité. Celle-ci est dès lors le compositum de $\mathbf{Q}_p^{\mathrm{nr}}$ par $\mathbf{Q}_p(\zeta_{p^\infty})$. Ces extensions de $\mathbf{Q}_p$ étant linéairement disjointes, on a

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

Exercice 1.19. Pour $L \in \{\mathbf{Q}_3(\zeta_{12}), \mathbf{Q}_3(\zeta_3, \sqrt[3]{2})\}$, déterminer le treillis complet de $L/\mathbf{Q}_3$, l'indice de ramification de chaque sous-extension et leur degré résiduel. Même question en remplaçant $\mathbf{Q}_3$ par $\mathbf{Q}_2$.

Proposition 1.20. À isomorphisme près, il n'existe qu'un nombre fini d'extensions totalement ramifiées de K d'un degré fixé.

Démonstration. Soit $n \geqslant 2$ un degré fixé. Nous montrons qu'il ne peut y avoir qu'un nombre fini d'extensions totalement ramifiées de K de degré au plus n. Chaque point $(b_1, \ldots, b_{n-1}, b_n) \in \mathfrak{m}_K \times \cdots \times \mathfrak{m}_K \times \pi_K O_K^\times$ définit un polynôme d'Eisenstein de degré n et par suite un ensemble fini d'extensions totalement ramifiées de K de degré n. Selon le lemme de Krasner [Mil20, Proposition 7.63], chaque point de ce 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. □

1.4 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 1.21. Une extension de corps p-adiques L/K est modérément ramifiée si p ne divise pas $e_{L/K}$, est sauvage sinon.

Exemple 1.22. Les extensions de K engendrées par une racine de $X^n - \pi_K$ avec $n \geqslant 2$ sont des extensions totalement ramifiées. Elles sont modérées pour p ne divisant pas n et sauvages sinon.

Exemple 1.23. L'extension engendrée par une racine primitive n-ième de l'unité sur $\mathbf{Q}_p$ est d'indice de ramification $\varphi(p^m)$ où $m := v_p(n)$. Ainsi, celle-ci est modérément ramifiée si $m \in \{0, 1\}$ et est sauvage sinon.

Les extensions non ramifiées sont automatiquement modérées, dès lors une extension L/K est modérément ramifiée si et seulement si la sous-extension L/L_0 l'est, ou encore si et seulement si $LK^{\mathrm{nr}}/K^{\mathrm{nr}}$ l'est. Pour que cette dernière expression ait un sens, il nous faut faire une légère entorse à notre contexte car K^{nr} n'est pas un corps p-adique. Seulement, il est hensélien et cela est suffisant pour étendre les principes et notions que nous avons définis.

Théorème 1.24. Si L/K^{nr} est une extension modérément ramifiée de degré fini $n \geqslant 2$, alors $L = K^{\mathrm{nr}}(\sqrt[n]{\pi_K})$.

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

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

pour une unité $u \in K(\alpha)$. Il nous suffit de montrer que u est une puissance n-ième dans une extension non ramifiée F/K pour en déduire l'assertion. La réduction de $X^n - u$ modulo $\pi_{K(\alpha)}$ 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 $X^n - u \in O_F[X]$ on trouve une racine n-ième de u dans $F \subseteq L$. □

Proposition 1.25. La classe des extensions modérément ramifiées de K est distinguée.

Démonstration. Ce résultat est une conséquence simple du Théorème 1.24, on laisse le soin aux lecteurs de le démontrer. □

Définition 1.26. Le compositum des extensions modérément ramifiées de K est une extension modérée K^{mr} de K, appelée extension maximale modérément ramifiée de K. Si L est une extension de K, l'extension maximale modérément ramifiée dans L est $L_1 = L \cap K^{\mathrm{mr}}$.

Les extensions maximales modérément ramifiées contiennent par construction les extensions maximales non ramifiées. Comme nous travaillons avec des corps p-adiques, le corps résiduel de K^{mr} n'est autre que la clôture algébrique de $\mathbf{F}_p$. Celui de L_1 est celui de L.

Exemple 1.27. Déterminer le groupe de Galois absolu de $\mathbf{Q}_p$ est une question difficile. Pour l'instant, on connaît seulement jusqu'à la partie maximale modérée $\mathbf{Q}_p^{\mathrm{mr}}$. Nous l'obtenons en adjoignant à $\mathbf{Q}_p^{\mathrm{nr}}$ les racines n-ièmes de p pour tout $n \geqslant 2$ non divisible par p. En chaque étape on ajoute une extension cyclique de $\mathbf{Q}_p^{\mathrm{nr}}$ et donc on se retrouve avec

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

Exercice 1.28. En reprenant les quatre treillis de l'Exercice 1.19, déterminer la nature modérée ou sauvage de chaque sous-extension.

1.5 Groupes de ramification

Nous terminons ce chapitre en donnant une décomposition du groupe de Galois d'une extension galoisienne de K, par exemple non ramifiée, sur laquelle on peut lire la ramification. Cette décomposition se fait via une filtration par des sous-groupes galoisiens.

Définition 1.29. Soit L/K une extension galoisienne, le n-ième groupe de ramification de $G := \mathrm{Gal}(L/K)$ est $G_n := \{g \in G \mid \forall \alpha \in \mathcal{O}_L,\ g.\alpha \equiv \alpha \bmod \mathfrak{m}_L^{n+1}\}$ pour tout $n \geqslant -1$ entier. Les groupes G_0, G_1 et les autres sont respectivement appelés groupe d'inertie, groupe de ramification et groupes de ramification supérieurs de L/K.

On vérifie simplement que les G_n sont des sous-groupes normaux de G et qu'ils sont triviaux à partir d'un certain rang. En somme, nous avons une filtration exhaustive décroissante de G par des sous-groupes normaux :

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

Nous montrerons que G est résoluble. Ce résultat met en lumière une contrainte très forte quant aux groupes de Galois d'extensions p-adiques : par exemple, A_5 ne peut pas être le groupe de Galois d'une telle extension.

Lemme 1.30. Pour tout $n \geqslant 1$ entier, on a $G_n = \{g \in G \mid g.\pi_L \equiv \pi_L \bmod \mathfrak{m}_L^{n+1}\}$.

Démonstration. Soit A l'anneau des entiers de L_0. Nous savons de la Remarque 1.15 que $\mathcal{O}_L = A[\pi_L]$ et par conséquent il suffit de vérifier la condition $g.\alpha \equiv \alpha \bmod \mathfrak{m}_L^{n+1}$ seulement en $\alpha = \pi_L$. □

Proposition 1.31. On véhicule les notations de la Définition 1.29.

(1) Le sous-corps de L fixe par G_0 est L_0, avec $G/G_0 \simeq \mathrm{Gal}(L_0/K) \simeq \mathrm{Gal}(k_L/k)$.

(2) L'application $G_0 \to k_L^\times : g \mapsto g.\pi_L/\pi_L \bmod \mathfrak{m}_L$ est un morphisme de groupes dont le noyau est G_1.

(3) Pour tout $n \geqslant 1$ entier, l'application $G_n \to k_L : g \mapsto (g.\pi_L - \pi_L)/\pi_L^{n+1} \bmod \mathfrak{m}_L$ est un morphisme de groupes dont le noyau est G_{n+1}.

(4) Le groupe G_1 est l'unique p-Sylow de G_0. Le sous-corps de L fixe par G_1 est L_1, avec $G/G_1 \simeq \mathrm{Gal}(L_1/K)$.

Démonstration.

(1) L'application naturelle $\mathrm{Gal}(L_0/K) \to \mathrm{Gal}(k_L/k)$ est un isomorphisme et G_0 est le noyau de $G \to \mathrm{Gal}(k_L/k)$ qui est surjectif.

(2) On montre facilement que cette application est bien définie, indépendante du choix de l'uniformisante et est un morphisme par définition de G_0. L'inertie est son noyau car $g.\pi_L/\pi_L \equiv 1 \bmod \mathfrak{m}_L$ si et seulement si $g.\pi_L \equiv \pi_L \bmod \mathfrak{m}_L^2$, ou encore si et seulement si $g \in G_1$ par le Lemme 1.30.

(3) Ces applications sont bien définies. Pour montrer qu'il s'agit de morphismes, il suffit de vérifier que $g.(h.\pi_L - \pi_L) \equiv h.\pi_L - \pi_L \bmod \mathfrak{m}_L^{n+2}$ pour tous $g, h \in G_n$. Bien sûr, si π_L est fixe par h cela est évident. Sinon, on a $h.\pi_L = u\pi_L$ avec $u \neq 1$ une unité de L et la congruence précédente devient

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

ce qui est vrai puisque $g \in G_0$. La détermination du noyau s'effectue comme avant, en utilisant le Lemme 1.30.

(4) Les quotients successifs G_n/G_{n+1} se plongent dans k_L à partir de $n \geqslant 1$ par (3) et sont donc des p-groupes. En particulier G_1 l'est aussi. Il s'agit d'un p-Sylow de G_0 car G_0/G_1 se plonge dans $k_L^\times$ par (2). L'unicité vient de la normalité. Le reste de l'assertion s'ensuit. □

Théorème 1.32. Le groupe de Galois de L/K est résoluble.

Démonstration. Le point (1) de la Proposition 1.31 nous apprend que le quotient G/G_0 est cyclique, et est donc abélien. Les points (2) et (3) nous apprennent que les autres quotients successifs sont abéliens. □

Nous déduisons des points (1) et (4) de la Proposition 1.31 une reformulation des différents types de ramification croisés dans ce document en termes de groupes de ramification.

Proposition 1.33. L'extension L/K est non ramifiée si et seulement si $G_0 = 1$, elle est totalement ramifiée si et seulement si $G_0 = G$, et elle est modérément ramifiée si et seulement si $G_1 = 1$.

Exemple 1.34. Travaillons sur $K = \mathbf{Q}_p$ et soit $K_m := \mathbf{Q}_p(\zeta_{p^m})$ pour tout entier $n \geqslant 1$. Les groupes de ramification de $G := \mathrm{Gal}(K_m/K)$ sont :

$$G_n = \begin{cases} G & \text{si } n \in \{-1, 0\}, \\ \mathrm{Gal}(K_m/K_s) & \text{si } n \in \{p^{s-1}, \dots, p^s - 1\} \text{ avec } 1 \leqslant s < m, \\ 1 & \text{si } n \geqslant p^{m-1} \end{cases}$$

Soit $\varepsilon = (\zeta_p, \dots, \zeta_{p^2}, \dots) \in \mathbf{Z}_p(1)$ une suite cohérente de racines primitives de l'unité. Étant donné $g \in G$ non trivial, on pose $a \in \mathbf{Z}$ tel que $g.\zeta_{p^n} = \zeta_{p^n}^a$. Soient $s := v_p(a-1)$ et $c := (a-1)/p^s$, alors $g.\zeta_{p^n} - \zeta_{p^n} = \zeta_{p^n}(\zeta_{p^{n-s}}^c - 1)$. Comme le deuxième facteur est une uniformisante pour K_{n-s}, on en déduit que le tout est de valuation p-adique le degré $[K_n : K_{n-s}] = p^s$. Par le Lemme 1.30, on a $g \in G_{p^s-1}$ et $g \notin G_{p^s}$. D'un autre côté p^s est la plus grande puissance de p divisant $a-1$, signifiant que $g \in \mathrm{Gal}(K_n/K_s)$ et que $g \notin \mathrm{Gal}(K_n/K_{s+1})$.

❖ Vers les extensions de corps de nombres

Nous basculons désormais vers les corps de nombres (les extensions finies de $\mathbf{Q}$). On fixe K un tel corps, que l'on munit d'une valeur absolue $|*|$. Le complété de cette paire est noté $\widehat{K}$.

2.1 Extensions de valeurs absolues et places

Théorème 2.1. Soit $L = K(\alpha)$ une extension finie de K. Les extensions de $|*|$ à L sont en correspondance avec les facteurs moniques irréductibles du polynôme minimal de α sur K dans $\widehat{K}[X]$.

Démonstration. Soit P le polynôme minimal de α sur K. Si l'on se donne une extension de $|*|$ à L, on peut compléter L et l'on a $\widehat{L} = \widehat{K}(\alpha)$. Soit Q le polynôme minimal de α sur $\widehat{K}$, alors Q divise P dans $\widehat{K}[X]$. Nous obtenons donc, pour chaque extension de $|*|$ à L, 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 $\widehat{K}(x) = \widehat{K}[X]/(Q(X))$ 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 deux opérations sont inverses l'une de l'autre. □

Nous venons de caractériser les extensions de $|*|$. Noter que nous retrouvons le résultat bien connu (présent dans la démonstration) sur l'unicité de l'extension de la valeur absolue sur un corps valué complet.

Corollaire 2.2. Soit L/K finie et soient $L_1, \dots, L_g$ les complétions de L selon les g différentes valeurs absolues étendant $|*|$. Alors :

(1) $L \otimes_K \widehat{K} \simeq L_1 \cdots L_g$.

(2) $\mathrm{Nm}_{L/K} = \prod_{i=1}^{g} \mathrm{Nm}_{L_i/\widehat{K}}$ et $\mathrm{Tr}_{L/K} = \sum_{i=1}^{g} \mathrm{Tr}_{L_i/\widehat{K}}$.

Démonstration. Soit α un élément primitif de L/K de polynôme minimal P. On en a en particulier que $L = K(\alpha) = K[X]/(P(X))$. Soit $P = P_1 \cdots P_g$ la décomposition en facteurs moniques irréductibles dans $\widehat{K}[X]$. D'après le théorème des restes chinois, 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 point (1) découle du Théorème 2.1. Pour (2), on se rappelle que 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 par $\widehat{K}$. On voit aisément que la norme dans le produit (1) se décompose en un produit. Il en va de même pour la trace. □

Remarque 2.3. Supposons que L/K est une extension de corps de nombres telle que les anneaux d'entiers sont $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. 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 nous apprend que P_i est une puissance $e_i \geqslant 1$ d'un polynôme irréductible $Q_i \in \mathcal{O}_L[X]$. Par [Mil20, Theorem 3.41] 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 2.4. Une place d'un corps de nombres L est une classe d'équivalence de valeurs absolues non triviales sur L. L'ensemble des places sur L est noté $S(L)$.

Exemple 2.5. Les places sur $\mathbf{Q}$ sont les premiers naturels et ce que l'on note par ∞, donnant respectivement lieu aux valeurs absolues p-adiques et à la valeur absolue archimédienne (= l'usuelle).

Soit L/K une extension finie. Compte tenu de la première partie de cette section, nous disons qu'une place w de L divise une place v de K si les valeurs absolues de w étendent celles de v. Nous allons généraliser la formule du produit (voir par exemple [De22b]). Nous rappelons qu'une valeur absolue est normalisée s'il s'agit de la valeur absolue archimédienne sur $\mathbf{R}$, du carré [1] de l'usuelle sur $\mathbf{C}$ ou de $(\mathcal{O}_K : \mathfrak{p})^{-v_\mathfrak{p}(*)}$ si elle est définie en un premier $\mathfrak{p}$.

Lemme 2.6. Soit L/K finie. Pour tout $v \in S(K)$, on a $\prod_{w|v} |*|_w = |\mathrm{Nm}_{L/K}(*)|_v$ où les valeurs absolues sont normalisées.

Démonstration. Découle du point (2) du Corollaire 2.2 et de l'extension des valeurs absolues sur les corps complets. □

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.

Théorème 2.7 (Formule du produit généralisée)**.** En choisissant les valeurs absolues normalisées, 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 $\mathbf{Q}$ vie le Lemme 2.6 et l'on a

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

Remarque 2.8. Artin et Whaples ont donné une caractérisation des corps globaux dans [AW45] dans le language des places. Soit L un corps de nombres muni d'un ensemble S de places satisfaisant les points :

(A1) Il existe un ensemble de représentants v des places tel que pour tout $x \in L^\times$ 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 le complété L_v est un corps local.

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

2.2 Groupes de décomposition

Étudier le groupe de Galois d'une extension de $\mathbf{Q}$ peut se révéler être une tâche ardue ; on pense notamment à son groupe de Galois absolu ! La multitude de premiers et *a fortiori* la ramification n'arrange en rien cette étude. Pour faciliter cela, on peut décomposer le groupe en chaque premier, permettant après complétion de travailler localement.

Définition 2.9. Soit $L/\mathbf{Q}$ une extension finie galoisienne et soit p un nombre premier fixé. Le groupe de décomposition de $\mathrm{Gal}(L/\mathbf{Q})$ en un premier $\mathfrak{p}$ de $\mathcal{O}_L$ étendant p est le stabilisateur $D_\mathfrak{p} := \{g \in \mathrm{Gal}(L/\mathbf{Q}) \mid g.\mathfrak{p} = \mathfrak{p}\}$.

Afin de garder la définition concise, nous n'avons pas discuté de la nature de cet objet. Le groupe $\mathrm{Gal}(L/\mathbf{Q})$ agit sur le spectre de $\mathcal{O}_L$ et cette action devient 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. On laisse les lecteurs généraliser ces notions de $\mathbf{Q}$ à K (adapter les notations).

Lemme 2.10. Soient L et $\mathfrak{p}$ comme en 2.9. Si $\mathfrak{q} \in S_p(L)$ est un autre premier, alors $D_\mathfrak{q}$ et $D_\mathfrak{p}$ sont conjugués via n'importe quel automorphisme de L envoyant $\mathfrak{q}$ sur $\mathfrak{p}$.

L'action de $\mathrm{Gal}(L/\mathbf{Q})$ 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 $g := (\mathrm{Gal}(L/\mathbf{Q}) : D_\mathfrak{p})$ par le théorème de l'orbite-stabilisateur, nous obtenons le résultat suivant :

Théorème 2.11. Soient L et $\mathfrak{p}$ comme en 2.9. 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 $g \in D_\mathfrak{p}$ s'étend par continuité de façon univoque en un automorphisme $\mathbf{Q}_p$-linéaire de $L_\mathfrak{p}$ et donc $|D_\mathfrak{p}| \leq [L_\mathfrak{p} : \mathbf{Q}_p]$. Toutefois, nous savons du Lemme 2.10 que $|D_\mathfrak{p}| = |D_{g.\mathfrak{p}}|$ pour tout $g \in \mathrm{Gal}(L/\mathbf{Q})$. Dès lors,

$$|\mathrm{Gal}(L/\mathbf{Q})| = (\mathrm{Gal}(L/\mathbf{Q}) : D_\mathfrak{p})|D_\mathfrak{p}| \leqslant \sum_{g\in G/D_\mathfrak{p}} [L_{g.\mathfrak{p}} : \mathbf{Q}_p] = [L : \mathbf{Q}]$$

où la dernière égalité provient du Corollaire 2.2. Nous en déduisons finalement que $|D_\mathfrak{p}| = [L_\mathfrak{p} : \mathbf{Q}_p] = |\mathrm{Gal}(L_\mathfrak{p}/\mathbf{Q}_p|$ et donc l'assertion. $\square$

Définition 2.12. Soient L et $\mathfrak{p}$ comme en 2.9. Le groupe d'inertie $I_\mathfrak{p}$ de $\mathrm{Gal}(L/\mathbf{Q})$ en $\mathfrak{p}$ est le noyau du morphisme $D_\mathfrak{p} \to \mathrm{Gal}(k_{L_\mathfrak{p}}/\mathbf{F}_p)$ résultant du Théorème 2.11.

La flèche précédente est surjective, on 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 2.13. Soient L et $\mathfrak{p}$ comme en 2.9. Les indices de ramification et les degrés résiduels 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 $(\mathrm{Gal}(L/\mathbf{Q}) : D_\mathfrak{p})$ et cette quantité vaut g. Au vu des contraintes sur les indices et degrés, on en déduit les annotations de l'étage inférieur de chaque tour. À nouveau, la théorie de Galois nous apprend que $|D_\mathfrak{p}| = ef$ et donc la suite exacte donne $|I_\mathfrak{p}| = e$. Les autres étages s'ensuivent. □

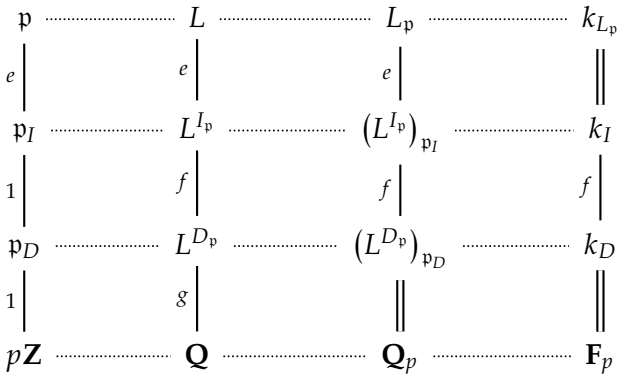

Figure 1 – Étude locale-globale d'une extension finie galoisienne de $\mathbf{Q}$ en un premier $\mathfrak{p}$ étendant p.

Remarque 2.14. Il est ainsi possible de construire une tour d'extensions telle que la ramification de $\mathfrak{p}$ sur p prend place en son sommet, et toutes les extensions de corps résiduels en son milieu.

Exercice 2.15. Nous combinons des extensions de corps de nombres. Soit $M \supseteq L \supseteq \mathbf{Q}$ une telle tour avec $M/\mathbf{Q}$ et $L/\mathbf{Q}$ galoisiens. Posons $G := \mathrm{Gal}(M/\mathbf{Q})$ et $H := \mathrm{Gal}(M/L)$. Soient $\mathfrak{P}$ un premier de O_M divisant un premier $\mathfrak{p}$ de O_L, divisant p. Montrer que le groupe de décomposition de H en $\mathfrak{P}$ est $D_\mathfrak{P}(L) = H \cap D_\mathfrak{P}$. Il s'agit de l'image de $D_\mathfrak{P}$ dans G/H.

Exemple 2.16. Soit L/K une extension quadratique. Selon le type de ramification, la table suivante détermine les groupes de décomposition 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

Table 2 – Groupes de décomposition et d'inertie d'une extension quadratique.

Exemple 2.17. Soit $L = \mathbf{Q}(\zeta_n)$ où $\zeta_n \in \mathbf{C}$ est une racine primitive n-ième de l'unité. Soient $p \in \mathbf{Z}$ un premier ne divisant pas n et $\mathfrak{p} \in S_p(L)$. Dès lors, p ne se ramifie pas dans 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 absolu $\zeta_n \mapsto \zeta_n^p$.

2.3 L'opérateur de Frobenius

Définition 2.18. Soit $L/\mathbf{Q}$ une extension finie galoisienne non ramifiée en un nombre premier p. 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 $x \in O_L$.

Compte tenu de l'égalité des indices de ramification des premiers d'une factorisation dans une extension galoisienne et du Lemme 2.10, les opérateurs de Frobenius entre tels premiers sont conjugués. Nous allons nous intéresser à des extensions abéliennes dans cette section, où donc les Frobenius sont égaux. Pour cette raison, nous abandonnons la dépendance en le premier.

Exemple 2.19. 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 2.20. Soit $L = \mathbf{Q}(\sqrt{d})$ avec $d \in \mathbf{Z}$ sans facteur carré et soit p un nombre premier non ramifié dans L. Identifions $\mathrm{Gal}(L/\mathbf{Q}) \simeq \{1, -1\}$. Dès lors, l'opérateur de Frobenius vaut 1 ou -1 selon que p se décompose ou non dans L, autrement dit selon que d est un carré ou non modulo $p\mathbf{Z}$.

Sur base de la théorie de Galois et des exemples précédents, nous donnons une démonstration selon [Mil20] de la loi de réciprocité quadratique.

Proposition 2.21. 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 découle du théorème de Lagrange que 4 divise $p-1$. Réciproquement, le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $p-1$, il admet un générateur a et ainsi $a^{(p-1)/2} = -1 \bmod p\mathbf{Z}$. □

Théorème 2.22. Soient p et $q \in \mathbf{Z}$ deux nombres premiers impairs distincts. On a la relation :

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

Démonstration. Soit $L = \mathbf{Q}(\zeta_p)$. Le groupe de Galois de $L/\mathbf{Q}$ est cyclique d'ordre $p-1$, il contient donc un unique sous-groupe d'indice 2 et de suite L contient une unique sous-extension quadratique $F/\mathbf{Q}$. Puisque p est l'unique premier de $\mathbf{Z}$ se ramifiant dans L, il doit se ramifier aussi dans F sinon un autre le fera [Mil20, Theorem 4.9]. Si $p \equiv 1 \bmod 4\mathbf{Z}$, alors p est le seul se ramifiant dans $\mathbf{Q}(\sqrt{p})$ et ce corps est l'unique 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 $L/\mathbf{Q}$ 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 $p\mathbf{Z}$. 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 2.23. 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 prise dans une clôture algébrique de $\mathbf{F}_p$ et posons $a := \zeta_8 + \zeta_8^{-1}$. Puisque $\zeta_8^4 = -1$, nous constatons que

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

étant donné que les racines des deux polynômes sont $\pm\zeta_8$ et $\pm\zeta_8^{-1}$. Nous en déduisons que $\zeta_8^2 + \zeta_8^{-2} = 0$ et donc que $a^2 = 2$. Si l'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 l'on suppose $p \equiv \pm 5 \bmod 8\mathbf{Z}$, alors $a^p = -a$ et on trouve une égalité similaire, achevant la démonstration. □

Documentation et 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)

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

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

[De22b] ———— – *Une introduction analytique aux corps ultramétriques*, Projet de Master, Université de Mons, disponible sur https://martindbx.github.io/notes/ (2022).

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

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

[3] Alison Miller – *Algebraic Number Theory* (notes), Math **223A**, 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/ (2020).

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

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

[6] Romyar Sharifi – *Algebraic Number Theory*, disponible sur https://www.math.ucla.edu/~sharifi/lecnotes.html.

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