Introduction à la théorie du corps de classe local

Benjamin Schraen

1er septembre 2023

1 Corps locaux

1.1 Définitions

Soit F un corps. On appelle *valuation discrète* (normalisée) sur F une application $v : F \to \mathbb{Z} \cup \{+\infty\}$ telle que

- pour tout $x \in F$, $v(x) = +\infty \Leftrightarrow x = 0$;
- pour tous $x, y \in F$, $v(xy) = v(x) + v(y)$;
- pour tous $x, y \in F$, $v(x + y) \geqslant \inf\{v(x), v(y)\}$;
- $v(F^\times) = \mathbb{Z}$.

Si v est une valuation discrète sur F, on munit l'ensemble F de la topologie induite par la distance $(x, y) \mapsto \alpha^{v(x-y)}$ pour tout réel $0 < \alpha < 1$ (cette topologie ne dépend pas du choix de α).

Définition 1.1. *Un* corps local *est un corps F tel que F est un espace topologique localement compact pour la topologie définie par une valuation discrète v.*

On peut montrer que si F est un corps local il existe une unique valuation discrète normalisée sur F induisant la topologie de F, on la note v_F (ou parfois v lorsque le contexte est clair), voir la remarque 1.5 et l'exercice 1.3 un peu plus loin.

Exercice 1.1. Soit F un corps valué. Vérifier que pour tout $n \in \mathbb{Z}$ et tout $a \in F$, la partie $\{x \in F \mid v(x - a) \geqslant n\}$ est à la fois ouverte et fermée dans F. En déduire que F est totalement discontinu (ses composantes connexes sont les singletons).

Si F est un corps et v une valuation discrète de F, notons $\widehat{F}$ le complété de F pour la distance $(x, y) \mapsto \alpha^{v(x-y)}$ (pour n'importe quelle valeur de $0 < \alpha < 1$).

La valuation v s'étend de façon unique en une application continue $v_{\widehat{F}} : \widehat{F} \to \mathbb{Z} \cup \{+\infty\}$. Alors $v_{\widehat{F}}$ est une valuation discrète sur $\widehat{F}$.

Remarque 1.2. Si F est un corps local, alors F est un espace métrique complet. La réciproque est fausse.

Exemple 1.3. Soit p un nombre premier. Si $\frac{a}{b} \in \mathbb{Q}$, posons $v(\frac{a}{b})_p \coloneqq v_p(a) - v_p(b)$. Il s'agit d'une valuation discrète sur $\mathbb{Q}$. Notons $\mathbb{Q}_p$ son complété. Le corps $\mathbb{Q}_p$ est un corps dont les éléments sont appelés *nombres p-adiques*. On note $\mathbb{Z}_p$ l'ensemble des nombres p-adiques x tels que $v_p(x) \leqslant 0$. Il s'agit d'un sous-anneau de $\mathbb{Q}_p$. Il contient $\mathbb{Z}$ comme sous-anneau dense. On remarque de plus que

$$\{x \in \mathbb{Z}_p \mid v(x) \geqslant n\} = p^n\mathbb{Z}_p.$$

Comme $p^n\mathbb{Z}_p \subset \mathbb{Z}_p$ est ouvert et $\mathbb{Z} \subset \mathbb{Z}_p$ est dense, on a un isomorphisme d'anneaux $\mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$. On en déduit un morphisme d'anneau

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Par complétude de $\mathbb{Z}_p$, ce morphisme est surjectif et il est injectif car $\bigcap_n p^n\mathbb{Z}_p = \bigcap_n \{v_p(x) \geqslant n\} = \{0\}$. On vérifie de plus que ce morphisme est un homémorphisme et donc que $\mathbb{Z}_p$ est compact. Ainsi le corps $\mathbb{Q}_p$ est un corps local.

Exercice 1.2. Démontrer toutes les assertions non démontrées de l'exemple 1.3.

1.2 Structure des corps locaux

Soit F un corps local. L'ensemble $\mathcal{O}_F \coloneqq \{x \in F \mid v(x) \geqslant 0\}$ est un sous-anneau ouvert et fermé de F appelé *anneau de valuation de* F. L'ensemble $\mathfrak{p}_F \coloneqq \{x \in \mathcal{O}_F \mid v(x) > 0\}$ est un idéal de $\mathcal{O}_F$ et c'est le plus grand idéal non trivial de $\mathcal{O}_F$. On a donc $\mathcal{O}_F^\times = \mathcal{O}_F \backslash \mathfrak{p}_F$.

Un élément $\pi \in F$ tel que $v(\pi) = 1$ est appelé *uniformisante* de F. On vérifie qu'un élément π de F est une uniformisante si et seulement si π est un générateur de $\mathfrak{p}_F$.

Le quotient $k_F \coloneqq \mathcal{O}_F/\mathfrak{p}_F$ est un corps qui est à la fois discret et compact, c'est donc un corps fini. On l'appelle le *corps résiduel de* F. On note q_F son cardinal. L'entier q_F est alors une puissance d'un nombre premier p_F appelé *caractéristique résiduelle de* F.

Exemple 1.4. Soit $\mathbb{F}_q$ un corps fini à q éléments et soit $F = \mathbb{F}_q((T))$ le corps des séries de Laurent à coefficients dans $\mathbb{F}_q$. C'est-à-dire

$$F \coloneqq \left\{ \sum_{n >> -\infty} a_n T^n \right\}.$$

On pose $v\left(\sum_{n>>-\infty} a_n T^n\right) = \min\{n \in \mathbb{Z} \mid a_n \neq 0\}$. L'application v est une valuation discrète sur F qui fait de F un corps local. On a alors

$$\mathcal{O}_F = \mathbb{F}_q[[T]] = \left\{\sum_{n\geqslant 0} a_n T^n\right\},$$

$\mathfrak{p}_F = T\mathbb{F}_q[[T]]$ ainsi que $k_F = \mathbb{F}_q$. L'élément T est une uniformisante de F. On a donc

$$\mathcal{O}_F^\times = \left\{\sum_{n\geqslant 0} a_n T^n \mid a_0 \neq 0\right\}.$$

Ainsi $T/(1-T)$ est une autre uniformisante de F.

Remarque 1.5. On a alors, pour $x \in \mathcal{O}_F$, $v_F(x) = \min\{i \in \mathbb{N} \mid x \in \mathfrak{p}_F^i\}$. On en déduit que la valuation v_F ne dépend que de la topologie de F.

Exercice 1.3. Soit F un corps local de valuation v.

1) Montrer que $\mathfrak{p}_F = \{x \in F \mid \lim_{n\to+\infty} x^n = 0\}$.
2) En déduire que v ne dépend que de la topologie de F.

Dans la suite de ce cours, on utilisera la notation U_F pour le groupe multiplicatif $\mathcal{O}_F^\times$. Ce groupe topologique contient des sous-groupes ouverts intéressants. Si $n \in \mathbb{N}_{\geqslant 1}$, on pose $U_F^n := 1 + \pi^n \mathcal{O}_F$ et, par convention, $U_F^0 := U_F$. Le morphisme d'anneaux $\mathcal{O}_F \to k_F$ induit un morphisme de groupes $\mathcal{O}_F^\times \to k_F^\times$. Ce morphisme est surjectif car $\mathcal{O}_F$ est un anneau local et son noyau est U_F^1. On a donc un isomorphisme de groupes finis $U_F^0/U_F^1 \xrightarrow{\sim} k_F^\times$.

Exercice 1.4. Si $i \geqslant 1$, on définit une application $U_F^i \to k_F$ par $1 + \pi_F a \mapsto \overline{a}$. Vérifier que cette application est un morphisme surjectif de groupes de noyau U_F^{i+1} de sorte que l'on dispose d'un isomorphisme de groupes $U_F^i/U_F^{i+1} \xrightarrow{\sim} k_F$.

1.3 Résolution des équations polynomiales

Théorème 1.6 (Lemme de Hensel)**.** *Soit F un corps local et soit $P \in \mathcal{O}_F[X]$ un polynôme. On note $\overline{P}$ l'image de P dans $k_F[X]$. Soit $x \in k_F$ une racine de $\overline{P}$ telle que $\overline{P}'(x) \neq 0$. Alors il existe une unique racine $\widetilde{x} \in \mathcal{O}_F$ de P telle que $(\widetilde{x} \ mod\ \mathfrak{p}_F) = x$.*

On peut utiliser ce résultat pour déterminer quelques racines de l'unité appartenant à un corps local F. Rappelons que comme le corps résiduel k_F est fini, son groupe des inversibles $k_F^\times$ est cyclique, d'ordre $q_F - 1$. Soit ζ un générateur de ce groupe. Alors ζ est une racine du polynôme $P = X^{q_F-1} - 1$. De plus

$P'(\zeta) = (q_F - 1)\zeta^{q_F-2} \neq 0$. Il existe donc une unique racine $\widetilde{\zeta} \in \mathcal{O}_F$ au polynôme $X^{q-1} - 1$. Ainsi $\widetilde{\zeta}^{q_F-1} = 1$ et $\widetilde{\zeta}$ est un élément d'ordre $q_F - 1$. On en déduit que $\mu_{q_F-1} \subset F^\times$.

Exercice 1.5. Démontrer que si n est un entier premier à p_F, alors $\mu_n \cap F = \mu_{n\wedge(q_F-1)}$. Que dire si n n'est pas premier à p_F ?

1.4 Extensions de corps locaux

Soit F un corps local et soit E/F une extension finie.

Théorème 1.7. *Il existe une unique valuation discrète v sur E telle que la topologie de F soit induite par v. De plus E est un corps local pour la topologie définie par cette valuation et l'inclusion $F \subset E$ est continue.*

Exercice 1.6. Vérifier que $\mathcal{O}_E \cap F = \mathcal{O}_F$ et $\mathfrak{p}_E \cap F = \mathfrak{p}_F$.

Les inclusions $\mathcal{O}_F \subset \mathcal{O}_E$ et $\mathfrak{p}_F \subset \mathfrak{p}_E$ induisent un morphisme de corps résiduel $k_F \hookrightarrow k_E$ (rappelons qu'un morphisme de corps est toujours injectif). Comme k_E et k_F sont des corps finis, l'extension k_E/k_F est finie. On note $f_{E/F}$ son degré, qu'on appelle *degré résiduel* de l'extension E/F.

Comme $\pi_F \in \mathfrak{p}_F \subset \mathfrak{p}_E$, il existe un entier $e_{E/F} \in \mathbb{N}_{\geqslant 1}$ et un inversible $u \in \mathcal{O}_E^\times$ tels que $\pi_F = u\pi_E^{e_{E/F}}$. De façon équivalente, $\mathfrak{p}_F\mathcal{O}_E E = \mathfrak{p}_E^{e_{E/F}}$ prouvant que $e_{E/F}$ ne dépend pas du choix des uniformisantes π_E et π_F. L'entier $e_{E/F}$ est appelé *indice de ramification* de l'extension E/F.

Théorème 1.8. *On a $e_{E/F}f_{E/F} = [E : F]$.*

Lorsque $e_{E/F} = 1$, on dit que l'extension E/F est *non ramifiée*, ce qui est encore équivalent au fait qu'une uniformisante de F est une uniformisante de E. Dans le cas contraire, on dit que l'extension est *ramifiée*.

Lorsque $f_{E/F} = 1$, on dit que l'extension est *totalement ramifiée*.

Exemple 1.9. Posons $E = \mathbb{Q}_p(\zeta_p)$. Dans $\mathcal{O}_E$, on a $(1 - \zeta_p^i) \in (1 - \zeta_p)\mathcal{O}_E$ pour tout $i \geqslant 1$. Par ailleurs si $1 \leqslant i \leqslant p - 1$, il existe $j \geqslant 1$ tel que $ij \equiv 1\,[p]$, on en déduit que

$$(1 - \zeta_p) = (1 - \zeta_p^{ij}) \in (1 - \zeta_p^i)\mathcal{O}_E.$$

On en déduit que $(1 - \zeta_p^i)\mathcal{O}_E = (1 - \zeta_p)\mathcal{O}_E$. De plus l'égalité $\prod_{i=1}^{p-1}(1 - \zeta_p^i) = p$ implique que $p\mathcal{O}_E = (1 - \zeta_p)^{p-1}\mathcal{O}_E$ et donc que $p - 1 | e_{E/\mathbb{Q}_p}$. Comme par ailleurs $[E : \mathbb{Q}_p] \leqslant p - 1$, on a finalement

$$e_{E/\mathbb{Q}_p} = [E : \mathbb{Q}_p] = p - 1$$

et l'extension est totalement ramifiée.

Exemple 1.10. Soit $n \in \mathbb{N}_{\geqslant 1}$ un entier premier à p et soit $E = \mathbb{Q}_p(\zeta_n)$. Remarquons que comme $\zeta_n^n = 1$, on a $\zeta_n \in \mathcal{O}_E$. Notons $\overline{\zeta}_n$ l'image de ζ_n dans $\mathbb{F}_p$. Soit $\overline{P} \in \mathbb{F}_p[X]$ le polynôme minimal de $\overline{\zeta}_n$ sur $\mathbb{F}_p$ et soit $P \in \mathbb{Z}_p[X]$ un relevé de $\overline{P}$ tel que $\deg P = \deg \overline{P}$. On a $\overline{P} | X^n - 1$ dans $\mathbb{F}_p[X]$ et $X^n - 1$ est à racines simples, il en est donc de même de $\overline{P}$, ce qui implique $\overline{P}'(\overline{\zeta_n}) = 1$. Il existe donc un unique $x \in \mathcal{O}_E$ tel que $P(x) = 0$ et $x \mapsto \overline{\zeta_n}$. Alors $[\mathbb{Q}_p(x) : \mathbb{Q}_p] = \deg P = \deg \overline{P} = [k_E : k_F]$, ce qui prouve que $\mathbb{Q}_p(x)/\mathbb{Q}_p$ est non ramifiée. On peut appliquer le lemme de Hensel au polynôme $X^n - 1$ dans l'extension $\mathbb{Q}_p(x)/\mathbb{Q}_p$ et en déduire qu'il existe une unique racine ζ_n de $X^n - 1$ dans $\mathbb{Q}_p(x)$ se réduisant sur $\overline{\zeta}_n$. Ainsi $\zeta_n \in \mathbb{Q}_p(x)$ et donc $E = \mathbb{Q}_p(x)$ est une extension non ramifiée de $\mathbb{Q}_p$.

Exercice 1.7. Soit E'/F une extension finie de corps de nombres et soit $F \subset E \subset E'$ une extension intermédiaire. Montrer alors que

$$f_{E'/F} = f_{E'/E} f_{E/F}, \qquad e_{E'/F} = e_{E'/E} e_{E/F}.$$

Supposons à présent que l'extension E/F est galoisienne. Par unicité de la valuation v_E, on a

$$v_E(\sigma(\cdot)) = v_E \tag{1}$$

pour tout $\sigma \in \mathrm{Gal}(E/F)$. Ainsi le groupe agit par isométries sur E. En particulier $\mathrm{Gal}(E/F)$ préserve $\mathcal{O}_E$ et $\mathfrak{p}_E$ et induit donc une action sur $\mathrm{Gal}(k_E/k_F)$. En particulier on obtient un morphisme de groupes $\sigma \mapsto \overline{\sigma}$ de $\mathrm{Gal}(E/F)$ vers $\mathrm{Gal}(k_E/k_F)$. On note $I(E/F)$ son noyau, on l'appelle le *sous-groupe d'inertie* de E/F.

Théorème 1.11. *Le morphisme* $\mathrm{Gal}(E/F) \to \mathrm{Gal}(k_E/k_F)$ *est surjectif. De plus on a* $f_{E/F} = |\mathrm{Gal}(k_E/k_F)|$ *et* $e_{E/F} = |I(E/F)|$.

En particulier, l'extension E/F est totalement ramifiée si et seulement si $I(E/F) = \mathrm{Gal}(E/F)$. Le sous-groupe d'inertie peut encore être caractérisé comme suit :

$$I(E/F) = \{\sigma \in \mathrm{Gal}(E/F) \mid \forall x \in \mathcal{O}_E,\ \sigma(x) \in x + \mathfrak{p}_E\}.$$

Exercice 1.8. Soit E'/F une extension galoisienne finie de corps de nombres et soit $F \subset E \subset E'$ une extension intermédiaire. Montrer alors que $I(E'/E) = \mathrm{Gal}(E'/E) \cap I(E'/E)$. Si de plus E/F est galoisienne, montrer que $I(E/F)$ est l'image dans $\mathrm{Gal}(E/F)$ de $I(E'/F)$ et que l'on a une suite exacte de groupes finis

$$0 \longrightarrow I(E'/E) \longrightarrow I(E'/F) \longrightarrow I(E/F) \longrightarrow 0.$$

Rappelons que si $k/\mathbb{F}_q$ est une extension de corps finis, alors cette extension est galoisienne et le groupe $\mathrm{Gal}(k/\mathbb{F}_q)$ est cyclique, engendré par la sustitution de Frobenius $\varphi_q : x \mapsto x^q$.

Si E/F est une extension galoisienne non ramifiée de corps locaux, on appelle *élément de Frobenius* l'unique élément $\mathrm{Frob}_{E/F} \in \mathrm{Gal}(E/F)$ s'envoyant sur la substitution de Frobenius dans $\mathrm{Gal}(k_E/k_F)$.

Exercice 1.9. 1) Montrer qu'une extension non ramifiée de corps locaux est automatiquement galoisienne (on pourra utiliser le lemme de Hensel).

2) Soit E'/F une extension non ramifiée finie de corps locaux et soit $F \subset E \subset E'$ une extension intermédiaire. Montrer que E/F et E'/E sont non ramifiée et que

$$(\mathrm{Frob}_{E'/F})_{|E} = \mathrm{Frob}_{E/F}, \qquad \mathrm{Frob}_{E'/E} = \mathrm{Frob}_{E'/F}^{f_{E/F}}.$$

Proposition 1.12. *Soit E/F une extension galoisienne finie de corps locaux. Il existe une plus grande sous-extension $F' \subset E$ telle que F'/F est non ramifiée. Alors E/F' est totalement ramifiée et $I(E/F) = \mathrm{Gal}(E/F')$.*

Démonstration. Soit alors F' une sous-extension non ramifiée de F contenue dans E. D'après l'exercice 1.8, l'image de $I(E/F)$ dans $\mathrm{Gal}(F'/F)$ est triviale, de sorte que $I(E/F) \subset \mathrm{Gal}(E/F')$ et $F' \subset E^{I(E/F)}$. Le même exercice 1.8 montre par ailleurs que $I(E^{I(E/F)}/F) = \{1\}$ de sorte que $E^{I(E/F)}/F$ est non ramifiée. □

Remarque 1.13. Attention, en général il n'existe pas de plus grande sous-extension totalement ramifiée !

2 Théorie du corps de classe locale

2.1 Extensions non ramifiées

Soit E/F une extension galoisienne de corps locaux.

Proposition 2.1. *Si l'extension E/F est non ramifiée , alors $N_{E/F}(U_E) = U_F$.*

Démonstration. On a bien $N_{E/F}(U_E) \subset U_F$. Comme l'extension E/F est galoisienne, on a $N_{E/F}(x) = \prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(x)$. On en déduit que $N_{E/F}(U_E) \subset U_F$ et que, si $i \geqslant 1$, $\sigma(U_F^i) = U_F^i$ pour tout $\sigma \in \mathrm{Gal}(E/F)$ de sorte que $N_{E/F}(U_E^i) \subset U_E^i \cap U_F = (1 + \pi_F^i \mathcal{O}_E) \cap \mathcal{O}_F = 1 + \pi_F^i \mathcal{O}_F = U_F^i$ (nous avons utilisé ici le fait que π_F est également une uniformisante de E puisque E/F est non ramifiée). Nous avons donc deux diagrammes commutatifs, $i \geqslant 1$,

$$\begin{array}{ccc} U_E/U_E^1 & \xrightarrow{N_{E/F}} & U_F/U_F^1 \\ \downarrow \wr & & \downarrow \wr \\ k_E^\times & \xrightarrow{N_{k_E/k_F}} & k_F^\times \end{array} \qquad \begin{array}{ccc} U_E^i/U_E^{i+1} & \xrightarrow{N_{E/F}} & U_F^i/U_F^{i+1} \\ \downarrow \wr & & \downarrow \wr \\ k_E & \xrightarrow{\mathrm{Tr}_{k_E/k_F}} & k_F \end{array}$$

En effet, si $x \in \mathcal{O}_E$, on a, pour $i \geqslant 1$,

$$N_{E/F}(1+\pi_F^i x) = \prod_{\sigma \in \mathrm{Gal}(E/F)} (1+\pi_F^i \sigma(x)) \equiv 1 + \pi_F^i \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(x) \, [\mathfrak{p}]_F^{i+1}.$$

Comme k_E/k_F est une extension séparable, l'application $\mathrm{Tr}_{k_E/k_F} : k_E \to k_F$ est surjective et il en est de même de $N_{E/F} : U_E^i/U_E^{i+1} \to U_F^i/U_F^{i+1}$ pour tout $i \geqslant 1$. De même, si $x \in k_E^\times$, on a

$$N_{k_E/k_F}(x) = x^{1+q_F+\cdots+q_F^{d-1}}$$

de sorte que N_{k_E/k_F} est surjective (exercice) et donc aussi $N_{E/F} : U_E/U_E^1 \to U_F/U_F^1$. On déduit de ce résultat que l'application $N_{E/F} : U_E/U_E^i \to U_F/U_F^i$ est surjective pour tout i. Si $x \in U_F$, on peut trouver, pour tout $n \geqslant 1$, un élément $y_n \in U_E$ tel que $x - N_{E/F}(y_n) \in \pi_F^n \mathcal{O}_F$. On en déduit l'existence de $y \in \mathcal{O}_E$ tel que $x = N_{E/F}(y)$. □

Si E/F est une extension non ramifiée, alors $N_{E/F}(\pi_E) \in \pi_F^{[E:F]}\mathcal{O}_F^\times$ et donc $F^\times/N_{E/F}(E^\times)$ est un groupe cyclique d'ordre $[E:F]$ engendré par l'image de l'uniformisante π_F. Il existe donc un unique isomorphisme de groupes

$$\mathrm{rec}_{E/F} : F^\times/N_{E/F}(E^\times) \xrightarrow{\sim} \mathrm{Gal}(E/F)$$

envoyant π_F sur l'élément de Frobenius $\mathrm{Frob}_{E/F}$. Cet isomorphisme est un cas très particulier de l'isomorphisme de réciprocité locale.

Corollaire 2.2. *Soit E/F une extension non ramifiée de corps locaux. L'application $F' \mapsto N_{E/F'}(E^\times)$ induit une bijection décroissante entre l'ensemble des sous-extensions $F \subset F' \subset E$ et l'ensemble des sous-groupes de $F^\times$ contenant $N_{E/F}(E^\times)$.*

Démonstration. C'est une conséquence immédiate de la théorie de Galois. Soit $N_{E/F}(E^\times) \subset H \subset F^\times$ un sous-groupe. Alors $\mathrm{rec}_{E/F}(H)$ est un sous-groupe de $\mathrm{Gal}(E/F)$. Posons $F' = E^H$. Il suffit de vérifier que $H = N_{E/F'}(E^\times)$. C'est un exercice. □

Proposition 2.3. *Soit F un corps local et soit F_s une clôture séparable de F. Soit $d \geqslant 1$ un entier. Alors il existe une extension non ramifiée E/F de degré d contenue dans F_s et celle-ci est cyclique.*

Démonstration. D'après la théorie de Galois des corps finis, on sait que le corps k_F qu'il existe un polynôme unitaire irréductible $P \in k_F[X]$ de degré d. Soit $\widetilde{P} \in \mathcal{O}_F[X]$ un relevé unitaire de P. Comme k_F est fini, donc parfait, le polynôme P

est séparable et donc le polynôme $\widetilde{P}$ également. Soit $E \subset F_s$ un sous-corps engendré par une racine de $\widetilde{P}$. D'après le théorème 1.7, le corps E est un corps local. Comme P est irréductible, $\widetilde{P}$ l'est aussi et $[E : F] = \deg P$. Comme le polynôme P est scindé sur le corps résiduel de E, on a nécessairement $[k_E : k_F] \geqslant \deg P = [E : F]$. Ainsi l'extension E/F est non ramifiée de degré d. Cette extension est cyclique de degré d en vertu de l'exercice 1.9, du théorème 1.11 et du fait que $\mathrm{Gal}(k_E/k_F)$ est cyclique. Si E'/F est une autre extension non ramifiée de degré d incluse dans F_s. Alors EE'/F est non ramifiée par la proposition 1.12, et donc cyclique, ce qui implique que $E = EE' = E'$. □

2.2 Le cas général

On dit qu'une extension finie de corps E/F est *abélienne* si elle est galoisienne et si le groupe $\mathrm{Gal}(E/F)$ est abélien.

Théorème 2.4 (Loi de réciprocité locale)**.** *Pour toute extension abélienne finie E/F de corps locaux, le sous-groupe $N_{E/F}(E^\times)$ est ouvert dans $F^\times$ et il existe un isomorphisme de groupes*

$$\mathrm{rec}_{E/F} : F^\times/N_{E/F}(E^\times) \xrightarrow{\sim} \mathrm{Gal}(E/F)$$

tel que les propriétés suivantes sont satisfaites.

(i) Si E/F est non ramifiée, alors $\mathrm{rec}_{E/F}(\pi_F) = \mathrm{Frob}_{E/F}$.

(ii) Si E'/F' est une extension abélienne finie telle que $F \subset F'$ et $E \subset E'$, alors le diagramme suivant commute

$$\begin{array}{ccc} F'^\times/N_{E'/F'}(E'^\times) & \xrightarrow{N_{F'/F}} & F^\times/N_{E/F}(E^\times) \\ \downarrow{\scriptstyle \mathrm{rec}_{E'/F'}} & & \downarrow{\scriptstyle \mathrm{rec}_{E/F}} \\ \mathrm{Gal}(E'/F') & \xrightarrow{\sigma \mapsto \sigma_{|E}} & \mathrm{Gal}(E/F) \end{array}$$

où la flèche horizontale du bas est le morphisme induit par l'application de restriction $\mathrm{Gal}(E'/F') \to \mathrm{Gal}(E/F)$.

(iii) Si $\tau : E \xrightarrow{\sim} E'$ est un isomorphisme de corps valués et si $F' \coloneqq \tau(F)$, on a un diagramme commutatif

$$\begin{array}{ccc} F^\times/N_{E/F}(E^\times) & \xrightarrow{\tau} & F'^\times/N_{E'/F'}(E'^\times) \\ \downarrow{\scriptstyle \mathrm{rec}_{E/F}} & & \downarrow{\scriptstyle \mathrm{rec}_{E'/F'}} \\ \mathrm{Gal}(E/F) & \xrightarrow{\sigma \mapsto \tau\sigma\tau^{-1}} & \mathrm{Gal}(E'/F'). \end{array}$$

De plus, il existe au plus une famille d'isomorphismes vérifiant les propriétés (i) et (ii).

Explicitons quelques cas particuliers de la fonctorialité (ii) dans le théorème 2.4.

Si $F' = F$, on a un diagramme commutatif :

$$\begin{array}{ccc} F^\times/N_{E'/F}(E'^\times) & \twoheadrightarrow & F^\times/N_{E/F}(E^\times) \\ \downarrow{\scriptstyle r_{E'/F}} & & \downarrow{\scriptstyle \mathrm{rec}_{E/F}} \\ \mathrm{Gal}(E'/F) & \twoheadrightarrow & \mathrm{Gal}(E/F). \end{array}$$

La flèche horizontale supérieure est ici l'application quotient map et la flèche horizontale inférieure est la restriction à E.

Si $E = E'$, on a un diagramme commutatif :

$$\begin{array}{ccc} F'^\times/N_{E/F'}(E^\times) & \xrightarrow{N_{F'/F}} & F^\times/N_{E/F}(E^\times) \\ \downarrow{\scriptstyle r_{E/F'}} & & \downarrow{\scriptstyle \mathrm{rec}_{E/F}} \\ \mathrm{Gal}(E/F')^{\mathrm{ab}} & \longrightarrow & \mathrm{Gal}(E/F)^{\mathrm{ab}}. \end{array}$$

La flèche horizontale inférieure est induite par l'inclusion $\mathrm{Gal}(E/F') \subset \mathrm{Gal}(E/F)$.

Théorème 2.5 (Théorème d'existence local)**.** *Soit $N \subset F^\times$ un sous-groupe ouvert d'indice fini. Alors il existe une extension abélienne E/F telle que $N = N_{E/F}(E^\times)$.*

Corollaire 2.6. *Soit F_s une clôture séparable de F. L'application $E \mapsto N_{E/F}(E^\times)$ induit une bijection décroissante de l'ensemble des extensions abéliennes finies $E \subset F_s$ de F sur l'ensemble des sous-groupes ouverts d'indice fini dans $F^\times$.*

Démonstration. Remarquons tout d'abord que si $E \subset F_s$ est une extension abélienne finie de F, alors $N_{E/F}(E^\times)$ est un sous-groupe ouvert d'indice fini dans $F^\times$ d'après le théorème 2.4. Si $E \subset E'$, l'égalité $N_{E'/F} = N_{E/F} \circ N_{E'/E}$ implique que $N_{E'/F}(E'^\times) \subset N_{E/F}(E^\times)$. L'application est donc décroissante. Elle est surjective d'après le théorème 2.5. Il nous reste donc à prouver son injectivité.

Supposons que $E_1, E_2 \subset F_s$ sont deux extensions abéliennes finies de F telles que $N_{E_1/F}(E_1^\times) = N_{E_2/F}(E_2^\times)$. Posons $E = E_1E_2$. Il s'agit d'une extension galoisienne et abélienne car

$$\mathrm{Gal}(E/F) \hookrightarrow \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F).$$

Si $i \in \{1,2\}$, on déduit de la propriété (ii) du théorème 2.4 que l'on a un diagramme commutatif

$$\begin{array}{ccc} F^\times/N_{E/F}(E^\times) & \longrightarrow & F^\times/N_{E_i/F}(E_i^\times) \\ \downarrow{\scriptstyle \mathrm{rec}_{E/F}} & & \downarrow{\scriptstyle \mathrm{rec}_{E_i/F}} \\ \mathrm{Gal}(E/F) & \longrightarrow & \mathrm{Gal}(E_i/F) \end{array}$$

qui implique que $\mathrm{Gal}(E/E_i) = \mathrm{rec}_{E/F}(N_{E_i/F}(E_i^\times))$. On en déduit que $\mathrm{Gal}(E/E_1) = \mathrm{Gal}(E/E_2)$ et donc que $E_1 = E_2$. □

Corollaire 2.7. *Soit E/F une extension finie abélienne. Alors l'extension E/F est non ramifiée si et seulement si $\mathcal{O}_F^\times \subset N_{E/F}(E^\times)$.*

Démonstration. Si l'extension E/F est non ramifiée, alors $U_F \subset N_{E/F}(E^\times)$ par la proposition 2.1. Réciproquement supposons que $\mathcal{O}_F^\times \subset N_{E/F}(E^\times)$. Soit $d = [E : F]$ et soit E' l'extension (unique à isomorphisme près) non ramifiée de F de degré d qui existe par la proposition 2.3. On a alors $N_{E'/F}(E'^\times) = (\pi_F^d)^{\mathbb{Z}}\mathcal{O}_F^\times$ d'après la proposition 2.1. Comme $\pi_F^d = N_{E/F}(\pi_F) \in N_{E/F}(E^\times)$, on a $N_{E'/F}(E'^\times) \subset N_{E/F}(E^\times)$. On déduit du corollaire 2.6 qu'il existe un morphisme F-linéaire $E \hookrightarrow E'$ et donc $E \simeq E'$ par égalité des degrés. Ainsi E/F est non ramifiée. □

2.3 Le cas des extensions infinies

Soit F_s une clôture séparable de F. Le corps F_s est l'union de ses sous-extensions galoisiennes finies. On note $F^{\mathrm{ab}} \subset F_s$ l'union des sous-extensions abéliennes finies de F. On rappelle que le groupe de Galois $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ est le groupe des automorphismes du corps F^{ab} fixant les éléments de F. On a alors un isomorphisme de groupes

$$\mathrm{Gal}(F^{\mathrm{ab}}/F) \simeq \varprojlim_{E/F} \mathrm{Gal}(E/F)$$

où la limite projective de droite est prise sur les extensions abéliennes finies $E \subset F_s$. On munit le groupe $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ de la topologie de la limite projective (ou de la topologie de la convergence simple, ce qui est équivalent), ce qui en fait un groupe topologique compact. La théorie des Galois des extensions infinies nous fournit alors une bijection décroissante $E \mapsto \mathrm{Gal}(F^{\mathrm{ab}}/E)$ entre les sous-corps E de F^{ab} contenant F et les sous-groupes fermés de $\mathrm{Gal}(F^{\mathrm{ab}}/F)$. La bijection réciproque est donnée par $H \mapsto (F^{\mathrm{ab}})^H$.

La proriété (ii) du théorème 2.4 implique alors que les morphismes $\mathrm{rec}_{E/F}$ se recollent en un morphisme de groupes topologiques

$$\mathrm{rec}_F : F^\times \longrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F).$$

Proposition 2.8. *Le morphisme* rec_F *est injectif et d'image dense.*

Démonstration. Soit $a \in F^\times$ un élément différent de 1. Il existe alors un sous-groupe ouvert $N \subset F^\times$ tel que $a \notin F^\times$. Soit E/F l'extension abélienne de F telle que $N = \mathrm{Gal}(F^{\mathrm{ab}}/E)$. Alors l'image $\mathrm{rec}_{E/F}(a)$ de $\mathrm{rec}_F(a)$ dans $\mathrm{Gal}(E/F)$ est non trivial et donc $\mathrm{rec}_F(a)$ est non trivial.

Il est d'image dense car, si E/F est finie, la composée $F^\times \xrightarrow{\mathrm{rec}_F} \mathrm{Gal}(F_s/F) \to \mathrm{Gal}(E/F)$ coïncide avec $\mathrm{rec}_{E/F}$ et est donc surjective. □

2.4 Le groupe de Weil

On note F^{nr} l'union de toutes les extensions non ramifiée de F_s/F. Pour tout $d \geqslant 1$, notons $F_d \subset F_s$ l'unique extension non ramifiée de F de degré d dont l'existence et l'unicité sont fournies par la proposition 2.3. On a donc un isomorphisme

$$\mathrm{Gal}(F^{\mathrm{nr}}/F) \simeq \varprojlim_{d\in\mathbb{N}^*} \mathrm{Gal}(F_d/F) \simeq \varprojlim_{d\in\mathbb{N}^*} (\mathbb{Z}/d\mathbb{Z}) \simeq \widehat{\mathbb{Z}}.$$

Un pro-générateur de ce groupe est donné par la famille des éléments de Frobenius $\mathrm{Frob}_F \coloneqq (\mathrm{Frob}_{F_d/F})_{d\geqslant 1}$.

On note $I(F_S/F)$ le noyau du morphisme de restriction $\mathrm{Gal}(F_s/F) \to \mathrm{Gal}(F^{\mathrm{nr}}/F)$.

Exercice 2.1. Vérifier que $I(F_s/F) \simeq \varprojlim_{E/F} I(E/F)$ où la limite est prise sur les sous-extensions galoisiennes finies E/F de F_s.

Le morphisme composé

$$F^\times \xrightarrow{\mathrm{rec}_F} \mathrm{Gal}(F_s/F)^{\mathrm{ab}} \twoheadrightarrow \mathrm{Gal}(F^{\mathrm{nr}}/F)$$

a pour noyau $\mathcal{O}_F^\times$ et envoie π_F sur Frob_F. On en déduit que le morphisme rec_F n'est *pas* surjectif. L'introduction du groupe de Weil permet de remédier à ce problème.

Définition 2.9. *On appelle* groupe de Weil *de* F *le sous-groupe* W_F *de* $\mathrm{Gal}(F_s/F)$ *obtenu comme image inverse de* Frob_F *par l'application quotient* $\mathrm{Gal}(F_s/F) \twoheadrightarrow \mathrm{Gal}(F^{\mathrm{nr}}/F)$.

Noter que l'on peut identifier W_F au produit fibré $\mathrm{Gal}(F_s/F) \times_{\mathrm{Gal}(F^{\mathrm{nr}}/F)} \mathrm{Frob}_F^{\mathbb{Z}}$. On munit le groupe W_F de la topologie induite par la topologie produit sur $\mathrm{Gal}(F_s/F) \times \mathrm{Frob}_F^{\mathbb{Z}}$ où $\mathrm{Frob}_F^{\mathbb{Z}}$ est muni de la topologie discrète. Cette topologie est compatible avec la structure de groupe et fait de W_F un groupe topologique.

Exercice 2.2. 1) Vérifier que l'inclusion $W_F \subset \mathrm{Gal}(F_s/F)$ est continue.

2) Vérifier que $I(F_s/F)$ est un sous-groupe ouvert et compact de W_F.

3) Si H est un groupe topologique, on note H^{ab} le quotient de H par l'adhérence du sous-groupe dérivé H'. Montrer que $\mathrm{Gal}(F_s/F)^{\mathrm{ab}} \simeq \mathrm{Gal}(F^{\mathrm{ab}}/F)$.

4) Montrer que W_F^{ab} est l'image de W_F dans $\mathrm{Gal}(F^{\mathrm{ab}}/F)$.

Théorème 2.10. *Le morphisme* rec_F *induit un isomorphisme de groupes topologiques* $F^\times \xrightarrow{\sim} W_F^{\mathrm{ab}}$.

Démonstration. Soit E/F une extension finie avec $E \subset F_s$. On déduit de la proposition 2.1 que $U_F \subset N_{E/F}(E^\times)$ et du théorème 2.4 que $\mathrm{rec}_{E/F}(U_F) = \{1\} \subset \mathrm{Gal}(E/F)$. En particulier $\mathrm{rec}_F(U_F) \subset \varprojlim_{E/F,\mathrm{ab}} I(E/F) = I(F^{\mathrm{ab}}/F)$. Ainsi rec_F induit un morphisme de groupes $F^\times/U_F \to W_E/I(F^{\mathrm{ab}}/F)$ envoyant π_F sur Frob_F, et qui est donc un isomorphisme. Par ailleurs $\mathrm{rec}_{F|U_F}$ induit un morphisme injectif continu $U_F \hookrightarrow I(F^{\mathrm{ab}}/F)$ et d'image dense. Comme U_F est compact, il s'agit d'un homéomorphisme. On en déduit le résultat. □

2.5 Caractères

Si G est un groupe topologique, on note $\widehat{G}$ l'ensemble des morphismes de groupes topologiques $\chi : G \to \mathbb{C}^\times$. Le théorème 2.10 implique que rec_F induit une bijection

$$\widehat{W_F} \simeq \widehat{F^\times}$$

définie par $\chi \mapsto \chi \circ \mathrm{rec}_F$. On obtient un *cas particulier de la correspondance de Langlands locale*, le cas du groupe GL_1.

Il est important de remarquer que tout caractère de W_F ne se prolonge pas en un caractère de $\mathrm{Gal}(F_s/F)$.

Exercice 2.3. 1. Montrer que si χ est un caractère de W_F, alors $\chi(I(F_s/F))$ est un sous-groupe fini de $\mathbb{C}^\times$.

2. Montrer qu'un caractère $\chi : W_F \to \mathbb{C}^\times$ se prolonge en un caractère de $\mathrm{Gal}(F_s/F)$ si et seulement si $\chi(W_F) \subset \{|z| = 1\}$ si et seuement si $|\chi(\mathrm{rec}_F(\pi_F))| = 1$ pour une (resp. toute) uniformisante π_F de F.

Remarque 2.11. On peut bien sûr remplacer $\mathbb{C}$ par un corps local non archimédien du type $\mathbb{Q}_\ell$ pour ℓ un nombre premier. Dans ce cas, il le groupe $\chi(I(F_s/F))$ peut-être infini, on parle alors de *représentation ℓ-adique* du groupe de Weil.

2.6 Démonstration de l'unicité de la loi de réciprocité locale

Nous démontrons l'assertion d'unicité dans le théorème 2.4. Nous utilisons le lemme suivant.

Lemme 2.12. *Soit E/F une extension finie galoisienne. Soit $\sigma \in \mathrm{Gal}(E/F)$. Il existe alors une extension finie E'/E telle que E'/F est galoisienne et il existe $\widetilde{\sigma} \in \mathrm{Gal}(E'/F)$ relevant σ tel que $E'/(E')^{\widetilde{\sigma}}$ est non ramifiée.*

Vérifions dans un premier temps que le lemme implique l'unicité de la loi de réciprocité locale. Soit E/F une extension galoisienne finie. Soit $\sigma \in \mathrm{Gal}(E/F)$ et soient E' et $\widetilde{\sigma}$ comme dans le lemme 2.12. Posons $F' := (E')^{\widetilde{\sigma}}$. On a $\widetilde{\sigma} \in \mathrm{Gal}(E'/E'^{\widetilde{\sigma}})$. Il existe donc un entier $m \geqslant 0$ tel que $\widetilde{\sigma} = (\mathfrak{p}_{F'}, E'/F')^m$. La propriété (i) du théorème 2.4 montre que $r_{E'/F'}(\pi_F^m) = \widetilde{\sigma}$ et la propriété (ii) montre alors que $r_{E/F}^{-1}(\sigma) = N_{F'/F}(\pi_{F'})^m$. Ceci implique que la famille des isomorphismes $r_{E/F}$ est entièrement caractérisée par les propriétés (i) et (ii).

Démonstration du lemme 2.12. Soit $K \subset E$ la sous-extension maximale non ramifiée de F. et soit $r \geqslant 0$ tel que $\sigma|_K = (\mathfrak{p}_F, K/F)^r$. Soit $N \geqslant 1$ un entier multiple de l'ordre de σ dans $\mathrm{Gal}(E/F)$. Soit E_1 la sous-extension maximale non ramifiée de E de degré rN et soit $F_1 \subset E_1$ la sous-extension maximale non ramifiée de F containue dans E_1. On a alors

$$[F_1 : F] = [k_{E_1} : k_F] = rN[k_E : k_F]$$

et $[K : F] = [k_E : k_F]$ de sorte que $[F_1 : K] = rN$. De plus, on a clairement $F_1 \cap E = K$. Ainsi $[F_1E : E] = [F_1 : K] = rN = [E_1 : E]$. Ainsi $E_1 = F_1E$. On en déduit que l'extension E_1/F est galoisienne. De plus l'application $\tau \mapsto (\tau|_E, \tau|_{F_1})$ identifie $\mathrm{Gal}(E/F)$ au sous-groupe de $\mathrm{Gal}(E/F) \times \mathrm{Gal}(F_1/F)$ constitué des paires (τ_1, τ_2) telles que $\tau_1|_K = \tau_2|_K$. Il existe donc un unique élément $\widetilde{\sigma} \in \mathrm{Gal}(E_1/F)$ tel que $\widetilde{\sigma}|_E = \sigma$ et $\widetilde{\sigma}|_{F_1} = (\mathfrak{p}_F, F_1/F)^r$ (en effet on a $(\mathfrak{p}_F, F_1/F)^r|_K = (\mathfrak{p}_F, K/F)^r = \sigma|_K$). Il reste donc à vérifier que l'extension $E_1/E_1^{\widetilde{\sigma}}$ est non ramifiée. Remarquons que le morphisme de groupes induit par la restriction à F_1 est surjectif :

$$\mathrm{Gal}(E_1/E_1^{\widetilde{\sigma}}) \twoheadrightarrow \mathrm{Gal}(F_1/F_1^{\widetilde{\sigma}}). \tag{2}$$

En effet les deux groupes sont cycliques, engendrés respectivement par $\widetilde{\sigma}$ et $\widetilde{\sigma}|_{F_1}$. De plus, le membre de droite est un sous-groupe du groupe cyclique $\mathrm{Gal}(F_1/F) \simeq \mathbb{Z}/rN[k_E : k_F]\mathbb{Z}$. Comme $\widetilde{\sigma}|_{F_1} = (\mathfrak{p}_F, F_1/F)^r$, on voit que le groupe $\mathrm{Gal}(F_1/F)$ est cyclique d'ordre $N[k_E : k_F]$. Par ailleurs, on a $\sigma^N = 1$. Ainsi $\widetilde{\sigma}^N|_E = 1$ et $\widetilde{\sigma}|_{F_1}^{N[k_E:k_F]} = 1$, ce qui implique que $\widetilde{\sigma}^{N[k_E:k_F]} = 1$. On en déduit que le morphisme surjectif (2) est un isomorphisme, ce qui implique que $E_1 = E_1^{\widetilde{\sigma}}F_1$. Comme $F_1/F_1^{\widetilde{\sigma}}$ est non ramifiée, l'extension composée $F_1E_1^{\widetilde{\sigma}}/E_1^{\widetilde{\sigma}}$ est également non ramifiée. □

2.7 Le théorème de Kronecker–Weber local

3 Théorie de Lubin–Tate

3.1 Groupes formels de Lubin–Tate

Définition 3.1. *Une* loi de groupe formel *sur $\mathcal{O}_F$ est une série entière $G \in \mathcal{O}_F[[X,Y]]$ vérifiant les propriétés suivantes :*

a) $G(X, G(Y,Z)) = G(G(X,Y), Z)$;

b) $G(0,Y) = Y$ *et* $G(X,0) = X$;

c) il existe une (unique) série $H(X) \in \mathcal{O}_F[[X]]$ *telle que* $G(X, H(X)) = 0$;

d) $G(Y,X) = G(X,Y)$;

e) $G(X,Y) \equiv X + Y$ *dans* $\mathcal{O}_F[[X,Y]]/(X,Y)^2$.

Si G est une loi de groupe formel et E/F est une extension finie de F, on munit l'ensemble $\mathfrak{p}_E$ d'une structure de groupe commutatif en posant, pour $x, y \in \mathfrak{p}_E$,

$$x +_G y \coloneqq G(x,y).$$

Si E' est une extension finie de E, alors $(\mathfrak{p}_E, +_G)$ est un sous-groupe de $(\mathfrak{p}_{E'}, +_G)$. On note $G(E)$ le groupe $(\mathfrak{p}_E, +_G)$. On définit alors $G(F_s) \coloneqq \bigcup_{E/F} G(E)$.

Si $\sigma \in \mathrm{Gal}(F_s/F)$ et si $x, y \in \mathfrak{p}_E$ pour E/F galoisienne finie alors, en utilisant la continuité de l'action du groupe de Galois sur E, on a

$$\sigma(x +_G y) = \sigma(x) +_G \sigma(y).$$

On note $\mathcal{F}_\pi$ l'ensemble des séries formelles $f \in \mathcal{O}_F[[X]]$ ayant les propriétés suivantes

(i) $f(X) \equiv \pi X$ dans $\mathcal{O}_F[[X]]/(X^2)$;

(ii) $f(X) \equiv X^q$ modulo π.

Exemple 3.2. La série $\pi X + X^q$ est toujours dans $\mathcal{F}_\pi$. Si $K = \mathbb{Q}_p$, la série

$$(1+X)^p - 1 = pX + \binom{p}{2} X^2 + \cdots + X^p$$

est dans $\mathcal{F}_p$.

Les séries de $\mathcal{F}_\pi$ permettent de construire des lois de groupe formel.

On appelle *endomorphisme* d'une loi de groupe formelle G une série $f \in X\mathcal{O}_F[[X]]$ telle que

$$G(f(X), f(Y)) = f(G(X, Y))$$

dans $\mathcal{O}_F[[X, Y]]$.

Proposition 3.3. *Soit $f \in \mathcal{F}_\pi$. Il existe alors une unique loi de groupe formel G_f pour laquelle f est un endomorphisme. De plus, il existe un unique morphisme d'anneaux $a \mapsto [a]_f$ de $\mathcal{O}_F$ dans $\mathrm{End}(G_f)$ telle que $[\pi]_f = f$ et telle que pour tout $a \in \mathcal{O}_F$, on a $[a]_f(X) \equiv aX$ dans $\mathcal{O}_F[[X]]/(X^2)$. En particulier, on a, pour tous $a, b \in \mathcal{O}_F$,*

$$[a + b]_f(X) = G_f([a]_f(X), [b]_f(X)), \quad [ab]_f(X) = [a]_f([b]_f(X)).$$

En particulier la condition $[a]_f(X) \equiv aX$ modulo X^2 implique que le morphisme $a \mapsto [a]_f$ est injectif.

Le morphisme $a \mapsto [a]_f$ permet de munir le groupe $G_f(F_s)$ d'une structure de $\mathcal{O}_F$-module en posant, pour $x \in G_f(F_s)$ et $a \in \mathcal{O}_F$,

$$a \cdot_f x = [a]_f(x).$$

3.2 Points de torsion

Fixons $f \in \mathcal{F}_\pi$. On note E_f^n le noyau de l'endomorphisme $[\pi^n]_f = [pi]_f^n$ de $G_f(F_s)$. Il s'agit de l'ensemble

$$E_f^n = \{x \in \mathfrak{p}_{F_s} \mid [\pi]_f^n(x) = 0\}.$$

Par exemple, si $f(X) = (1 + X)^p - 1$ et $F = \mathbb{Q}_p$, on a $E_f^n = \{\zeta - 1 \mid \zeta \in \mu_{p^n}\}$. L'ensemble E_f^n est en fait un sous-$\mathcal{O}_F$-module de $G_f(F_s)$, stable sous l'action de $\mathrm{Gal}(F_s/F)$. On note E_f l'union des sous-$\mathcal{O}_F$-modules E_f^n.

Exercice 3.1. Montrer que E_f est l'ensemble des éléments de torsion du groupe abélien $G_f(F_s)$.

On note alors F_π^n l'extension de F engendrée par les éléments $x \in E_f^n$. Comme E_f^n est stable sous l'action du groupe $\mathrm{Gal}(F_s/F)$, on en déduit que l'extension F_π^n/F est galoisienne.

Comme son nom l'indique, l'extension F_π^n ne dépend pas du choix de $f \in \mathcal{F}_\pi$ mais uniquement de π. C'est une conséquence du résultat suivant.

Proposition 3.4. *Soit f et g deux éléments de $\mathcal{F}_\pi$. Les lois de groupes G_f et G_g sont isomorphes. Plus précisément il existe une unique série formelle $u \in X\mathcal{O}_F[[X]]$ telle que $u \equiv X$ dans $\mathcal{O}_F[[X]]/(X^2)$ et $G_g(u(X), u(Y)) = u(G_f(X, y))$ dans $\mathcal{O}_F[[X, Y]]$.*

Exercice 3.2. Montrer que l'application $x \mapsto u(x)$ induit un isomorphisme de $\mathcal{O}_F$-modules de $G_f(F_s)$ sur $G_g(F_s)$.

Proposition 3.5. *Pour tout $n \geqslant 1$, le $\mathcal{O}_F$-module E_f^n est isomorphe à $\mathcal{O}_F/(\pi^n)$ et le $\mathcal{O}_F$-module E_f est isomorphe à $F/\mathcal{O}_F$.*

Démonstration. D'après le résultat de l'exercice 3.2, il suffit de montrer que le résultat pour E_f^n lorsque $f = \pi X + X^q$ puisqe tous les groupes E_f^n sont isomorphes. Il suffit de prouver que E_f^n est un ensemble de cardinal q^n pour tout $n \geqslant 1$. En effet, supposons ceci démontré. La structure des modules de type fini sur l'anneau principal $\mathcal{O}_F$ implique qu'il existe un isomorphisme de $\mathcal{O}_F$-modules $E_f^n \simeq \mathcal{O}_F/(\pi^{n_1}) \oplus \cdots \oplus \mathcal{O}_F/(\pi^{n_r})$ avec $n_1 + \cdots + n_r = n$. Par ailleurs, l'égalité $|E_f^1| = q$ implique $r = 1$, de sorte que $n_1 = n$.

Démontrons donc que $|E_f^n| = q^n$ pour tout $n \geqslant 1$. Comme E_f^n est l'ensemble des racines du polynôme $[\pi^n]_f = f^{(n)}$ qui appartiennent à $\bigcup_{E/F} \mathfrak{p}_E$, il suffir de montrer que pour tout $\alpha \in F_s$ appartenant à un extension finie $E \subset F_s$ et tel que $v_E(\alpha) > 0$, le polynôme $\pi X + X^q = \alpha$ a exactement q racines dans une extensions finie $E' \subset F_s$ de E et que ses solutions sont dans $\mathfrak{p}_{E'}$. Soit donc E' le corps de décomposition de $\pi X + X^q - \alpha$. Soit $\beta \in E'$ une racine de ce polynôme. On a $(\pi X + X^q - \alpha)' = \pi + qX^{q-1}$. Ainsi si $q = 0$ dans F, le polynôme est séparable et ses racines sont simples. Si $q \neq 0$, et si β est racine double, alors $\pi + q\beta^{q-1} = 0$, ce qui implique que $(q-1)v_{E'}(\beta) = v_{E'}(\pi) - v_{E'}(q) \leqslant 0$. Ainsi $v_{E'}(\beta) \leqslant 0$. Alors $v_{E'}(\pi\beta + \beta^q) \leqslant 0$ et donc $v_{E'}(\alpha) \leqslant 0$, ce qui est faux. L'élément β est donc racine simple du polynôme et vérifie $v_{E'}(\beta) > 0$, ce qu'il fallait démontrer. □

La proposition 3.5 implique l'existence d'un isomorphisme canonique $\mathcal{O}_F^\times \simeq \mathrm{Aut}(E_f)$, l'élément $a \in \mathcal{O}_F^\times$ étant envoyé sur la multiplication $x \mapsto a \cdot_f x$.

Si $\sigma \in \mathrm{Gal}(F_s/F)$, l'élément σ induit un automorphisme du $\mathcal{O}_F$-module E_f. On en déduit un morphisme de groupes $\chi_{\mathrm{LT}} : \mathrm{Gal}(F_s/F) \to \mathrm{Aut}(E_f) \simeq \mathcal{O}_F^\times$ dont le noyau est $\mathrm{Gal}(F_s/F_\pi)$.

Proposition 3.6. *Le morphisme de groupes χ_{LT} induit un isomorphisme de groupes $\mathrm{Gal}(F_\pi/F) \to \mathrm{Aut}(E_f) \simeq \mathcal{O}_F^\times$.*

Démonstration. On peut encore supposer que $f = \pi X + X^q$. Le morphisme de groupes χ_{LT} induit une injection $\mathrm{Gal}(F_\pi^n/F) \hookrightarrow (\mathcal{O}_F/(\pi^n))^\times$, il suffit donc de

prouver que $[F_\pi^n : F] \geqslant q^n - q^{n-1}$. Soit $\alpha \in E_f^n$ un élément tel que $[\pi]_f^n(\alpha) = 0$ mais $[\pi]_f^{n-1}(\alpha) \neq 0$, un tel élément existe d'après la proposition 3.5. On a

$$f^{(n)} = \pi f^{(n-1)} + (f^{(n-1)})^q$$

de sorte que $f^{(n-1)}$ divise $f^{(n)}$. Posons $P = \frac{f^{(n)}}{f^{(n-1)}}$. On a alors $P(\alpha) = 0$. Il suffit alors de prouver que P est un polynôme irréductible de degré $q^n - q^{n-1}$. La congruence $f(X) \equiv X^q\,[\pi]$ implique que $P(X) \equiv X^{q^n - q^{n-1}}\,[\pi]$. Par ailleurs $P(X) = f^{(n-)}(X)^{q-1} + \pi$ de sorte que P est un polynôme d'Eisenstein dans $\mathcal{O}_F[X]$. Il s'agit donc d'un polynôme irréductible. □

Remarquons qu'il découle encore de la proposition 3.4 que le morphisme $\chi_{\mathrm{LT}} : \mathrm{Gal}(F_\pi/F) \to \mathcal{O}_F^\times$ ne dépend pas du choix de $f \in \mathcal{F}_\pi$.

Proposition 3.7. *Pour tout $n \geqslant 1$, l'extensions F_π^n/F est totalement ramifiée.*

Démonstration. Soit α un élément de E_f^n comme dans la preuve de la proposition 3.6. On a vu que α est racine de P et que F_π^n est un corps de rupture de P. Comme le terme constant de P est π, on a $N_{F_\pi^n/F}(\alpha)\pi$. Ainsi $v_{F_\pi^n}(\alpha) = v_{F_\pi^n}(\pi)/(q^n - q^{n-1})$. On en déduit que $v_{F_\pi^n}(\alpha) = 1$ et que F_π^n/F est totalement ramifiée. □

3.3 L'isomorphisme de réciprocité

On pose $L_\pi = F_\pi F^{\mathrm{nr}}$. On définit alors un morphisme de groupes rec_π de $F^\times$ vers $\mathrm{Gal}(L_\pi/F) \simeq \mathrm{Gal}(F^{\mathrm{nr}}/F) \times \mathrm{Gal}(F_\pi/F)$ en posant

$$\mathrm{rec}_\pi(\pi^n, a) = (\mathrm{Frob}_F^n, \chi_{\mathrm{LT}}^{-1}(a^{-1})) \in \mathrm{Gal}(F^{\mathrm{nr}}/F) \times \mathrm{Gal}(F_\pi/F).$$

Théorème 3.8. *1. On a $F^{\mathrm{ab}} = L_\pi$.*

2. Le morphisme rec_π ne dépend pas du choix de π.

3. De plus si E/F est une extension finie séparable, on a un diagramme commutatif

$$\begin{array}{ccc} E^\times & \xrightarrow{\quad N_{E/F} \quad} & F^\times \\ \downarrow{\scriptstyle \mathrm{rec}_{\pi_E}} & & \downarrow{\scriptstyle \mathrm{rec}_{\pi_F}} \\ \mathrm{Gal}(E^{\mathrm{ab}}/E) & \xrightarrow{\sigma \mapsto \sigma_{|F}} & \mathrm{Gal}(F^{\mathrm{ab}}/F)^{\mathrm{ab}}. \end{array}$$

Exercice 3.3. Vérifier que le théorème 3.8 implique les théorèmes 2.4 et 2.5.

Nous allons essentiellement démontrer le premier point du théorème et renvoyons à [Yos08] pour les autres assertions.

4 Ramification

4.1 La filtration de ramification inférieure

Soit E/F une extension finie galoisienne de corps locaux. On note G le groupe de Galois $\mathrm{Gal}(E/F)$. Pour $i \in \mathbb{Z}$, on pose

$$G_i \coloneqq \{\sigma \in G \mid \forall x \in \mathcal{O}_E,\ \sigma(x) - x \in \mathfrak{p}_E^{i+1}\}$$

(avec la convention $\mathfrak{p}_E^i = \mathcal{O}_E$ pour $i \leqslant 0$). Il s'agit d'un sous-groupe distingué de G. On a

$$G_{-1} = G, \quad G_0 = I(E/F), \quad \bigcap_{n\in\mathbb{Z}} G_n = \{1\}.$$

En particulier, puisque G est fini, il existe $n \geqslant 0$ tel que $G_n = \{1\}$. Notons $E_0 = E^{I(E/F)} \subset E$ la plus grande sous-extension non ramifiée de F contenue dans E. On sait alors que $\mathcal{O}_E = \mathcal{O}_{E_0}[\pi_E]$ pour une uniformisante π_E de E et on en déduit que, pour $i \geqslant 0$,

$$G_i = \{\sigma \in G_0 \mid \sigma(\pi_E) - \pi_E \in \mathfrak{p}_E^i\} = \left\{\sigma \in G_0 \mid v_E\left(\frac{\sigma(\pi_E)}{\pi_E} - 1\right) \geqslant i\right\}.$$

Si $\sigma \in G_0$, la classe de $\frac{\sigma(\pi_E)}{\pi_E}$ dans k_E ne dépend pas du choix de l'uniformisante π_E. Notons cet élément $\theta_0(\sigma) \in k_E^\times$. L'application θ_0 est un morphisme de groupes $G_0 \to k_E^\times$ dont le noyau est G_1. Le groupe quotient G_0/G_1 est donc isomorphe à un sous-groupe de $k_E^\times$. Le groupe G_0/G_1 est donc un groupe cyclique d'ordre premier à p_F.

Si $i \geqslant 1$ et $\sigma \in G_i$, on montre de même que la classe de l'élément $\frac{\sigma(\pi_E)}{\pi_E}$ dans U_E^i/U_E^{i+1} ne dépend pas du choix de π_E. On note cet élément $\theta_i(\sigma)$. L'application θ_i est alors un morphisme de groupes de G_i vers U_E^i/U_E^{i+1} dont le noyau est G_{i+1}. Ainsi le groupe G_i/G_{i+1} est isomorphe à un sous-groupe de $U_E^i/U_E^{i+1} \simeq \mathfrak{p}_E^i/\mathfrak{p}_E^{i+1} \simeq k_E$ et est donc isomorphe à un produit fini de groupes cycliques d'ordre p_F. En particulier on en conclut que le groupe G_1 est un pro-p_F-groupe et que le quotient G_0/G_1 est cyclique d'ordre premier à p_F. Le sous-groupe G_1 est donc l'unique p_F-Sylow de $I(E/F)$ est appelé *sous-groupe d'inertie sauvage*. Le quotient G_0/G_1 est appelé *groupe d'inertie modérée*.

4.2 La filtration de ramification des extensions de Luin–Tate

À titre d'exemple calculons la filtration de ramification des extension de Lubin–Tate F_π^n/F. Fixons donc $n \geqslant 1$ et posons $G = \mathrm{Gal}(F_\pi^n/F)$.

Tout d'abord on a $G_0 = G$ puisque l'extension est totalement ramifiée. On sait de plus que le caractère χ_{LT} induit un isomorphisme de G sur U_F/U_F^n. Comme U_F/U_F^n possède un unique p_F-Sylow, on a nécessairement $\chi_{\mathrm{LT}}(G_1) = U_F^1/U_F^n$. On fixe donc un élément $\sigma \in G_1$. On a $\chi_{\mathrm{LT}}(\sigma) = 1 + \pi^i a$ pour un entier $i \geqslant 1$ et un élément $a \in U_F$.

On fixe $f \in \mathcal{F}_\pi$ et $\lambda \in E_f^n$ un élément primitif, c'est-à-dire un élément tel que $[\pi]_f^{n-1}(\lambda) \neq 0$. On a déjà vu qu'un tel élément est nécessairement une uniformisante de F_π^n. On a alors

$$\sigma(\lambda) = [1 + \pi^i a]_f(\lambda) = \lambda +_{G_f} [\pi^i a]_f(\lambda).$$

L'élément $\beta \coloneqq [\pi^i a]_f(\lambda)$ est alors un élément de E_f^{n-i} vérifiant $[\pi]_f^{n-i-1}(\beta) \neq 0$. En particulier β est une uniformisante du corps F_π^{n-i}. Comme l'extension F_π^n/F_π^{n-i} est totalement ramifiée de degré q^i, on a nécessairement $v_{F_\pi^n}(\beta) = q^i$. Les relations $G_f(X, 0) = X$ et $G_f(0, Y) = Y$ impliquent qu'il n'y a pas de termes en X^n et Y^n pour $n \geqslant 2$ dans la loi de groupe formelle $G_f(X, Y)$. En particulier on peut écrire

$$G_f(X, Y) = X + Y + \sum_{i>0, j>0} c_{i,j} X^i Y^j$$

pour des éléments $c_{i,j} \in \mathcal{O}_F$. En conséquence,

$$\sigma(\lambda) - \lambda = \beta + \sum_{i>0, j>0} c_{i,j} \lambda^i \beta^j$$

ce qui implique que $v_{F_\pi^n}(\sigma(\lambda) - \lambda) = v_{F_\pi^n}(\beta) = q^i$. On en conclut que $\sigma \in G_m$ si et seulement si $m \leqslant q^i - 1$. La filtration des sous-groupes de ramification de $\mathrm{Gal}(F_\pi^n/F)$ est donc

$$\mathrm{Gal}(F_\pi^n/F) = G_0 = G_1 = \cdots = G_{q-1} \supsetneq G_q = \cdots = G_{q^2-1} \supsetneq G_{q^2} \cdots$$

En particulier les sauts de la filtration sont des entiers de la forme $q^i - 1$. Remarquons par ailleurs que $G_{q^i-1} = \mathrm{Gal}(F_\pi^n/F_\pi^i)$ pour $0 \leqslant i \leqslant n$, de sorte que $G_{q^i-1}/G_{q^{i+1}-1}$ est un groupe d'ordre q isomorphe à $(\mathbb{Z}/p\mathbb{Z})^f$ où $q = p^f$.

4.3 La filtration de ramification supérieure

Au vu du calcul de la section précédente, il semble naturel de renormaliser la filtration de ramification.

Soit E/F une extension galoisienne finie de corps locaux et posons $G = \mathrm{Gal}(E/F)$. Pour $t \in [-1, +\infty[$, on pose

$$G_t \coloneqq \{\sigma \in G \mid \forall x \in \mathcal{O}_E,\ v_E(\sigma(x) - x) \geqslant t\} = G_{\lceil t \rceil}$$

et, pour $u \in [-1, +\infty[$

$$\phi(u) \coloneqq \int_0^u \frac{dt}{[G_0 : G_t]}.$$

On vérifie que l'on a bien $\phi(-1) = -1$, $\phi(0) = 0$. De plus, si $E = F_\pi^n$, on a $\phi(q^i - 1) = i$ pour $0 \leqslant i \leqslant n$.

On définit la *filtration de ramification supérieure* sur G en posant, pour $u \in [-1, +\infty[$,

$$G^u \coloneqq G_{\phi(u)}.$$

On appelle *sauts de la filtration* les nombres réels u tels que $G^u \neq G^{u+\varepsilon}$ pour tout $\varepsilon > 0$ et on a alors $G^u/G^{u+\varepsilon} \simeq G_{\varphi(u)}/G_{\varphi(u)+1}$ pour $\varepsilon > 0$ assez petit. Remarquons que ces sauts sont automatiquement des nombres rationnels.

L'intérêt de la filtration de ramification supérieure est qu'elle est compatible avec le passage au quotient.

Proposition 4.1. *Soient $F \subset E \subset E'$ des extensions de corps locaux telles que E/F et E'/F sont galoisiennes finies. Alors pour tout $u \in [-1, +\infty[$, on a*

$$\mathrm{Gal}(E/F)^u = \mathrm{Im}(\mathrm{Gal}(E'/F)^u \to \mathrm{Gal}(E/F)).$$

Démonstration. Voir [Ser79, IV. Lemma 5]. □

En particulier si E_1/F et E_2/F sont deux extensions galoisiennes finies telles que $\mathrm{Gal}(E_1/F)^u = \{1\}$ et $\mathrm{Gal}(E_2/F)^u = \{1\}$, alors l'extension composée E_1E_2 a la même propriété.

Nous admettrons le résultat suivant, qui est équivalent au théorème de Kronecker–Weber local.

Théorème 4.2 (Hasse–Arf)**.** *Soit E/F une extension abélienne finie de corps locaux. Alors les sauts de la filtration de ramification supérieure de* $\mathrm{Gal}(E/F)$ *sont des entiers.*

Démonstration. Voir [Ser79, V. §7] ou [Sen69]. □

De façon équivalente, le théorème assure que pour une extension abélienne E/F, $\mathrm{Gal}(E/F)_i \neq \mathrm{Gal}(E/F)_{i+1}$ implique que i est de la forme $\phi(n)$ pour un entier $n \in \mathbb{Z}_{\geqslant -1}$.

On appelle *conducteur* d'une extension abélienne E/F le plus petit entier n tel que $\mathrm{Gal}(E/F)^{n+1} = \{1\}$ et on le note $n(E/F)$. Dans la pratique, c'est plutôt l'idéal $\mathfrak{f}(E/F) \coloneqq \mathfrak{p}^{n(E/F)}$ que l'on appelle conducteur de l'extension. La proposition 4.1 implique que si E_1/F et E_2/F sont deux extensions abéliennes, on a $n(E_1E_2/F) = \sup\{n(E_1/F), n(E_2/F)\}$. Étant donné un entier $n \geqslant 0$, il existe donc une plus grande extension abélienne (non finie cependant) de F de conducteur n.

4.4 Démonstration du théorème de Kronecker–Weber local

On fixe un corps local F, une uniformisante π de F. On rappelle que l'on a construit une tour d'extensions totalement ramifiées $(F_\pi^n)_{n\geqslant 1}$ de F. On veut montrer que

$$F^{\mathrm{ab}} = \bigcup_{n\geqslant 1} F^{\mathrm{nr}} F_\pi^n.$$

Commençons par démontrer l'inégalité suivante, qui découle du théorème 4.2. On note q le cardinal du corps résiduel de F.

Proposition 4.3. *Soit E/F une extension abélienne finie. Soit $E_0 \subset E$ la plus grande extensions non ramifiée de F. Soit $n \geqslant 0$ un entier tel que $\mathrm{Gal}(E/F)^{n+1} = \{1\}$. Alors on a*

$$[E : E_0] \leqslant q^n(q-1).$$

Démonstration. Posons $G = \mathrm{Gal}(E/F)$. D'après le théorème 4.3, les sauts de la filtration de ramification supérieure sont entiers. En particulier, pour tout $i \geqslant 0$, on a

$$G^i/G^{i+1} \simeq G_{\phi(i)}/G_{\phi(i)+1}.$$

Comme $G^0 = G_0$, il suffit donc de prouver que $|G_0/G_1| \leqslant q-1$ et $|G_i/G_{i+1}| \leqslant q$ pour tout $i \geqslant 1$.

Rappelons que nous avons construit un morphisme injectif de groupes $\theta_0 : G_0/G_1 \hookrightarrow k_E^\times$ dans la section 4.1. Si π_E est une uniformisante de E, on a $\theta_0(\tau) = \frac{\tau(\pi_E)}{\pi_E}$ modulo π_E. Si $\sigma \in G$, on a alors

$$\theta_0(\sigma\tau\sigma^{-1}) = \frac{\sigma\tau\sigma^{-1}(\pi_E)}{\pi_E} = \sigma\left(\frac{\tau(\sigma^{-1}(\pi_E))}{\sigma^{-1}(\pi_E)}\right).$$

Comme $\sigma^{-1}(\pi_E)$ est aussi une uniformisante de E, on a $\theta_0(\sigma\tau\sigma^{-1}) = \overline{\sigma}(\theta_0(\tau))$. Comme le groupe G est abélien, on a donc $\theta(\tau) = \overline{\sigma}(\theta_0(\tau))$ pour tout $\sigma \in \mathrm{Gal}(E/F)$. Comme le morphisme $\sigma \mapsto \overline{\sigma}$ de $\mathrm{Gal}(E/F)$ vers $\mathrm{Gal}(k_E/k_F)$ est surjectif (théorème 1.11), on a donc $\theta_0(G_0/G_1) \subset (k_E^\times)^{\mathrm{Gal}(k_E/k_F)} = k_F^\times$ et donc $|G_0/G_1| \leqslant q-1$.

Soit maintenant $i \geqslant 1$. Si $\tau \in G_i$, on pose $\theta_i(\tau) = \frac{\tau(\pi_E)}{\pi_E} - 1 \in \mathfrak{p}_E^i/\mathfrak{p}_E^{i+1}$. On montre de même que si $\sigma \in G$, on a $\sigma(\theta_i(\tau)) = \theta_i(\tau)$ pour tout $\tau \in G_i$, de sorte que $\theta_i(G_i/G_{i+1}) \subset (\mathfrak{p}_E^i/\mathfrak{p}_E^{i+1})^{\mathrm{Gal}(E/F)}$.

Inspectons un peu plus en détail l'action du groupe $\mathrm{Gal}(E/F)$ sur le quotient $\mathfrak{p}_E^i/\mathfrak{p}_E^{i+1}$. Si $\sigma \in G_0 = I(E/F)$ et $a \in \mathfrak{p}_E^i \smallsetminus \mathfrak{p}_E^{i+1}$, on peut écrire $a = b\pi_E^i$ avec

$b \in U_F$. On a alors $\sigma(a) = a\frac{\sigma(\pi_E^i)}{\pi_E^i}\frac{\sigma(b)}{b}$. Comme $\sigma \in I(E/F)$, on a $\frac{\sigma(b)}{b} \in 1 + \mathfrak{p}_E$ et $\frac{\sigma(\pi_E)}{\pi_E} \in \theta_0(\sigma)^i + \mathfrak{p}_E$. On en déduit donc que $\sigma(a) \in \theta_0(\sigma)^i a + \mathfrak{p}_E^{i+1}$. Autrement dit σ agit sur $\mathfrak{p}_E^i/\mathfrak{p}_E^{i+1}$ par multiplication par $\theta_0(\sigma)^i$. On en conclut que si $|G_0/G_1| \nmid i$, on a $(\mathfrak{p}_E^i/\mathfrak{p}_E^{i+1})^{I(E/F)} = \{0\}$, de sorte que $|G_i/G_{i+1}| = 1 \leqslant q$. Supposons donc que $|G_0/G_1| \mid i$. Alors $I(E/F)$ agit trivialement sur $\mathfrak{p}_E^i/\mathfrak{p}_E^{i+1}$ et on a $\theta_i(G_i/G_{i+1}) \subset (\mathfrak{p}_E^i/\mathfrak{p}_E^{i+1})^{\mathrm{Gal}(k_E/k_E)}$. On vérifie alors que l'application $\pi_E^i a \mapsto a$ est un isomorphisme $\mathrm{Gal}(k_E/k_F)$-équivariant de $\mathfrak{p}_E^i/\mathfrak{p}_E^{i+1}$ sur k_E et on conclut que

$$|G_i/G_{i+1}| \leqslant |k_E^{\mathrm{Gal}(k_E/k_F)}| = |k_F| = q. \qquad \square$$

On peut à présent démontrer le théorème de Kronecker–Weber local.

Théorème 4.4. *Soit E/F une extension abélienne finie. Alors $E \subset L_\pi$.*

Démonstration. Soit $n = n(E/F)$ le conducteur de E/F, de sorte que $\mathrm{Gal}(E/F)^{n+1} = \{1\}$. Posons $E' = EF_\pi^{n+1}$ et soit E_0 la sous-extensions maximale non ramifiée de E'. Comme E_0/F est non ramifiée et F_π^{n+1} totalement ramifiée, on a

$$[E_0F_\pi^{n+1} : E_0] = [F_\pi^{n+1} : F] = q^n(q-1).$$

Par ailleurs, comme E et F_π^{n+1} sont toutes deux de conducteurs $\leqslant n$, il en est de même de E'. On déduit donc de la proposition 4.3 que $[E' : E_0] \leqslant q^n(q-1)$. On a donc nécessairement $E' = E_0F_\pi^{n+1}$ et donc

$$E \subset E' \subset L_\pi = F^{\mathrm{nr}}F_\pi. \qquad \square$$

Références

[Sen69] Shankar Sen. On automorphisms of local fields. *Ann. of Math. (2)*, 90 :33–46, 1969.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Yos08] Teruyoshi Yoshida. Local class field theory via Lubin-Tate theory. *Ann. Fac. Sci. Toulouse Math. (6)*, 17(2) :411–438, 2008.