Ramification et points de petite hauteur

Arnaud Plessis

Normandie Université

THÈSE

Pour obtenir le diplôme de doctorat

Spécialité MATHEMATIQUES

Préparée au sein de l'Université de Caen Normandie

Ramification et points de petite hauteur

Présentée et soutenue par
Arnaud PLESSIS

Thèse soutenue publiquement le 18/10/2019 devant le jury composé de		
M. YURI BILU	Professeur des universités, Université Bordeaux 1 Sciences et Techno	Rapporteur du jury
Mme ILARIA DEL CORSO	Professeur des universités, Universita di Pisa	Rapporteur du jury
M. VINCENT BOSSER	Maître de conférences, Université Caen Normandie	Membre du jury
Mme SARA CHECCOLI	Maître de conférences, Institut Fourier	Membre du jury
M. AURÉLIEN GALATEAU	Maître de conférences HDR, Université de Franche Comté	Membre du jury
M. FRANCESCO AMOROSO	Professeur des universités, Université Caen Normandie	Directeur de thèse

Thèse dirigée par FRANCESCO AMOROSO, Laboratoire de Mathématiques 'Nicolas Oresme' (Caen)

UNIVERSITÉ CAEN NORMANDIE

Table des matières

Chapitre 0

Introduction

Cette thèse est composée de trois chapitres hors introduction. Dans le premier chapitre, on calculera explicitement les groupes de ramification d'une extension radicale et galoisienne de la forme $\mathrm{Gal}(F(\zeta_{p^r}, a^{1/p^s})/F)$, où p est un nombre premier impair, où $F/\mathbb{Q}_p$ est une extension non ramifiée, où $a \in F \backslash F^p$ et où r et s sont deux entiers positifs tels que $r \geq s$. Ce travail généralise celui de Viviani [46].

Dans le deuxième chapitre, on étudiera les corps $L \subset \overline{\mathbb{Q}}$ qui ne possèdent pas de point de petite hauteur, sauf 0 et les éventuelles racines de l'unité appartenant à L. On dira d'un corps ayant cette propriété qu'il possède (ou a) la propriété (B) (pour Bogomolov). Récemment, Galateau donna des exemples de corps ayant la propriété (B), sous une hypothèse assez restrictive. Le but de ce chapitre est de la supprimer. Ce résultat a donné lieu à la publication [34].

Dans le troisième chapitre, on s'intéressera à un cas particulier d'une conjecture de Rémond, qui permet de localiser les points de petite hauteur de $\mathbb{G}_m^n(\mathbb{Q}(\Gamma))$ où $\Gamma \subset \mathbb{G}_m^n(\overline{\mathbb{Q}})$ est un groupe de rang fini. On s'intéressera d'abord à cette conjecture dans le cas où $n = 1$ en généralisant un exemple non trivial allant dans le sens de celle-ci. On la généralisera ensuite en y incluant les variétés semi-abéliennes isotriviales. Cette généralisation permettra de relier entre eux plusieurs résultats déjà présents dans la littérature. On conclura ce chapitre en donnant un nouvel exemple non trivial de cette généralisation.

0.1 Groupes de ramification

Pour un corps local K, notons $\mathfrak{p}_K$ son idéal premier. Soit L/K une extension finie et galoisienne de corps locaux. Pour un entier $i \geq -1$, notons

$$\mathrm{Gal}(L/K)_i = \{\sigma \in \mathrm{Gal}(L/K) \mid \forall x \in \mathcal{O}_L,\ \sigma x \equiv x \mod \mathfrak{p}_L^{i+1}\}$$

le i-ième groupe de ramification de $\mathrm{Gal}(L/K)$. On dira que t est un saut de L/K si $\mathrm{Gal}(L/K)_t \neq \mathrm{Gal}(L/K)_{t+1}$.

Dans cette thèse, on s'intéressera aux extensions L/K qui sont galoisiennes, radicales et finies, i.e. $L = K(\zeta_{m_0}, a_1^{1/m_1}, \ldots, a_n^{1/m_n})$ avec $m_i \mid m_0$ pour tout i et $a_1, \ldots, a_n \in K^*$. En général, une telle extension n'est pas nécessairement abélienne. En fait, il s'agit des extensions galoisiennes non abéliennes les "plus

simples". Ce sont donc les "premières" extensions qui ne sont pas classifiées par la théorie des corps de classes locaux.

Dans cette section, p désignera, sauf indication contraire, un nombre premier impair. Plusieurs résultats concernant le calcul des sauts d'une extension L/K galoisienne et finie de corps locaux existent déjà dans la littérature :

i) si $K = \mathbb{Q}_p$ et L est une extension cyclotomique de $\mathbb{Q}_p$ [39, Chapitre IV,Proposition 18] ;

ii) si K est une extension finie de $\mathbb{Q}_p$ quelconque et L est le compositum de toutes les extensions de degré p sur K (cf [20, Proposition 15] pour le cas où $\zeta_p \in K$ et cf [12, Theorem 12] pour le cas général) ;

iii) si $K = \mathbb{Q}_p$ et $L = \mathbb{Q}_p\left(\sqrt[p^n]{\mathbb{Q}_p^*}\right)$ (avec $n \in \mathbb{N}^*$) [42, Theorem 6, Theorem 8] ;

iv) si $K = \mathbb{Q}_p$ et $L = \mathbb{Q}_p(\zeta_{p^r}, a^{1/p^s})$ avec $r \geq s \geq 0$ deux entiers et $a \in \mathbb{Z} \subset \mathbb{Z}_p$ tel que $v_p(a) \in \{0, 1\}$ [46, Theorem 5.8, Theorem 6.5].

En ce qui concerne la cas $p = 2$, Obus [33, Theorem 5.1] a calculé la borne supérieure de l'ensemble $\{\omega \geq -1 \mid \mathrm{Gal}(L/K)_{\psi_{L/K}(\omega)} \neq \{1\}\}$ (que l'on appelle le conducteur) en supprimant la condition technique $v_2(a) \in \{0, 1\}$, où $L = \mathbb{Q}_p(\zeta_{2^r}, a^{1/2^s})$ (avec $r \geq s$), où $K = \mathbb{Q}_p$ et où $\psi_{L/K}$ désigne la fonction ψ de Herbrand [39, Chapitre IV, §3]. Néanmoins, son approche ne permet ni de supprimer cette condition sur la valuation dans le cas où p est impair, ni de calculer toute la suite des groupes de ramification de l'extension $\mathbb{Q}_p(\zeta_{2^r}, a^{1/2^s})/\mathbb{Q}_p$.

Soit F une extension finie non ramifiée de $\mathbb{Q}_p$. Dans cette thèse, on se propose de généraliser le travail de Viviani [46] (point *iv*) ci-dessus) en déterminant la suite des groupes de ramification d'une extension de la forme $F(\zeta_{p^r}, a^{1/p^s})/F$ avec $r \geq s$ deux entiers positifs et $a \in F \backslash F^p$.

Outre les généralisations évidentes que l'on a faites par rapport à [46], notre approche nous permet de calculer des sauts que l'on ne peut calculer avec les méthodes employées dans [46]. Par exemple, on sera en mesure de déterminer l'unique saut de l'extension $\mathbb{Q}_p(\zeta_{p^2}, a^{1/p^4})/\mathbb{Q}_p(\zeta_{p^2}, a^{1/p^3})$.

Dans le chapitre 1, on montrera les théorèmes suivants :

Théorème 0.1.1. *Supposons que $p \mid v_F(a)$. Soient $r \geq s \geq 0$ des entiers tels que $r \geq 1$. Construisons par récurrence deux suites d'entiers positifs $(r^{(i)})_{i\geq 0}$ et $(s^{(i)})_{i\geq 0}$ comme suit : $r^{(0)} = s^{(0)} = 0$ et, pour $i \geq 0$,*

$$(r^{(i+1)}, s^{(i+1)}) = \begin{cases} (\min\{r, r^{(i)} + 1\}, s^{(i)}) \text{ si } s^{(i)} = s \\ (r^{(i)} + 1, s^{(i)}) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} = s^{(i)} \\ (r^{(i)}, s^{(i)} + 1) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} \neq s^{(i)} \end{cases}.$$

Alors :

i) les suites $(r^{(i)})_i$ et $(s^{(i)})_i$ sont croissantes et stationnaires de limites respectives r et s. Notons i_0 le plus petit entier i tel que $(r^{(i_0)}, s^{(i_0)}) = (r, s)$;

ii) les i_0 sauts de $F_{r,s}/F$ sont les

$$\tau_i = \begin{cases} t_1(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} = s \text{ ou si } r^{(i)} = s^{(i)} \\ t_2(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} \neq s^{(i)} \end{cases}$$

avec $i \in \{0, \dots, i_0 - 1\}$. *De plus, pour* $i \in \{0, \dots, i_0 - 1\}$, *on a*

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_i} = \mathrm{Gal}(F_{r,s}/F_{r^{(i)},s^{(i)}}).$$

Nous avons un résultat analogue, mais techniquement plus difficile, dans le cas où $p \nmid v_F(a)$.

Théorème 0.1.2. *Supposons que* $p \nmid v_F(a)$. *Soient* $r \geq s \geq 0$ *des entiers. Construisons par récurrence deux suites d'entiers positifs* $(r^{(i)})_i$ *et* $(s^{(i)})_i$ *comme suit :* $r^{(0)} = s^{(0)} = 0, r^{(1)} = 1$ *et* $s^{(1)} = 0$ *et, pour tout* $i \geq 1$,

$$(r^{(i+1)}, s^{(i+1)}) = \begin{cases} (\min\{r, r^{(i)} + 1\}, s^{(i)}) \text{ si } s^{(i)} = s \\ (r^{(i)}, s^{(i)} + 1) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} = r \\ (r^{(i)} + 1, s^{(i)}) \text{ si } s^{(i)} \neq s, \text{ si } r^{(i)} \neq r \text{ et si } r^{(i)} = s^{(i)} + 1 \\ (r^{(i)}, s^{(i)} + 1) \text{ si } s^{(i)} \neq s, \text{ si } r^{(i)} \neq r \text{ et si } r^{(i)} \neq s^{(i)} + 1 \end{cases}.$$

Alors :

i) les suites $(r^{(i)})_i$ *et* $(s^{(i)})_i$ *sont croissantes et stationnaires de limites respectives* r *et* s. *On note alors* i_0 *le plus petit entier* i *tel que* $(r^{(i_0)}, s^{(i_0)}) = (r, s)$;

ii) les i_0 *sauts de* $F_{r,s}/F$ *sont* $\tau_0 = t_1(1, 0) = 0$ *et les*

$$\tau_i = \begin{cases} t_1(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} = s \\ t_2(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s \text{ et } r^{(i)} = r \\ t_1(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s, \ r^{(i)} \neq r \text{ et } r^{(i)} = s^{(i)} + 1 \\ t_2(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s, \ r^{(i)} \neq r \text{ et } r^{(i)} \neq s^{(i)} + 1 \end{cases},$$

avec $i \in \{1, \dots, i_0 - 1\}$. *De plus, pour* $i \in \{0, \dots, i_0 - 1\}$, *on a :*

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_i} = \mathrm{Gal}(F_{r,s}/F_{r^{(i)},s^{(i)}}).$$

Nous allons maintenant décrire brièvement les différentes techniques utilisées pour montrer ces théorèmes. Soient $r \geq s$ deux entiers positifs, F une extension non ramifiée de $\mathbb{Q}_p$ et $a \in F \backslash F^p$. L'idée pour montrer les théorèmes 0.1.1 et 0.1.2 repose sur la construction explicite d'une tour d'extensions de la forme

$$K_0 = F \subset K_1 = F(\zeta_p) \subset \cdots \subset K_{i_0} = F(\zeta_{p^r}, a^{1/p^s})$$

ayant les propriétés suivantes :

i) K_{i+1}/K_i est une extension abélienne de degré p pour tout $i \geq 1$. Elle possède alors un unique saut τ_i pour tout $i \geq 1$.

ii) $0 < \tau_1 < \cdots < \tau_{i_0 - 1}$.

Une fois une telle tour construite, on conclura à l'aide d'une conséquence d'un théorème de Herbrand [39, Chapitre IV, §3, Lemme 5].

Pour calculer explicitement les τ_i, on utilisera un théorème de Hecke [16, Theorem 10.2.9] ainsi que plusieurs récurrences.

0.2 Minorations de la hauteur

0.2.1 État de l'art

Soient K un corps de nombres et notons $\mathcal{M}(K)$ l'ensemble des places de K. Pour $\nu \in \mathcal{M}(K)$, on note K_ν le complété de K en ν. Si ν est une place finie, on note d_ν le degré local $[K_\nu : \mathbb{Q}_p]$ où p est le premier au-dessous de ν. De la même façon, si ν est une place infinie, on note $d_\nu = [K_\nu : \mathbb{R}]$.

Définissons maintenant la hauteur logarithmique et absolue de Weil.

Définition 0.2.1 (Hauteur de Weil). *Soient $x \in \overline{\mathbb{Q}}^*$ et K un corps de nombres le contenant. On définit la hauteur logarithmique et absolue de Weil, notée* $\mathrm{h}(x)$, *par :*

$$\mathrm{h}(x) = \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in \mathcal{M}(K)} d_\nu \log \max\{1, |x|_\nu\}.$$

Cette hauteur est bien définie puisque $|x|_\nu = 1$ pour toute place ν, sauf pour un nombre fini d'entre elles. De plus, elle ne dépend pas du corps contenant x [10, §1.5]. Pour simplifier, on la désignera simplement par le mot "hauteur".

Cette hauteur possède d'autres propriétés importantes comme celles ci-dessous [10, Proposition 1.5.17, Lemma 1.5.18] :

Proposition 0.2.2. *Soient $x \in \overline{\mathbb{Q}}$ et $\lambda \in \mathbb{Z}$. Alors* $\mathrm{h}(x^\lambda) = |\lambda|\mathrm{h}(x)$ *et, pour tout* $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *on a* $\mathrm{h}(\sigma x) = \mathrm{h}(x)$.

La hauteur est aussi utilisée pour prouver la finitude d'un ensemble de points algébriques via le théorème fondamental ci-dessous :

Théorème 0.2.3 (Northcott, §1.6, [10]). *Fixons $B, D > 0$. Alors l'ensemble*

$$\{\alpha \in \overline{\mathbb{Q}}^* \mid \mathrm{h}(\alpha) \leq B \text{ et } [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq D\}$$

est fini.

Notons μ_∞ l'ensemble des racines de l'unité de $\overline{\mathbb{Q}}$. Soit $\alpha \in \overline{\mathbb{Q}}^*$ tel que $\mathrm{h}(\alpha) = 0$. Alors pour tout entier $k \geq 1$,

$$\mathrm{h}(\alpha^k) = k\,\mathrm{h}(\alpha) = 0.$$

Par le théorème 0.2.3, la suite $(\alpha^k)_{k \geq 1}$ ne possède alors qu'un nombre fini de termes distincts. Ainsi, $\alpha \in \mu_\infty$. La réciproque étant triviale, on en déduit la proposition ci-dessous :

Proposition 0.2.4 (Kronecker). *Soit $\alpha \in \overline{\mathbb{Q}}^*$. Alors* $\mathrm{h}(\alpha) = 0$ *si et seulement si* $\alpha \in \mu_\infty$.

En théorie des hauteurs, la conjecture suivante est très importante :

Conjecture 0.2.5 (Lehmer, §13, [31]). *Il existe $c > 0$ tel que pour tout $x \in \overline{\mathbb{Q}}^* \backslash \mu_\infty$,*

$$\mathrm{h}(x) \geq \frac{c}{[\mathbb{Q}(x) : \mathbb{Q}]}.$$

Actuellement, le meilleur résultat connu allant dans la direction de cette conjecture est dû à Dobrowolski :

Théorème 0.2.6 (Dobrowolski, [21]). *Il existe $c > 0$ tel que pour tout $x \in \overline{\mathbb{Q}}^* \backslash \mu_\infty$,*

$$\mathrm{h}(x) \geq \frac{c}{[\mathbb{Q}(x) : \mathbb{Q}]} \left(\frac{\log \log(3[\mathbb{Q}(x) : \mathbb{Q}])}{\log(2[\mathbb{Q}(x) : \mathbb{Q}])} \right)^3.$$

Propriété (B)

Afin de mieux comprendre la conjecture de Lehmer, Bombieri et Zannier ont introduit la notion de propriété (B) (pour Bogolomov) ci-dessous.

Définition 0.2.7 ([11]). *On dira qu'un corps $K \subset \overline{\mathbb{Q}}$ satisfait (ou a) la propriété (B) s'il existe un réel $T_0 > 0$ tel que l'ensemble*

$$\mathcal{A}(T_0) = \{\alpha \in K^* | \ \mathrm{h}(\alpha) \leq T_0\}$$

ne contienne que les racines de l'unité.

Nous allons maintenant nous intéresser à certaines familles de corps qui ont la propriété (B). D'après le théorème 0.2.3, les corps de nombres ont la propriété (B). Ainsi, la notion de propriété (B) est intéressante uniquement lorsque l'on considère des extensions infinies de $\mathbb{Q}$. Citons quelques exemples de corps ayant la propriété (B). Le premier concerne les corps totalement réels (un corps K est dit totalement réel si pour tout plongement $\sigma : K \hookrightarrow \mathbb{C}$, son image est dans $\mathbb{R}$).

Théorème 0.2.8 (Schinzel, [37] et Smyth, [45]). *Soit K un corps totalement réel. Alors pour tout $x \in K^* \backslash \{-1, 1\}$, on a :*

$$\mathrm{h}(x) \geq \frac{1}{2} \log \left(\frac{1 + \sqrt{5}}{2} \right).$$

Le prochain exemple est un analogue p-adique du théorème 0.2.8. On dit que $\alpha \in \overline{\mathbb{Q}}$ est un nombre totalement p-adique si p est totalement décomposé dans $\mathbb{Q}(\alpha)$. Le corps $\mathbb{Q}^{tp}$ constitué de tous les nombres algébriques totalement p-adique est alors galoisienne sur $\mathbb{Q}$.

Théorème 0.2.9 (Bombieri-Zannier, Theorem 2, [11]). *Soient $L/\mathbb{Q}$ une extension galoisienne et p un nombre premier. Si L peut être plongé dans une extension finie de $\mathbb{Q}_p$, alors L a la propriété (B).*

La clôture abélienne $\mathbb{Q}^{ab}$ de $\mathbb{Q}$ possède également la propriété (B). Plus précisément :

Théorème 0.2.10 (Amoroso-Dvornicich, [4]). *Pour tout $x \in (\mathbb{Q}^{ab})^* \backslash \mu_\infty$:*

$$\mathrm{h}(x) \geq (\log 5)/12.$$

Dans [5, Theorem 1.2], les auteurs ont étendu le théorème 0.2.10 en montrant que pour tout corps de nombres K de degré d sur $\mathbb{Q}$ et tout $x \in (K^{ab})^* \backslash \mu_\infty$,

$$\mathrm{h}(x) > 3^{-d^2-2d-6}.$$

Notons $\mathbb{G}_m$ le groupe multiplicatif. Par le théorème de Kronecker-Weber :

$$\mathbb{Q}^{ab} = \mathbb{Q}(\mu_\infty) = \mathbb{Q}((\mathbb{G}_m)_{\mathrm{tors}}).$$

Dans [26, Theorem 1], Habegger a montré l'analogue du théorème 0.2.10 dans le cas des courbes elliptiques. Plus précisément, si E est une courbe elliptique définie sur $\mathbb{Q}$ sans multiplication complexe, alors $\mathbb{Q}(E_{\text{tors}})$ a la propriété (B), où E_{tors} désigne l'ensemble des points de torsion de E. Notons que si E est à multiplication complexe, alors $\mathbb{Q}(E_{\text{tors}}) \subset K^{ab}$ pour un certain corps de nombres K. Ainsi, $\mathbb{Q}(E_{\text{tors}})$ a aussi la propriété (B) dans le cas où E est à multiplication complexe [5, Theorem 1.8].

Une conjecture de Rémond

Notons $\mathbb{G}$ le groupe multiplicatif $\mathbb{G}_m^n$ de dimension n ou une variété abélienne définie sur un corps de nombres k. Notons $\hat{\mathrm{h}}$ une hauteur sur $\mathbb{G}(\overline{k})$ (avec $k = \mathbb{Q}$ si $\mathbb{G} = \mathbb{G}_m^n$) définie de la manière suivante : dans le cas où $\mathbb{G} = \mathbb{G}_m^n$, la hauteur $\hat{\mathrm{h}}(P)$ d'un point $P = (a_1, \ldots, a_n)$ est la somme des hauteurs de Weil $\mathrm{h}(a_1) + \cdots + \mathrm{h}(a_n)$. Dans le cas où $\mathbb{G}$ est une variété abélienne, $\hat{\mathrm{h}}$ désignera la hauteur canonique associée à un fibré en droite ample et symétrique L que l'on fixe. Notons $[n] : \mathbb{G} \to \mathbb{G}$ la multiplication par un entier n. Pour un sous-groupe Γ de $\mathbb{G}(\overline{k})$, notons

$$\Gamma_{\text{sat}} = \{g \in \mathbb{G}(\overline{k}) \mid \exists n \in \mathbb{N}\backslash\{0\}, [n].g \in \mathrm{End}(\mathbb{G}).\Gamma\}$$

(où $\mathrm{End}(\mathbb{G}).\Gamma$ désigne le groupe engendré par les éléments de la forme $\phi(\gamma)$ avec $\phi \in \mathrm{End}(\mathbb{G})$ et $\gamma \in \Gamma$) le groupe saturé de Γ. Si $\mathrm{End}(\mathbb{G}) = \mathbb{Z}$ (comme c'est le cas si, par exemple, $\mathbb{G} = \mathbb{G}_m$ ou $\mathbb{G} = E$ est une courbe elliptique non CM), alors Γ_{sat} est le groupe de division de Γ, i.e. $\{g \in \mathbb{G}(\overline{k}) \mid \exists n \in \mathbb{N}\backslash\{0\}, [n].g \in \Gamma\}$. On définit aussi le rang de Γ comme étant égal à $\dim_{\mathbb{Q}} \Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$.

Récemment, Rémond a énoncé une conjecture très générale [36, Conjecture 3.4] sur la minoration de la hauteur $\hat{\mathrm{h}}$. Nous nous intéressons à un cas particulier de cette conjecture :

Conjecture 0.2.11. *Soit $\Gamma \subset \mathbb{G}(\overline{k})$ un groupe de rang fini. Alors il existe une constante $c_\Gamma > 0$ telle que $\hat{\mathrm{h}}(P) \geq c_\Gamma$ pour tout $P \in \mathbb{G}(k(\Gamma))\backslash\Gamma_{\text{sat}}$.*

Cette conjecture donne un énoncé apparemment plus fort que celui qu'on peut déduire directement de [36, Conjecture 3.4], où la condition "$P \notin \Gamma_{\text{sat}}$" est remplacée par la condition logiquement plus forte "P est Γ-transverse" (rappelons que, en suivant [36], une sous-variété V de $\mathbb{G}$ est dite Γ-transverse si elle n'est contenue dans aucun translaté d'un sous-groupe algébrique connexe B de A tel que $B \neq A$ par un point de Γ_{sat}). Cependant, [36, Théorème 3.7] avec $\varepsilon = 0$ (ce qui est possible d'après le dernier paragraphe de [36, section 3]) montre que l'on peut affaiblir la condition sur P.

0.2.2 Généralisation d'un résultat de Galateau

Rappelons que K^{ab} a la propriété (B) si K est un corps de nombres [5, Theorem 1.8]. On peut alors se demander si l'hypothèse "K est un corps de nombres" peut-être remplacée par "K a la propriété (B)". Cela n'est pas possible en général. Dans [3, Theorem 5.3], les auteurs donnent un contre-exemple en prenant pour K le corps $\mathbb{Q}^{tr}$ (le compositum de toutes les extensions totalement réelles), qui possède la propriété (B) par le théorème 0.2.8, et montrent que $\mathbb{Q}^{tr}(i) \subset K^{ab}$ n'a pas la propriété (B).

Définition 0.2.12. *Soient $K \subset \overline{\mathbb{Q}}$ un corps et ν une place finie de K. On dit qu'une extension algébrique L/K a un degré local borné en ν s'il existe un entier positif $B(\nu)$ tel que $[L_w : K_\nu] \leq B(\nu)$ pour toute place finie w de L étendant ν.*

Soit $K/\mathbb{Q}$ une extension galoisienne ayant un degré local en un premier p. Supposons que la suite $(B(p))_p$ est majorée. Alors $\mathrm{Gal}(K/\mathbb{Q})$ est d'exposant fini [14, Theorem 1] et a donc la propriété (B) [15, Corollary 2].

On a vu que si K est un corps ayant la propriété (B), alors K^{ab} n'a pas forcément la propriété (B). On peut se poser la même question en remplaçant "corps ayant la propriété (B)" par "corps ayant un degré local borné en un premier p". Cela conduit au problème suivant dont une réponse partielle a été donnée dans [3] :

Problème 0.2.13. *Si une extension algébrique $L/\mathbb{Q}$ a un degré local borné en un premier p fixé, est-il vrai que L^{ab} a la propriété (B) ? Plus généralement, si p est un nombre premier et $(L_i)_i$ une suite de corps algébriques ayant tous un degré local borné en p, est-il vrai que le compositum des L_i^{ab} a la propriété (B) ?*

De manière générale, la seconde affirmation est fausse. Pour p fixé, il suffit de prendre la suite $(L_i)_i$ de tous les corps de nombres. Ainsi, le compositum des L_i^{ab} est égal à $\overline{\mathbb{Q}}$ qui n'a pas la propriété (B).

Dans cette thèse, on imposera en plus que la suite $([L_i : \mathbb{Q}])_i$ est majorée. On étudiera donc le problème suivant.

Problème 0.2.14. *Soit $(K_n)_n$ une suite de corps de nombres telle que la suite $([K_n : \mathbb{Q}])_n$ est majorée. Est-il vrai que le compositum de tous les K_n^{ab} a la propriété (B) ?*

Pour un corps de nombres K, on note $H(K)$ le corps de Hilbert de K et $\mathcal{O}_K$ son anneau des entiers. Galateau a considéré un cas particulier de cette question. Il a montré que :

Théorème 0.2.15 (Galateau, §5, [25])**.** *Soit $(K_n/\mathbb{Q})_n$ une suite d'extensions finies telle que la suite $([K_n : \mathbb{Q}])_n$ est majorée. Si :*

i) $K_n/\mathbb{Q}$ est galoisienne pour tout n ;

ii) il existe un premier p inerte dans tous les K_n ;

iii) les discriminants des K_n sont deux à deux premiers entre eux ;

alors le compositum L de tous les $H(K_n)$ satisfait la propriété (B).

La condition *iii)* est assez restrictive. Par un théorème de Dirichlet (cf [24, Chapter III, Theorem 22]), cela implique que tout premier $q \in \mathbb{Q}$ doit être ramifié dans au plus un des K_n. Galateau a conjecturé qu'à l'aide d'une étude locale, on pouvait se passer de cette condition.

Notre résultat principal consiste à supprimer les conditions *i)* et *iii)* du théorème 0.2.15 ainsi qu' à affaiblir la condition *ii)* en supposant seulement qu'il existe un unique idéal premier de $\mathcal{O}_{K_n}$ au-dessus de p. En particulier, on autorise p à être ramifié dans K_n.

Théorème 0.2.16. *Soit $(K_n/\mathbb{Q})_n$ une suite d'extensions finies telle que la suite $([K_n : \mathbb{Q}])_n$ est majorée. Supposons qu'il existe un premier $p \in \mathbb{Q}$ tel que pour tout n, il existe un unique idéal premier $\mathfrak{p}_n$ de $\mathcal{O}_{K_n}$ au-dessus de p. Alors le compositum L de tous les $H(K_n)$ satisfait la propriété (B).*

Nous allons maintenant généraliser ce théorème en considérant des corps de rayon à la place des corps de Hilbert. Comme auparavant, soit K un corps de nombres.

Définition 0.2.17. *Un K- module est un produit formel $\mathfrak{m} = \mathfrak{m}_f\infty$ où ∞ désigne le produit formel de tous les plongements réels de K et $\mathfrak{m}_f$ (appelée la partie finie) est un idéal non-nul de $\mathcal{O}_K$.*

À partir de maintenant, $\mathfrak{m} = \mathfrak{m}_f\infty$ désigne un K-module et on confondra souvent $\mathfrak{m}$ et $\mathfrak{m}_f$. De ce module, on peut construire deux groupes importants. Le premier, est le groupe abélien $J_{\mathfrak{m}}(K)$ composé de tous les idéaux fractionnaires de K premier à $\mathfrak{m}_f$ et le second, noté $P_{\mathfrak{m}}(K)$, est le sous-groupe des idéaux principaux de $J_{\mathfrak{m}}(K)$ engendré par a/b où

i) $a, b \in \mathcal{O}_K \backslash \{0\}$ et $\text{pgcd}((a), (b)) = 1$,

ii) $a \equiv b \mod \mathfrak{m}$,

iii) $\sigma\left(\frac{a}{b}\right) > 0$ pour tout plongement réel σ de K.

Notons $Cl_{\mathfrak{m}}(K)$ le groupe quotient $J_{\mathfrak{m}}(K)/P_{\mathfrak{m}}(K)$. Remarquons que dans le cas où $\mathfrak{m} = (1)$, on retrouve le groupe des classes classique. De plus, de bonnes propriétés du groupe des classes classique restent valables pour $Cl_{\mathfrak{m}}(K)$. Par exemple :

Théorème 0.2.18 (Chapter 6, Proposition 1.8, [32])**.** *Soit K un corps de nombres. Le groupe $Cl_{\mathfrak{m}}(K)$ est fini.*

On a aussi le théorème de Takagi ci-dessous :

Théorème 0.2.19 (Takagi)**.** *Soit K un corps de nombres. Alors il existe un unique corps $K_{\mathfrak{m}}$, abélien sur K, tel que $\text{Gal}(K_{\mathfrak{m}}/K) \simeq Cl_{\mathfrak{m}}(K)$. De plus, tout premier $\mathfrak{p}$ de $\mathcal{O}_K$ ne divisant pas $\mathfrak{m}$ est non ramifié dans L et son degré résiduel $f_{\mathfrak{p}}(L|K)$ est égal à l'ordre de $\mathfrak{p}$ dans $Cl_{\mathfrak{m}}(K)$.*

Le corps $K_{\mathfrak{m}}$ du théorème ci-dessus est appelé *corps de rayon de module* $\mathfrak{m}$ de K. Il est intéressant de remarquer que dans le cas $K = \mathbb{Q}$ et $\mathfrak{m} = m\mathbb{Z}$, on a alors que $K_{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$. Comme on le verra plus tard, les corps de rayons sont, comme pour les corps cyclotomiques, des extensions abéliennes de K "maximales" dans le sens où toute extension abélienne de K est contenue dans un corps de rayon.

Une autre manière de définir le corps de Hilbert de K est de le voir comme étant l'extension abélienne maximale non-ramifiée de K (i.e. que tous les idéaux premiers de $\mathcal{O}_K$ sont non ramifiés dans $H(K)$). Cependant, dans la preuve du théorème 0.2.16, on utilisera uniquement le fait que $\mathfrak{p}_n$ ne se ramifie pas dans $H(K_n)$ pour tout n. On peut donc autoriser certains idéaux premiers à se ramifier, ce que permet les corps de rayons d'après le théorème 0.2.19. Ainsi, le théorème 0.2.16 se généralise bien si l'on remplace la terminologie "corps de Hilbert" par "corps de rayons". Dans sa version la plus générale, on obtient que

Théorème 0.2.20. *Soient K un corps de nombres et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Soit $(K_n/K)_{n\in\mathbb{N}}$ une suite d'extensions finies telle que la suite $([K_n : K])_n$ est majorée et telle que pour tout n, il existe un unique idéal premier $\mathfrak{p}_n$ de $\mathcal{O}_{K_n}$ au-dessus de $\mathfrak{p}$. Fixons $M \geq 1$ un entier. Pour $n \in \mathbb{N}$, notons*

$$\Omega_n = \{\textit{idéaux } \mathfrak{m} \subset \mathcal{O}_{K_n} |\ \exists m \leq M,\ p \nmid m,\ \textit{et } \mathfrak{m} \textit{ au-dessus de } m\}.$$

Pour $\mathfrak{m} \in \Omega_n$, notons $K_{n,\mathfrak{m}}$ le corps de rayon de K_n associé à $\mathfrak{m}$. Alors le compositum L de tous les $K_{n,\mathfrak{m}}$ a la propriété (B).

Pour retrouver le théorème 0.2.16, il suffit de prendre $K = \mathbb{Q}$, $\mathfrak{p} = p\mathbb{Z}$ et $M = 1$.

Techniques utilisées dans la preuve du théorème 0.2.20

Soient K un corps de nombres et L/K une extension algébrique. Choisissons un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ au-dessus d'un premier rationnel p. Pour montrer le théorème 0.2.20, on s'appuie sur une méthode désormais classique, à savoir qu'un corps L a la propriété (B) si la suite $([L_\nu : \mathbb{Q}_p])_{\nu|\mathfrak{p}}$, où ν parcourt l'ensemble des places de L au-dessus de $\mathfrak{p}$, est majorée. Pour montrer cela, on utilisera des propriétés sur les corps de rayon issues de la théorie des groupes et de la théorie algébrique des nombres (le lien entre ces théories apparaissent dans le théorème 0.2.19).

0.2.3 Autour d'une conjecture de Rémond

Dans cette thèse, nous avons d'abord étudié la conjecture 0.2.11 dans le cas où $\mathbb{G} = \mathbb{G}_m$. Elle se réécrit alors comme suit :

Conjecture 0.2.21. *Soit Γ un groupe de rang fini. Alors il existe une constante $c_\Gamma > 0$ telle que pour tout $\alpha \in \mathbb{Q}(\Gamma)^* \backslash \Gamma_{\mathrm{sat}}$, on a $\mathrm{h}(\alpha) \geq c_\Gamma$.*

Cette conjecture affirme qu'en dehors de Γ_{sat}, il n'y a pas de point de petite hauteur dans $\mathbb{Q}(\Gamma)^*$. Tout groupe de rang fini est inclus dans un groupe de la forme G_{sat} [22], où G est un groupe de type fini. Ainsi, pour montrer la conjecture 0.2.21, il suffit de la montrer pour les groupes de la forme G_{sat}.

On ne connaît que peu de résultats non-triviaux dans la direction de cette conjecture, même dans des cas très particuliers. Le cas où $\Gamma = \{1\}_{\mathrm{sat}}$ est le groupe des racines de l'unité a été traité dans [4] et les auteurs ont montré que $c_\Gamma = (\log 5)/12$ convenait.

Cependant, on ne sait toujours pas si cette conjecture est vraie pour tout autre groupe de la forme $\Gamma = \langle b \rangle_{\mathrm{sat}}$ avec $b \in \mathbb{Z} \backslash \{-1, 0, 1\}$. En particulier, on ne sait pas si les points de petite hauteur de $\mathbb{Q}^{ab}(2^{1/2}, 2^{1/3}, \dots)$ sont dans $\langle 2 \rangle_{\mathrm{sat}}$.

Pour un nombre premier p, on définit le groupe p-saturé de Γ comme étant le groupe :

$$\Gamma_{\mathrm{sat},p} = \left\{ g \in \overline{\mathbb{Q}}^* \mid \exists n \in \mathbb{N}^*, g^{p^n} \in \Gamma \right\}.$$

Il y a peu, Amoroso a montré que la conjecture 0.2.21 est vérifiée pour le groupe $\Gamma = \langle 2 \rangle_{\mathrm{sat},3}$. Plus généralement, il a montré [2, Theorem 3.3] :

Théorème 0.2.22 (Amoroso)**.** *Soient $b \geq 2$ un entier et $p \geq 3$ un nombre premier. Supposons que $p \nmid b$ et que $p^2 \nmid (b^{p-1} - 1)$. Alors $\mathrm{h}(\alpha) \geq \min\left\{ \frac{1}{3\mathrm{h}(b)}, \frac{\log(p/2)}{2p^2} \right\}$ pour tout $\alpha \in \mathbb{Q}(\langle b \rangle_{\mathrm{sat},p})^* \backslash \langle b \rangle_{\mathrm{sat}}$.*

Un ingrédient indispensable dans la preuve de ce théorème repose sur l'étude du dernier saut de la suite des groupes de ramification de $\mathrm{Gal}\big(\mathbb{Q}_p(\zeta_{p^r}, b^{1/p^s})/\mathbb{Q}_p\big)$ avec $r \geq s$ deux entiers positifs. Remarquons que cette étude a déjà été faite par Viviani. Comme on a déjà généralisé les résultats de Viviani (cf les théorèmes 0.1.1 et 0.1.2), cela nous permet de supprimer les conditions techniques du théorème 0.2.22 et de pouvoir considérer des corps de nombres à la place de $\mathbb{Q}$.

Théorème 0.2.23. *Soient F un corps de nombres, $a \in F^*\backslash(F^*)^p$ et p un nombre premier impair ne divisant pas le discriminant de F. Alors il existe $c > 0$ tel que $\mathrm{h}(\alpha) \geq c$ pour tout $\alpha \in F(\langle a\rangle_{\mathrm{sat},p})^*\backslash\langle a\rangle_{\mathrm{sat}}$.*

Remarquons que dans le cas $F = \mathbb{Q}$, la condition technique "p ne divise pas le discriminant de F" est vide puisque le discriminant de $\mathbb{Q}$ vaut 1. Le théorème 0.2.23 est donc bien une généralisation du théorème 0.2.22.

Une généralisation de la conjecture 0.2.11

Comme l'a déjà montré Rémond dans [36, section 5], la conjecture 0.2.11 ne peut s'énoncer dans le cas plus général où $\mathbb{G}$ est une variété semi-abélienne. Son contre-exemple repose sur le fait que $\mathbb{G}$ puisse posséder des points de Ribet (le lecteur souhaitant lire la définition d'un point de Ribet pourra voir [27]). Dans le cas où $\mathbb{G}$ est une variété semi-abélienne isotriviale, les points de Ribet sont des points de torsion. Par conséquent, il semble raisonnable de proposer la conjecture suivante :

Conjecture 0.2.24. *La conjecture 0.2.11 reste valable pour les variétés abéliennes isotriviales.*

À partir de maintenant, considérons des variétés abéliennes isotriviales de la forme $\mathbb{G} = \mathbb{G}_m \times A$ où A est une variété abélienne définie sur un corps de nombres k. Notons $\hat{\mathrm{h}}(\alpha, Q)$ la hauteur d'un point $(\alpha, Q) \in \mathbb{G}$ comme étant la somme $\mathrm{h}(\alpha) + \hat{\mathrm{h}}(Q)$.

La conjecture 0.2.24 permet d'interpréter différents résultats déjà présents dans la littérature comme des cas particuliers de celle-ci. Le premier concerne le cas où $\Gamma = (\mathbb{G}_m)_{\mathrm{tors}} \times \{0\}$. On a alors $\Gamma_{\mathrm{sat}} = \mathbb{G}_{\mathrm{tors}}$ et $k(\Gamma) = k((\mathbb{G}_m)_{\mathrm{tors}}) \subset k^{ab}$. La conjecture 0.2.24 prédit donc l'existence d'un $c > 0$ tel que $\mathrm{h}(\alpha) + \hat{\mathrm{h}}(P) \geq c$ pour tout

$$(\alpha, P) \in \mathbb{G}(k((\mathbb{G}_m)_{\mathrm{tors}}))\backslash\mathbb{G}_{\mathrm{tors}}.$$

Clairement, cette affirmation est contenue dans les deux affirmations suivantes :

i) il existe $c > 0$ telle que $\mathrm{h}(\alpha) \geq c$ pour tout $\alpha \in \mathbb{G}_m(k^{ab})\backslash(\mathbb{G}_m)_{\mathrm{tors}}$;

ii) il existe $c > 0$ telle que $\hat{\mathrm{h}}(P) \geq c$ pour tout $P \in A(k^{ab})\backslash A_{\mathrm{tors}}$.

Le point *i)* est un théorème dû à Amoroso et Zannier [5] et le point *ii)* a été prouvé par Baker et Silverman [6, Theorem 0.1]. La conjecture 0.2.24 est donc satisfaite dans ce cas.

Le second exemple concerne le cas où $\mathbb{G} = \mathbb{G}_m \times E$, avec E une courbe elliptique définie sur $\mathbb{Q}$, et $\Gamma = \{1\} \times E_{\mathrm{tors}}$. À nouveau, $\Gamma_{\mathrm{sat}} = \mathbb{G}_{\mathrm{tors}}$. De plus, $\mathbb{Q}(\Gamma) = \mathbb{Q}(E_{\mathrm{tors}})$. La conjecture 0.2.24 prédit donc l'existence d'un $c > 0$ tel que $\mathrm{h}(\alpha) + \hat{\mathrm{h}}(P) \geq c$ pour tout

$$(\alpha, P) \in \mathbb{G}(\mathbb{Q}(E_{\mathrm{tors}}))\backslash\mathbb{G}_{\mathrm{tors}},$$

ce qui correspond précisément à [26, Corollary 1].

Dans les deux exemples cités ci-dessus, on a $\Gamma_{\mathrm{sat}} = \mathbb{G}_{\mathrm{tors}}$. Dans cette thèse, on se propose de donner un exemple de la conjecture 0.2.24 dans le cas où $\Gamma_{\mathrm{sat}} \neq \mathbb{G}_{\mathrm{tors}}$.

Théorème 0.2.25. *Soient E une courbe elliptique et $p \geq 5$ un premier tel que E a une réduction supersingulière en p. Soit $b \geq 2$ un entier tel que $p \nmid b$ et $p^2 \nmid (b^{p-1}-1)$. Alors il existe $c_{\Gamma,E} > 0$ tel que $\hat{\mathrm{h}}(\alpha, P) \geq c_{\Gamma,E}$ pour tout $(\alpha, P) \in \mathbb{G}(\mathbb{Q}(\Gamma))\backslash\Gamma_{\mathrm{sat}}$ où $\Gamma = \langle b\rangle_{\mathrm{sat},\{p\}} \times \{0\}$ et où $\mathbb{G} = \mathbb{G}_m \times E$.*

Remarquons que $\Gamma_{\mathrm{sat}} = \langle b\rangle_{\mathrm{sat}} \times E_{\mathrm{tors}} \neq \mathbb{G}_{\mathrm{tors}}$. Clairement, il suffit de montrer les deux assertions ci-dessous pour en déduire le théorème 0.2.25 :

i) il existe $c > 0$ telle que $\mathrm{h}(\alpha) \geq c$ pour tout $\alpha \in \mathbb{G}_m(\mathbb{Q}(\Gamma))\backslash\langle b\rangle_{\mathrm{sat}}$;

ii) il existe $c > 0$ telle que $\hat{\mathrm{h}}(P) \geq c$ pour tout $P \in E(\mathbb{Q}(\Gamma))\backslash E_{\mathrm{tors}}$.

Remarquons que le point $i)$ correspond précisément au théorème 0.2.22. Par conséquent, il nous reste à montrer :

Théorème 0.2.26. *Soient E une courbe elliptique et $p \geq 5$ un premier tel que E a une réduction supersingulière en p. Soit $b \geq 2$ un entier tel que $p \nmid b$ et $p^2 \nmid (b^{p-1}-1)$. Alors il existe $c > 0$ tel que $\hat{\mathrm{h}}(P) \geq c$ pour tout $P \in E(\mathbb{Q}(\langle b\rangle_{\mathrm{sat},p}))\backslash(E(\mathbb{Q}(\zeta_p)) \cap E_{\mathrm{tors}})$.*

Remarquons que le résultat que l'on obtient est apparemment légèrement plus précis car on retire seulement $E(\mathbb{Q}(\zeta_p)) \cap E_{\mathrm{tors}} \subset E(\mathbb{Q}(\langle b\rangle_{\mathrm{sat},p}) \cap E_{\mathrm{tors}}$. Cependant, on montrera dans le fait 3.2.13 que cette inclusion est en fait une égalité.

Techniques utilisées dans la preuve des théorèmes 0.2.23 et 0.2.26

Reprenons les notations du théorème 0.2.23. Soient $L \subset F(\langle a\rangle_{\mathrm{sat},p})$ une extension galoisienne et finie de F et $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$ au-dessus de p. Pour montrer ce théorème, notre méthode repose sur deux arguments : le premier est une inégalité métrique, *à la Dobrowolski*.

Notons $P(X) = (\sigma X)^{p^3} - X^{p^3}$, où $\sigma \in \mathrm{Gal}(F(\langle a\rangle_{\mathrm{sat},p})/F)$. Soit $\alpha \in L$. On montrera alors que

$$|P(\alpha)|_{\mathfrak{P}} \leq p^{-1} \max\{1, |\alpha|_{\mathfrak{P}}\}^{p^3} \ \max\{1, |\sigma\alpha|_{\mathfrak{P}}\}^{p^3}.$$

Si $P(\alpha) \neq 0$, alors par la formule du produit, on en déduira une minoration de $\mathrm{h}(\alpha)$ indépendante de α et de L. Dans le cas où $P(\alpha) = 0$, cela signifiera que α est, à une division par un élément de Γ_{sat} près, dans le corps fixé par $\langle\sigma\rangle$. Par une méthode de la descente, on en déduira que soit α est dans le saturé de Γ, soit que l'on peut minorer $\mathrm{h}(\alpha)$ par une constante ne dépendant ni de α, ni de L.

Enfin, pour montrer notre théorème 0.2.26, on utilisera encore une inégalité *à la Dobrowolski*. Ensuite, on montrera par des techniques d'équidistribution que si un point P a une hauteur "suffisamment petite", alors P est la somme de l'un de ses conjugués et d'un point de torsion. On peut ensuite effectuer un analogue elliptique de la méthode de la descente faite dans la preuve du théorème 0.2.23 pour en déduire notre dernier théorème.

Chapitre 1

Groupes de ramification

1.1 Résultats principaux.

Dans ce chapitre, fixons un premier p impair. Tous les corps considérés seront des extensions finies de $\mathbb{Q}_p$. Pour un corps K, notons p_K son idéal premier. Pour un entier $i \geq -1$, notons

$$\mathrm{Gal}(L/K)_i = \{\sigma \in \mathrm{Gal}(L/K) \mid \forall x \in \mathcal{O}_L,\ \sigma x \equiv x \mod \mathfrak{p}_L^{i+1}\}$$

le i-ième groupe de ramification de $\mathrm{Gal}(L/K)$. On dira que t est un saut de L/K si $\mathrm{Gal}(L/K)_t \neq \mathrm{Gal}(L/K)_{t+1}$.

Il est bien connu que $\mathrm{Gal}(L/K)_i$ est un sous-groupe normal de $\mathrm{Gal}(L/K)$ pour tout i, que $\mathrm{Gal}(L/K)_j = \{1\}$ pour tout j assez grand et que $\mathrm{Gal}(L/K)_1$ est le groupe trivial si et seulement si L/K est une extension modérément ramifiée (pour d'autres résultats, le lecteur pourra consulter [39, Chapitre IV]).

Fixons un corps local F qui est non ramifié sur $\mathbb{Q}_p$ et $a \in (F^*)\backslash(F^*)^p$. Notons v_F la valuation normalisée de F.

Définition 1.1.1. *Pour des entiers $r, s \geq 0$, notons $F_{r,s}$ le corps $F(\zeta_{p^r}, a^{1/p^s})$.*

Dans ce chapitre, nous nous proposons de calculer les groupes de ramification d'une extension de la forme $F_{r,s}/F$ où $r \geq s$ sont deux entiers positifs. Pour cela, nous allons calculer explicitement, pour tous entiers [1] r et s, le saut des extensions $F_{r,s}/F_{r-1,s}$ et $F_{r,s}/F_{r,s-1}$ en séparant le cas $p \mid v_F(a)$ (cf théorème 1.3.5) du cas $p \nmid v_F(a)$ (cf théorème 1.3.6).

Une fois ces sauts calculés, on sera en mesure de construire deux suites $(r^{(i)})_i$ et $(s^{(i)})_i$ de telle sorte que si τ_i, avec $i \geq 0$, désigne le $(i+1)$-ième plus petit saut de $F_{r,s}/F$, alors $\mathrm{Gal}(F_{r,s}/F)_{\tau_i} = \mathrm{Gal}(F_{r,s}/F_{r^{(i)},s^{(i)}})$ (cf théorème 1.1.5 si $p \mid v_F(a)$ et théorème 1.1.6 si $p \nmid v_F(a)$). De plus, les τ_i sont explicitement calculables.

Soit K un corps local. Pour un nombre $\alpha \in K^*$, on notera α^{1/p^s}, pour tout $s \geq 0$, une racine p^s-ième de α telle que $(\alpha^{1/p^s})^p = \alpha^{1/p^{s-1}}$.

Lemme 1.1.2. *Pour tous $r, s \geq 0$ avec $r \geq 1$, l'extension $F_{r,s}/F$ est totalement ramifiée de degré $(p-1)p^{r+s-1}$.*

[1] on n'a pas nécessairement que $r \geq s$

Démonstration. Comme $F/\mathbb{Q}_p$ est non ramifié et que $\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p$ est totalement ramifié de degré $(p-1)p^{r-1}$, on en déduit que $F(\zeta_{p^r})/F$ est une extension totalement ramifiée de degré $(p-1)p^{r-1}$. Ainsi, pour montrer le lemme, il reste à montrer que $F_{r,s}/F(\zeta_{p^r})$ est totalement ramifié de degré p^s.

Commençons par calculer le degré. Comme $a \in (F^*)\backslash(F^*)^p$ et que $\zeta_p \notin F$, une conséquence d'un théorème de Schinzel [38, Theorem 2], appliquée à $k = F$, $m = p$ et $n = p^r$, montre alors que $a \notin F(\zeta_{p^r})\backslash F(\zeta_{p^r})^p$. D'un lemme de Capelli [29, Chapitre 6, Theorem 9.1], il s'ensuit alors que

$$[F_{r,s} : F(\zeta_{p^r})] = p^s.$$

Montrons maintenant que $F_{r,s}/F(\zeta_{p^r})$ est totalement ramifié. Supposons par l'absurde que ce ne soit pas le cas. Les sous-corps de $F_{r,s}/F(\zeta_{p^r})$ sont les $F_{r,g}$, avec $g \in \{0, \ldots, s\}$ [1, Theorem 2.1]. Ainsi, $F_{r,1}/F(\zeta_{p^r})$ est une extension non ramifiée. La structure des extensions non ramifiées [13, Chapter 1, section 7] montre alors que $F_{r,1} = F(\zeta_m)$ pour un certain entier m. En particulier, $F_{1,1}/F$ est abélien. Comme $\zeta_p \notin F$, le théorème de Schinzel cité précédemment [38, Theorem 2], appliqué à $K = F$ et à $n = p$, montre que $a \in F(\zeta_p)^p$, ce qui est absurde. Ceci prouve le lemme. □

Remarque 1.1.3. Soient r, r', s, s' quatre entiers positifs avec $r, r' \geq 1$. En appliquant le lemme précédent avec r, s et avec r', s', on obtient que $[F_{r,s} : F] = (p-1)p^{r+s-1}$ et $[F_{r',s'} : F] = (p-1)p^{r'+s'-1}$. De la multiplicativité des degrés, on en déduit alors que

$$[F_{r,s} : F_{r',s'}] = p^{r-r'+s-s'}.$$

De plus, comme $F_{r,s}/F$ est totalement ramifié d'après le lemme 1.1.2, il s'ensuit que $F_{r,s}/F_{r',s'}$ est également totalement ramifié.

Lemme 1.1.4. *Soient r, s des entiers positifs avec $r \geq 1$. Alors $F_{r,s}/F_{r-1,s}$ possède un unique saut que l'on note $t_1(r,s)$. De même, si $s \geq 1$, alors $F_{r,s}/F_{r,s-1}$ possède un unique saut que l'on note $t_2(r,s)$.*

Démonstration. Commençons par montrer que $F_{r,s}/F_{r-1,s}$ possède un unique saut. Si $r = 1$, alors l'extension $F_{1,s}/F_{0,s} = F(\zeta_p, a^{1/p^s})/F(a^{1/p^s})$ est de degré au plus $p-1$. Le lemme 1.1.2, appliqué à $\alpha = a$ et à $r = s$, montre que $F_{s,s}/F$ est totalement ramifié. En particulier, $F_{1,s}/F_{0,s}$ est totalement ramifié. Comme elle est modérément ramifié, elle possède alors un unique saut qui est égal à 0.

Supposons maintenant que $r \geq 2$. En appliquant la remarque 1.1.3 avec $r' = r-1$ et $s' = s$, il s'ensuit que $F_{r,s}/F_{r-1,s}$ est une extension galoisienne totalement ramifiée de degré p. Elle possède donc aussi un unique saut.

De la même remarque 1.1.3, appliquée à $r' = r$ et à $s' = s-1$, il s'ensuit que $F_{r,s}/F_{r,s-1}$ est une extension galoisienne (car $\zeta_p \in F_{r,s-1}$) de degré p. Elle possède donc également un unique saut. □

Nous nous proposons dans un premier temps de calculer les sauts $t_1(r,s)$ et $t_2(r,s)$ (théorèmes 1.3.5 et 1.3.6). Nous allons ensuite en déduire par récurrence (section 1.4) les sauts et les groupes de ramification associés à l'extension $F_{r,s}/F$.

Théorème 1.1.5. *Supposons que $p \mid v_F(a)$. Soient $r \geq s \geq 0$ des entiers tels que $r \geq 1$. Construisons par récurrence deux suites d'entiers positifs $(r^{(i)})_{i\geq 0}$ et $(s^{(i)})_{i\geq 0}$ comme suit : $r^{(0)} = s^{(0)} = 0$ et, pour $i \geq 0$,*

$$(r^{(i+1)}, s^{(i+1)}) = \begin{cases} (\min\{r, r^{(i)}+1\}, s^{(i)}) \text{ si } s^{(i)} = s \\ (r^{(i)}+1, s^{(i)}) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} = s^{(i)} \\ (r^{(i)}, s^{(i)}+1) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} \neq s^{(i)} \end{cases}.$$

Alors :

i) les suites $(r^{(i)})_i$ et $(s^{(i)})_i$ sont croissantes et stationnaires de limites respectives r et s. Notons i_0 le plus petit entier i tel que $(r^{(i_0)}, s^{(i_0)}) = (r, s)$;

ii) les i_0 sauts de $F_{r,s}/F$ sont les

$$\tau_i = \begin{cases} t_1(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} = s \text{ ou si } r^{(i)} = s^{(i)} \\ t_2(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} \neq s^{(i)} \end{cases}$$

avec $i \in \{0, \ldots, i_0 - 1\}$. De plus, pour $i \in \{0, \ldots, i_0 - 1\}$, on a

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_i} = \mathrm{Gal}(F_{r,s}/F_{r^{(i)},s^{(i)}}).$$

Nous avons un résultat analogue, mais techniquement plus difficile, dans le cas où $p \nmid v_F(a)$.

Théorème 1.1.6. *Supposons que $p \nmid v_F(a)$. Soient $r \geq s \geq 0$ des entiers. Construisons par récurrence deux suites d'entiers positifs $(r^{(i)})_i$ et $(s^{(i)})_i$ comme suit : $r^{(0)} = s^{(0)} = 0, r^{(1)} = 1$ et $s^{(1)} = 0$ et, pour tout $i \geq 1$,*

$$(r^{(i+1)}, s^{(i+1)}) = \begin{cases} (\min\{r, r^{(i)}+1\}, s^{(i)}) \text{ si } s^{(i)} = s \\ (r^{(i)}, s^{(i)}+1) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} = r \\ (r^{(i)}+1, s^{(i)}) \text{ si } s^{(i)} \neq s, \text{ si } r^{(i)} \neq r \text{ et si } r^{(i)} = s^{(i)}+1 \\ (r^{(i)}, s^{(i)}+1) \text{ si } s^{(i)} \neq s, \text{ si } r^{(i)} \neq r \text{ et si } r^{(i)} \neq s^{(i)}+1 \end{cases}.$$

Alors :

i) les suites $(r^{(i)})_i$ et $(s^{(i)})_i$ sont croissantes et stationnaires de limites respectives r et s. On note alors i_0 le plus petit entier i tel que $(r^{(i_0)}, s^{(i_0)}) = (r, s)$;

ii) les i_0 sauts de $F_{r,s}/F$ sont $\tau_0 = t_1(1, 0) = 0$ et les

$$\tau_i = \begin{cases} t_1(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} = s \\ t_2(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s \text{ et } r^{(i)} = r \\ t_1(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s, \ r^{(i)} \neq r \text{ et } r^{(i)} = s^{(i)}+1 \\ t_2(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s, \ r^{(i)} \neq r \text{ et } r^{(i)} \neq s^{(i)}+1 \end{cases},$$

avec $i \in \{1, \ldots, i_0 - 1\}$. De plus, pour $i \in \{0, \ldots, i_0 - 1\}$, on a :

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_i} = \mathrm{Gal}(F_{r,s}/F_{r^{(i)},s^{(i)}}).$$

1.2 Rappels et préliminaires.

Pour une extension galoisienne L/K de groupe de Galois G, il est en général difficile de calculer les G_i (et même les sauts). En revanche, si H est un sous-groupe de G, il est facile de calculer les H_i en fonction des G_i. Plus précisément, on a $H_i = G_i \cap H$ pour tout $i \geq 0$ [39, Chapitre IV, Proposition 2].

Il est également possible, dans le cas où H est un sous groupe normal de G, de calculer explicitement les quotients $(G/H)_i$. Avant d'expliciter la formule, étendons de manière naturelle la notion de groupes de ramification en posant, pour tout réel $u \geq -1$, $G_u = G_{\lceil u \rceil}$ où $\lceil u \rceil$ désigne la partie entière supérieure de u. On peut ainsi définir la fonction $\phi_{L/K}$ de Herbrand, valable pour tout $u \geq -1$, par :

$$\phi_{L/K}(u) = \begin{cases} u & \text{si } -1 \leq u < 0 \\ \int_0^u [G_0 : G_t]^{-1} \mathrm{d}t & \text{si } u \geq 0 \end{cases}.$$

C'est une bijection de $[-1, +\infty[$ dans lui-même [39, Chapitre IV, Proposition 12]. Notons $\psi_{L/K}$ sa bijection réciproque.

Théorème 1.2.1 (Herbrand, Chapitre IV, §3, Lemme 5, [39])**.** *Soit $K \subset L \subset M$ une tour d'extensions finies telle que L/K et M/K sont galoisiennes. Notons G le groupe de Galois de M/K et H celui de M/L. Pour tout $v \geq 0$, posons $u = \psi_{M/L}(v)$. Alors* $\mathrm{Gal}(L/K)_u \simeq (G/H)_v = G_u H/H$.

Ce théorème va nous permettre de calculer les sauts d'une tour d'extensions en fonction des sauts de chaque étage, dès lors que chaque étage possède un unique saut et que ces sauts forment une suite strictement croissante.

Lemme 1.2.2. *Soit $K \subset L \subset M$ une tour d'extensions finies. Supposons que M/K et L/K sont galoisiennes. Notons $t_1 < \cdots < t_n$ les sauts de M/L. Supposons que L/K possède un unique saut que l'on note t et que $t < t_1$. Alors les sauts de M/K sont $t, t_1, \ldots, t_n$. De plus, pour tout $j \geq t+1$, on a* $\mathrm{Gal}(M/K)_j = \mathrm{Gal}(M/L)_j$.

Démonstration. Posons $G = \mathrm{Gal}(M/K)$ et $H = \mathrm{Gal}(M/L)$. Montrons d'abord que $G = G_t$. Comme $t < t_1$, il s'ensuit que $\psi_{M/L}(x) = x$ pour tout $x \leq t+1$ (car $\phi_{M/L}(x) = x$ si $x \leq t_1$). Ainsi, on déduit du théorème 1.2.1 que

$$G/H = (G/H)_t = G_t H/H \simeq G_t/(G_t \cap H).$$

Or, $H \cap G_t = H_t$ et $H_t = H$ puisque $t < t_1$. Ainsi, $G/H \simeq G_t/H$ et donc $G = G_t$ puisque $\#G = \#G_t$ et que $G_t \subset G$.

Comme L/K possède un unique saut, on a, toujours d'après le théorème 1.2.1 :

$$\{1\} = \mathrm{Gal}(L/K)_{t+1} \simeq G_{t+1} H/H.$$

Ceci montre donc que $G_{t+1} \subset H \neq G = G_t$. On en conclut que t est le premier saut de G. De plus, pour tout $i \geq t+1$, on a $H_i = G_i \cap H = G_i$, ce qui permet de montrer que les autres sauts de G sont $t_1, \ldots, t_n$. □

Corollaire 1.2.3. *Soient $n \geq 2$ et $K_0 \subset \cdots \subset K_n$ une tour d'extensions finies. On suppose que pour tout i, K_i/K_0 est galoisienne et K_{i+1}/K_i admet un unique saut que l'on note t_i. Si $t_0 < \cdots < t_{n-1}$, alors les sauts de K_n/K_1 sont $t_0, \ldots, t_{n-1}$ et* $\mathrm{Gal}(K_n/K_1)_{t_i} = \mathrm{Gal}(K_n/K_i)$ *pour tout i .*

Démonstration. Supposons que pour un entier $l \leq n-1$, les sauts de K_n/K_l soient $t_l, \ldots, t_{n-1}$ et que pour tout $j \geq l$, on a $\mathrm{Gal}(K_n/K_l)_{t_j} = \mathrm{Gal}(K_n/K_j)$ (par hypothèse, c'est vrai pour $l = n-1$). En appliquant alors le lemme 1.2.2 à $M = K_n$, à $L = K_l$ et à $K = K_{l-1}$, on en déduit que les sauts de K_n/K_{l-1} sont les $t_{l-1}, \ldots, t_{n-1}$ et que pour tout $j \geq l$,

$$\mathrm{Gal}(K_n/K_{l-1})_{t_j} = \mathrm{Gal}(K_n/K_l)_{t_j} = \mathrm{Gal}(K_n/K_j).$$

De plus, par définition de t_{l-1}, on a $\mathrm{Gal}(K_n/K_{l-1})_{t_{l-1}} = \mathrm{Gal}(K_n/K_{l-1})$. On en déduit le corollaire en procédant par récurrence. □

À partir de maintenant, on utilisera les notations suivantes. Pour un corps local K, notons v_K la valuation normalisée sur K et $\mathfrak{p}_K$ son idéal premier. Pour une extension finie L/K (non nécessairement galoisienne), on note $\mathcal{D}_{L/K}$ la différente de cette extension. Si L/K est galoisienne, il existe un lien entre sa différente et le cardinal de ses groupes de ramification. Ce lien est résumé dans la proposition ci-dessous.

Proposition 1.2.4 (Chapitre IV, Proposition 4, [39]). *Pour toute extension galoisienne et finie de corps locaux L/K, on a :*

$$v_L(\mathcal{D}_{L/K}) = \sum_{i=0}^{\infty} (\#\mathrm{Gal}(L/K)_i - 1).$$

En particulier, si L/K est une extension galoisienne totalement ramifiée de degré d et qu'elle possède un unique saut t, alors

$$v_L(\mathcal{D}_{L/K}) = (d-1)(t+1). \tag{1.1}$$

Nous allons maintenant étudier les sauts de certaines extensions radicales et principalement les extensions de Kummer d'exposant p. Commençons par déterminer le saut d'une extension cyclique de degré p.

Définition 1.2.5. *Soient K un corps local et $\alpha \in K \backslash K^p$. Notons*

i) pour tout entier $i \geq 0$, $U_K^{(i)} = \{x \in \mathcal{O}_K |\ x \equiv 1 \mod \mathfrak{p}_K^i\}$;

ii) $c_K(\alpha) = \sup\{i \in \mathbb{N}^* |\ \exists x \in K^*, \alpha x^{-p} \in U_K^{(i)}\}$.

Avec cette définition, il est immédiat que $c_K(\alpha x^{-p}) = c_K(\alpha)$ pour tout $x \in K^*$.

Remarque 1.2.6. Soient K un corps local et $\alpha \in K \backslash K^p$. Supposons qu'il existe $y \in K^*$ tel que $\alpha y^{-p} \in \mathcal{O}_K$ et $\alpha y^{-p} \equiv 1 \mod \mathfrak{p}_{F_{1,s}}$ (i.e. $c_K(\alpha) \geq 1$). En particulier, $v_K(\alpha y^{-p}) = 0$ et donc, $v_K(\alpha) = p v_K(y)$. Par conséquent, si $p \nmid v_K(\alpha)$, alors $c_K(\alpha) = 0$.

De cette remarque, on obtient alors le théorème suivant :

Théorème 1.2.7 (Hecke, Theorem 10.2.9, [16]). *Soient K un corps local tel que $\zeta_p \in K$ et $\alpha \in K \backslash K^p$. Si $K(\sqrt[p]{\alpha})/K$ est totalement ramifié, alors*

$$v_{K(\sqrt[p]{\alpha})}(\mathcal{D}_{K(\sqrt[p]{\alpha})/K}) = (p-1)\left(\frac{pe(K|\mathbb{Q}_p)}{p-1} - c_K(\alpha) + 1\right).$$

Dans [16, Theorem 10.2.9], le lecteur pourra remarquer que le a introduit dans le (3) de ce théorème correspond à notre $c_K(\alpha)$. En combinant (1.1) et le théorème 1.2.7, on en déduit que

Corollaire 1.2.8. *Soient K un corps local tel que $\zeta_p \in K$ et $\alpha \in K\backslash K^p$. Supposons que $K(\sqrt[p]{\alpha})/K$ soit totalement ramifié. Alors son (unique) saut vaut*

$$\frac{pe(K|\mathbb{Q}_p)}{p-1} - c_K(\alpha).$$

Proposition 1.2.9. *Soient $K/\mathbb{Q}_p$ une extension finie telle que $\zeta_p \in K$ et $\alpha \in K\backslash K^p$. Notons également $K_s = K(\alpha^{1/p^s})$ et t_s le saut de K_s/K_{s-1}. Si K_1/K est ramifié, alors la suite $(t_s)_{s\geq 1}$ est strictement croissante.*

Démonstration. Commençons par montrer que K_s/K_{s-1} est totalement ramifié pour tout $s \geq 1$. Supposons par l'absurde qu'il existe s tel que K_s/K_{s-1} ne soit pas ramifié. L'extension K_s/K n'est donc pas totalement ramifiée. Comme $p \neq 2$, les sous-corps de cette extension sont les K_g avec $g = 0, \ldots, s$ [1, Theorem 2.1]. Il s'ensuit que K_1/K est non ramifiée, ce qui est absurde par hypothèse.

Notons $\phi_s = \phi_{K_s/K_{s-1}}$ et $c_s = c_{K_s}(\alpha^{1/p^s})$. Soit $y \in K_s$ tel que

$$\alpha^{1/p^s} y^{-p} \in U_{K_s}^{(c_s)}.$$

En passant à la norme $N_s := N_{K_s/K_{s-1}}$, il s'ensuit que $\alpha^{1/p^{s-1}} N_s(y)^{-p} \in N_s(U_{K_s}^{(c_s)})$. D'après [39, Proposition 4, Chapitre V], on a donc que $\alpha^{1/p^{s-1}} N_s(y)^{-p} \in U_{K_{s-1}}^{(\lfloor \phi_s(c_s) \rfloor)}$. D'où $\lfloor \phi_s(c_s) \rfloor \leq c_{s-1}$. Par ailleurs, d'après le corollaire 1.2.8, on obtient que

$$t_s = \frac{p}{p-1} e(K_{s-1}|\mathbb{Q}_p) - c_{s-1} \tag{1.2}$$

$$t_{s+1} = \frac{p}{p-1} e(K_s|\mathbb{Q}_p) - c_s. \tag{1.3}$$

Si $c_s \leq t_s$, alors $\phi_s(c_s) = c_s$ et donc $c_s \leq c_{s-1}$. Comme $e(K_s|\mathbb{Q}_p) > e(K_{s-1}|\mathbb{Q}_p)$, il s'ensuit de (1.2) et (1.3) que $t_{s+1} > t_s$.

Si $c_s > t_s$, alors $\phi_s(c_s) = t_s + (c_s - t_s)/p$. D'où $t_s + (c_s - t_s)/p < c_{s-1} + 1$ ou encore

$$c_s < t_s + p(c_{s-1} + 1 - t_s).$$

En utilisant (1.2) et (1.3), on a, après quelques calculs, que

$$t_{s+1} + p\left(\frac{pe(K_{s-1}|\mathbb{Q}_p)}{p-1} - \frac{e(K_s|\mathbb{Q}_p)}{p-1}\right) > (2p-1)t_s - p.$$

Comme $\alpha \in K^*\backslash (K^*)^p$, alors K_s/K_{s-1} est une extension de degré p. De plus, elle est totalement ramifié d'après le début de la preuve. Il s'ensuit que $e(K_s|\mathbb{Q}_p) = pe(K_{s-1}|\mathbb{Q}_p)$. Il en résulte donc que $t_{s+1} > (2p-1)t_s - p$. Comme $(2p-1)t_s - p \geq t_s$ puisque $t_s \geq 1$, on en déduit alors la proposition.

□

Nous allons maintenant étudier les sauts d'une extension galoisienne de groupe de Galois $(\mathbb{Z}/p\mathbb{Z})^2$.

Proposition 1.2.10. *Soient K_1 et K_2 deux corps locaux et $K = K_1 \cap K_2$. On suppose que K_1/K et K_2/K sont galoisiennes, que K_1K_2/K est totalement ramifié et que K_1/K, K_2/K, K_1K_2/K_2 et K_1K_2/K_1 possèdent tous un unique saut que l'on note respectivement t_1, t_2, t_1' et t_2'. Notons $d_i = [K_i : K]$. Alors*

i) $d_2(d_1-1)t_1 + (d_2-1)t_2' = d_1(d_2-1)t_2 + (d_1-1)t_1'$.

ii) De plus, si $d_1 = d_2 = p$ *et* $t_1' < t_2'$, *alors*

$$\begin{cases} t_1' = t_1 \\ t_2' = pt_2 + (1-p)t_1. \end{cases}$$

Démonstration. i) Comme K_1K_2/K est totalement ramifié, on déduit de la formule [39, Chapitre III, Proposition 8] sur la composée de deux différentes que

$$\begin{aligned} v := v_{K_1K_2}(\mathcal{D}_{K_1K_2/K}) &= v_{K_1K_2}(\mathcal{D}_{K_1K_2/K_1}) + [K_1K_2 : K_1]v_{K_1}(\mathcal{D}_{K_1/K}) \\ &= v_{K_1K_2}(\mathcal{D}_{K_1K_2/K_2}) + [K_1K_2 : K_2]v_{K_2}(\mathcal{D}_{K_2/K}). \end{aligned}$$

Comme $[K_1K_2 : K_1] = d_2$ et $[K_1K_2 : K_2] = d_1$, on a, en utilisant quatre fois (1.1), que :

$$\begin{aligned} v &= (d_2-1)(t_2'+1) + d_2(d_1-1)(t_1+1) \\ &= (d_1-1)(t_1'+1) + d_1(d_2-1)(t_2+1). \end{aligned} \tag{1.4}$$

Le *i)* s'ensuit en comparant ces égalités.

ii) Supposons maintenant que $d_1 = d_2 = p$ et que $t_1' < t_2'$. Comme $\mathrm{Gal}(K_1K_2/K)$ est d'ordre p^2, il ne peut alors avoir qu'au plus deux sauts. De plus,

$$G := \mathrm{Gal}(K_1K_2/K) = \mathrm{Gal}(K_1K_2/K_1)\mathrm{Gal}(K_1K_2/K_2).$$

Ainsi, $G_{t_1'} = G$, $G_{t_1'+1} = \mathrm{Gal}(K_1K_2/K_1)$ et $G_{t_2'+1} = \{id\}$. Les sauts de K_1K_2/K sont donc t_1' et t_2' puisqu'ils sont distincts par hypothèse. En utilisant la proposition 1.2.4 avec $L = K_1K_2$, on en déduit que

$$\begin{aligned} v &= (p^2-1)(t_1'+1) + (p-1)(t_2' - t_1') \\ &= (p-1)(pt_1' + p + 1 + t_2'). \end{aligned}$$

Par ailleurs, (1.4) s'écrit (en factorisant par $d_1 - 1 = d_2 - 1 = p - 1$)

$$\begin{aligned} v &= (p-1)(t_2' + 1 + p(t_1+1)) \\ &= (p-1)(t_1' + 1 + p(t_2+1)). \end{aligned}$$

En comparant ces trois relations, on obtient que $pt_1 + t_2' = pt_2 + t_1' = pt_1' + t_2'$ et donc que $t_1 = t_1'$. De plus, $t_2' = pt_2 + t_1' - pt_1' = pt_2 + (1-p)t_1$, ce qui montre *ii)*. □

La proposition 1.2.11 n'est qu'un cas particulier de la proposition 1.2.10, mais qui se révèle être le point clé pour prouver les théorèmes 1.1.5 et 1.1.6.

Proposition 1.2.11. *Soient $r \geq 2$ et $s \geq 1$ des entiers. Alors*

i) $t_1(r,s) - t_2(r,s) = p(t_1(r,s-1) - t_2(r-1,s))$;

ii) si $t_1(r,s) < t_2(r,s)$, *alors*

$$t_1(r,s) = t_1(r,s-1);$$

iii) si $t_2(r,s) < t_1(r,s)$, *alors*

$$t_2(r,s) = t_2(r-1,s).$$

Démonstration. i) Appliquons la proposition 1.2.10 à $K_1 = F_{r,s-1}$ et à $K_2 = F_{r-1,s}$. Alors $K_1K_2 = F_{r,s}$ et $K_1 \cap K_2 = F_{r-1,s-1}$. D'après la remarque 1.1.3, appliquée avec $s-1$ au lieu de s, avec $r' = r-1$ ($r' \geq 1$ car $r \geq 2$) et avec $s' = s-1$, on en déduit que $K_1/K_1 \cap K_2 = F_{r,s-1}/F_{r-1,s-1}$ est galoisien (car $\zeta_p \in F_{r-1,s-1}$) de degré p. De même, la remarque 1.1.3, appliquée avec $r-1$ au lieu de r, avec $r' = r-1$ et avec $s' = s-1$, montre que $K_2/K_1 \cap K_2 = F_{r-1,s}/F_{r-1,s-1}$ est galoisien de degré p. Avec les notations de la proposition 1.2.10, on obtient que

$$\begin{cases} d_1 = d_2 = p \\ t_1 = t_1(r,s-1),\ t_2 = t_2(r-1,s) \\ t_1' = t_1(r,s),\ t_2' = t_2(r,s). \end{cases}$$

De plus, en appliquant de nouveau la remarque 1.1.3 avec $r' = r-1$ et avec $s' = s-1$, on obtient alors que $K_1K_2/K_1 \cap K_2 = F_{r,s}/F_{r-1,s-1}$ est totalement ramifié. Ainsi, d'après le i) de la proposition 1.2.10, $pt_1 + t_2' = pt_2 + t_1'$ ou encore $t_2' - t_1' = p(t_2 - t_1)$, ce qui correspond à la formule souhaitée.

ii) Gardons les notations du i). Supposons maintenant que $t_1(r,s) < t_2(r,s)$, i.e. $t_1' < t_2'$. Comme $d_1 = d_2 = p$, on déduit du *ii*) de la proposition 1.2.10 que $t_1' = t_1$, ce qui correspond à la formule souhaitée.

iii) La preuve du *iii*) est analogue à celle du point *ii*) en prenant cette fois-ci $K_1 = F_{r-1,s}$ et $K_2 = F_{r,s-1}$. Nous la réécrivons pour la commodité du lecteur.

Appliquons la proposition 1.2.10 à $K_1 = F_{r-1,s}$ et à $K_2 = F_{r,s-1}$. On obtient alors que $K_1K_2 = F_{r,s}$ et $K_1 \cap K_2 = F_{r-1,s-1}$. D'après la remarque 1.1.3, appliquée avec $r-1$ au lieu de r, avec $r' = r-1$ et avec $s' = s-1$, montre que $K_1/K_1 \cap K_2 = F_{r-1,s}/F_{r-1,s-1}$ est galoisien de degré p. De même, la remarque 1.1.3, appliquée avec $s-1$ au lieu de s, avec $r' = r-1$ ($r' \geq 1$ car $r \geq 2$) et avec $s' = s-1$, on en déduit que $K_2/K_1 \cap K_2 = F_{r,s-1}/F_{r-1,s-1}$ est galoisien (car $\zeta_p \in F_{r-1,s-1}$) de degré p. Avec les notations de la proposition 1.2.10, on a que

$$\begin{cases} d_1 = d_2 = p \\ t_1 = t_2(r-1,s),\ t_2 = t_1(r,s-1) \\ t_1' = t_2(r,s),\ t_2' = t_1(r,s). \end{cases}$$

De plus, d'après le lemme 1.1.2, $K_1K_2/K_1 \cap K_2$ est totalement ramifié. Comme $t_2(r,s) < t_1(r,s)$, i.e. $t_1' < t_2'$ et que $d_1 = d_2 = p$, on déduit du *ii*) de la proposition 1.2.10 que $t_1' = t_1$, ce qui correspond à la formule souhaitée. □

1.3 Calcul des $t_k(r,s)$ avec $k \in \{1,2\}$.

Dans cette section, on se propose de calculer explicitement les nombres $t_1(r,s)$ et $t_2(r,s)$ pour des valeurs de $r \geq 1$ et $s \geq 0$ quelconques. Le cas $F = \mathbb{Q}_p$ a été traité par Viviani dans [46]. Néanmoins, son approche est basée sur le fait que l'on connaisse une uniformisante de $F_{1,s+1}/F_{1,s}$ [46, Lemma 5.7, Lemma 6.4]. Cette méthode ne semble pas pouvoir se généraliser dès lors que l'on remplace $\mathbb{Q}_p$ par F, ce qui nous a conduit à plutôt utiliser le corollaire 1.2.8.

Remarque 1.3.1. En appliquant la remarque 1.1.3 avec $r = 1$, $r' = 1$ et avec $s' = 0$, on obtient alors que $F_{1,s}/F_{1,0}$ est une extension totalement ramifiée de degré p^s. De plus, $F_{1,0}/F$ est une extension totalement ramifiée de degré $p-1$. Ainsi, $F_{1,s}/F$ est une extension totalement ramifiée de degré $(p-1)p^s$. D'après le corollaire 1.2.8, appliqué à $K = F_{1,s}$ et à $\alpha = a^{1/p^s}$, on en déduit donc que

$$t_2(1, s+1) = p^{s+1} - c_{F_{1,s}}(a^{1/p^s}).$$

Remarque 1.3.2. Soit $s \geq 1$ un entier. D'après le lemme 1.1.2, $F_{1,s}/F$, et donc $F_{1,s}/F_{0,s}$, est totalement ramifié. De plus, remarquons que

$$[F_{1,s} : F_{0,s}] := [F(\zeta_p, a^{1/p^s}) : F(a^{1/p^s})] = p - 1.$$

Supposons par l'absurde que ce ne soit pas le cas, i.e. que $[F_{1,s} : F_{0,s}] < p-1$. Comme $[F(a^{1/p^s}) : F] \leq p^s$, il en résulterait alors que $[F_{1,s} : F] < (p-1)p^s$, ce qui contredit le lemme 1.1.2, appliqué avec $r = 1$.

Avant de pouvoir prouver les théorèmes 1.3.5 et 1.3.6, on aura besoin, au préalable, du calcul de $t_1(r,0)$ et de $t_2(1,s)$ pour tous entiers $r, s \geq 1$.

Lemme 1.3.3. *Pour tout $r \geq 1$, l'extension $F(\zeta_{p^r})/F(\zeta_{p^{r-1}})$ possède un unique saut égal à $p^{r-1} - 1$. En d'autres termes, $t_1(r,0) = p^{r-1} - 1$.*

Démonstration. La preuve a été faite dans [39, Chapitre IV, §4] pour le cas $F = \mathbb{Q}_p$. Néanmoins, comme $F/\mathbb{Q}_p$ est non ramifiée, on a alors, d'après [30, section 1, exemple 2], appliqué avec [2] $K' = F(\zeta_{p^{r-1}}), K = \mathbb{Q}_p(\zeta_{p^{r-1}})$ et $L = \mathbb{Q}_p(\zeta_{p^r})$, que

$$\mathrm{Gal}(F(\zeta_{p^r})/F(\zeta_{p^{r-1}}))_i \simeq \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p(\zeta_{p^{r-1}}))_i$$

pour tout $i \geq 0$. Il s'ensuit donc que $F(\zeta_{p^r})/F(\zeta_{p^{r-1}})$ possède un unique saut égal à $p^{r-1} - 1$. □

Lemme 1.3.4. *Soit $s \geq 0$ un entier. Alors*

i) $t_2(1, s+1) = p^{s+1} - p + 1$ *si* $p \mid v_F(a)$;

ii) $t_2(1, s+1) = p^{s+1}$ *si* $p \nmid v_F(a)$.

Démonstration. *i)* Posons $c_s = c_{F_{1,s}}(a^{1/p^s})$ et $f = [F : \mathbb{Q}_p]$. Comme $(a^{1/p^s})^{1-p^f} = a^{1/p^s}(a^{1/p^{s-f+1}})^{-p}$, on a, par définition de $c_K(\alpha)$, (cf définition 1.2.5),

$$c_s = c_{F_{1,s}}((a^{1/p^s})^{1-p^f}).$$

[2] K'/K est non ramifié puisque $F/\mathbb{Q}_p$ l'est

Supposons d'abord $v_F(a) = 0$. Dans ce cas, $a^{1/p^s} \in \mathcal{O}_{F_{1,s}}^{\times}$. Comme $F_{s,s}/F$ est totalement ramifiée d'après le lemme 1.1.2, il s'ensuit que $F_{0,s}/F$ est aussi totalement ramifié. Par conséquent,

$$\mathcal{O}_{F_{0,s}}/\mathfrak{p}_{F_{0,s}} \simeq \mathbb{F}_{p^f}.$$

On en déduit alors que $(a^{1/p^s})^{1-p^f} \equiv 1 \mod \mathfrak{p}_{F_{0,s}}$. D'après la remarque 1.3.2, $F_{1,s}/F_{0,s}$ est totalement ramifié de degré $p-1$. Il s'ensuit donc que $\mathfrak{p}_{F_{0,s}} = \mathfrak{p}_{F_{1,s}}^{p-1}$. Par définition de $c_K(\alpha)$, on en déduit ainsi que $c_s \geq p-1$ pour tout $s \geq 0$.

Montrons maintenant par récurrence sur s que $c_s \leq p-1$. Comme $c_0 \geq p-1$, on déduit de la remarque 1.3.1 que $t_2(1,1) \leq 1$. Or, $t_2(1,1) \neq 0$ car $F_{1,1}/F_{1,0}$ est totalement ramifié de degré p d'après la remarque 1.1.3, appliquée avec $r = s = r' = 1$ et avec $s' = 0$. Par conséquent, $t_2(1,1) = 1$ et donc, $c_0 = p-1$, ce qui initialise la récurrence.

Supposons maintenant que $c_s \leq p-1$ pour un certain $s \geq 0$ et montrons que $c_{s+1} \leq p-1$. Notons

$$x = a^{1/p^{s+1}} \in \mathcal{O}_{F_{1,s+1}}^{\times}.$$

Remarquons que $x^{1-p^f} \equiv 1 \mod \mathfrak{p}_{F_{1,s+1}}^{p-1}$. Soit $y \in F_{1,s+1}^{*}$ tel que

$$z = x^{1-p^f} y^{-p} \in \mathcal{O}_{F_{1,s+1}} \text{ et } z \equiv 1 \mod \mathfrak{p}_{F_{1,s+1}}^{c_{s+1}}. \tag{1.5}$$

Remarquons que $y \in \mathcal{O}_{F_{1,s+1}}^{\times}$ du fait que $x,\ z \in \mathcal{O}_{F_{1,s+1}}^{\times}$.

Supposons par l'absurde que $c_{s+1} \geq p$. Comme $\mathcal{O}_{F_{1,s+1}} = \mathbb{Z}_p[\pi_{F_{1,s+1}}]$, où $\pi_{F_{1,s+1}}$ désigne une uniformisante de $F_{1,s+1}$, on peut alors écrire

$$y = \sum_{i \geq 0} a_i \pi_{F_{1,s+1}}^i$$

avec $a_0 \in \mathbb{Z}_p^{\times}$, car $y \in \mathcal{O}_{F_{1,s+1}}^{\times}$, et $a_i \in \mathbb{Z}_p$ pour tout $i \geq 1$. Il s'ensuit donc que

$$y^p \equiv a_0^p \mod \mathfrak{p}_{F_{1,s+1}}^p.$$

Comme $a_0 \in \mathbb{Z}_p$, on a alors que $a_0^p \equiv a_0 \mod p$. Ainsi, $y^p \equiv a_0 \mod \mathfrak{p}_{F_{1,s+1}}^p$. Comme $z \equiv 1 \mod \mathfrak{p}_{F_{1,s+1}}^p$, on déduit de (1.5) que

$$x^{1-p^f} \equiv a_0 \mod \mathfrak{p}_{F_{1,s+1}}^p. \tag{1.6}$$

D'après la remarque 1.1.3, appliquée avec $r = 1$, $r' = 1$, $s' = s$ et où s est remplacé par $s+1$, on en déduit que $F_{1,s+1}/F_{1,s}$ est totalement ramifié de degré p. Ainsi, $\mathfrak{p}_{F_{1,s+1}}^p = \mathfrak{p}_{F_{1,s}}$. En élevant maintenant (1.6) à la puissance p, on a que

$$(x^p)^{1-p^f} a_0^{-p} \equiv 1 \mod \mathfrak{p}_{F_{1,s}}^p.$$

Comme $x^p = a^{1/p^s}$ et que $a_0 \in \mathbb{Z}_p^{\times}$, il en résulte que $c_s \geq p$, ce qui contredit l'hypothèse de récurrence.

On a ainsi montré que $c_s \leq p-1$ pour tout $s \geq 0$. Ainsi, $c_s = p-1$. De la remarque 1.3.1, il en résulte que $t_2(1,s+1) = p^{s+1} - p + 1$. Cela termine la preuve de la première affirmation du lemme dans le cas où $v_F(a) = 0$.

Supposons maintenant que $p \mid v_F(a) \neq 0$. Posons $a = p^{v_F(a)}\gamma = \pi_{F_{1,s}}^{(p-1)p^s v_F(a)}\gamma$ avec $v_F(\gamma) = 0$ et $y = \pi_{F_{1,s}}^{(p-1)v_F(a)p^{-1}}\beta$. Il est clair que $a^{1/p^s}y^{-p} = \gamma^{1/p^s}\beta^{-p}$ et donc $c_{F_{1,s}}(a^{1/p^s}) = c_{F_{1,s}}(\gamma^{1/p^s}) = p-1$ puisque $v_F(\gamma) = 0$. On conclut grâce à la remarque 1.3.1.

ii) De la remarque 1.2.6, il est clair que $c_{F_{1,s}}(a^{1/p^s}) = 0$. De la remarque 1.3.1, on en déduit donc que $t_2(1,s+1) = p^{s+1}$. □

On peut maintenant prouver les résultats principaux de cette section, à savoir les théorèmes 1.3.5 et 1.3.6.

Théorème 1.3.5. *Supposons $p \mid v_F(a)$. Soient r et s deux entiers positifs. Alors*

i) si $r \geq s \geq 1$, $t_2(s,r) = p^{r+s-1} - \frac{p-1}{p+1}(p^{2s-1}+1)$;

ii) si $r \geq s \geq 1$, $t_1(s,r) = \frac{p-1}{p+1}(p^{2s-2}-1)$;

iii) si $r \geq s \geq 1$, $t_2(r,s) = p^{2s-1} - \frac{p-1}{p+1}(p^{2s-1}+1)$;

iv) si $r > s$, alors $t_1(r,s) = p^{r+s-1} - p^{2s} + \frac{p-1}{p+1}(p^{2s}-1)$.

Démonstration. Supposons d'abord $s = 0$. Dans ce cas, *i*), *ii*) et *iii*) sont vides et *iv*) découle du lemme 1.3.3.

Supposons maintenant $s = 1$. Tout d'abord, *i*) découle du lemme 1.3.4 et *ii*) du fait que $F_{1,r}/F_{0,r}$ soit une extension totalement ramifiée de degré $p-1$ d'après la remarque 1.3.2 appliquée avec $s = r$ (et donc, $t_1(1,r) = 0 = \frac{p-1}{p+1}(p^0-1)$).

Nous allons maintenant montrer *iii*) et *iv*) par récurrence sur $r \geq 1$. Supposons $r = 1$. Dans ce cas, *iv*) est vide. De plus, *iii*) est aussi satisfait puisque $t_2(1,1) = 1$ d'après le *i*) du lemme 1.3.4 appliqué à $s = 0$. Ceci montre l'initialisation.

Supposons maintenant que *iii*) et *iv*) soient vérifiés pour un certain entier $r \geq 1$ et montrons qu'ils le sont encore pour l'entier $r+1$. Par hypothèse de récurrence, on déduit du *iii*) que $t_2(r,1) = 1$ et d'après le lemme 1.3.3, $t_1(r+1,0) = p^r - 1$. Le *i*) de la proposition 1.2.11 montre donc que

$$t_2(r+1,1) - t_1(r+1,1) = p(t_2(r,1) - t_1(r+1,0)) = p(2-p^r) < 0 \qquad (1.7)$$

car $r \geq 1$. Le *ii*) de la proposition 1.2.11 montre donc que

$$t_2(r+1,1) = t_2(r,1) = 1,$$

i.e. *iii*). On déduit alors de (1.7) que

$$t_1(r+1,1) = p^{r+1} - 2p + 1 = p^{r+1} - p^2 + \frac{p-1}{p+1}(p^2-1),$$

ce qui montre *iv*). Cela prouve donc le théorème dans le cas $s = 1$.

Notons maintenant Λ l'ensemble des couples $(r,s) \neq (0,0)$ de $\mathbb{N}^2$ tels que $r \geq s \geq 0$ et vérifiant les affirmations $i)$ à $iv)$ du théorème. Supposons par l'absurde qu'il existe $(r,s) \notin \Lambda$ avec $r \geq s \geq 0$. Choisissons le minimal pour l'ordre lexicographique. Par ce qui précède, $s \geq 2$.

Montrons dans un premier temps que (r,s) vérifie $i)$ et $ii)$. Par minimalité de (r,s), on a que $(r,s-1) \in \Lambda$. Ainsi, en utilisant $i)$,

$$t_2(s-1,r) = p^{r+s-2} - \frac{p-1}{p+1}(p^{2s-3}+1). \tag{1.8}$$

Par minimalité, on a aussi que $(s,s-1) \in \Lambda$. En utilisant $iv)$, on obtient alors que

$$t_1(s,s-1) = p^{2s-2} - p^{2(s-1)} - \frac{p-1}{p+1}(p^{2(s-1)}-1) = \frac{p-1}{p+1}(p^{2s-2}-1). \tag{1.9}$$

De plus, remarquons que l'on a

$$t_1(s,r-1) = \frac{p-1}{p+1}(p^{2s-2}-1). \tag{1.10}$$

En effet, cette égalité découle de (1.9) si $r = s$. Si $r \geq s+1$, alors $(r-1,s) \in \Lambda$ et (1.10) découle de $ii)$.

En utilisant maintenant (1.8) et (1.10), on déduit du $i)$ de la proposition 1.2.11 que

$$\begin{aligned} t_1(s,r) - t_2(s,r) &= p(t_1(s,r-1) - t_2(s-1,r)) \\ &= p\left(\frac{p-1}{p+1}p^{2s-2} - p^{r+s-2} + \frac{p-1}{p+1}p^{2s-3}\right) \\ &= p\left((p-1)p^{2s-3} - p^{r+s-2}\right) < 0, \end{aligned} \tag{1.11}$$

car $(p-1)p^{2s-3} - p^{r+s-2} = p^{2s-2}(p-1-p^{r-s+1}) < 0$ du fait que $r \geq s$. Le $ii)$ de la proposition 1.2.11, où l'on a permuté le rôle de r et de s, ainsi que (1.10), montrent alors que

$$t_1(s,r) = t_1(s,r-1) = \frac{p-1}{p+1}(p^{2s-2}-1).$$

En injectant maintenant cette équation dans (1.11), il s'ensuit que

$$\begin{aligned} t_2(s,r) &= p(p^{r+s-2} - (p-1)p^{2s-3}) + \frac{p-1}{p+1}(p^{2s-2}-1) \\ &= p^{r+s-1} - \frac{p-1}{p+1}(p^{2s-1}+1), \end{aligned}$$

ce qui montre que (r,s) vérifie $i)$ et $ii)$.

Nous sommes maintenant en mesure de prouver que $(s,s) \in \Lambda$. Supposons que $r > s$. Alors $(s,s) \in \Lambda$ par minimalité. En revanche, si $r = s$, alors du paragraphe précédent, on en déduit que (s,s) vérifie $i)$ et $ii)$. Par ailleurs, en appliquant le $i)$ avec $r = s$ (ce qui est licite puisque (r,s) vérifie $i)$ d'après le paragraphe précédent), on obtient alors $iii)$ dans le cas $r = s$. Enfin, $iv)$ est vide dans le cas $r = s$. Cela signifie donc que si $r = s$, alors $(s,s) \in \Lambda$. Comme

$(r,s) \notin \Lambda$, il s'ensuit alors que $r \geq s+1$.

Montrons maintenant que (r,s) vérifie *iii)* et *iv)*. Comme $r \geq s+1$, on en déduit, par minimalité, que $(r-1,s) \in \Lambda$. En utilisant *iii)*,

$$t_2(r-1,s) = p^{2s-1} - \frac{p-1}{p+1}(p^{2s-1}-1). \tag{1.12}$$

Toujours par minimalité, $(r,s-1) \in \Lambda$. En utilisant maintenant *iv)*, on a

$$t_1(r,s-1) = p^{r+s-2} - p^{2(s-1)} + \frac{p-1}{p+1}(p^{2(s-1)}-1). \tag{1.13}$$

En utilisant (1.12) et (1.13), il s'ensuit donc, d'après le *i)* de la proposition 1.2.11, que

$$\begin{aligned} t_2(r,s) - t_1(r,s) &= p(t_2(r-1,s) - t_1(r,s-1)) \\ &= p\left(p^{2s-1} - \frac{p-1}{p+1}(p^{2s-2}+p^{2s-1}) + p^{2s-2} - p^{r+s-2}\right) \\ &= p(2p^{2s-2} - p^{r+s-2}) < 0, \end{aligned} \tag{1.14}$$

car $r \geq s+1$. Le *iii)* de la proposition 1.2.11, ainsi que (1.12), montrent alors que

$$t_2(r,s) = t_2(r-1,s) = p^{2s-1} - \frac{p-1}{p+1}(p^{2s-1}-1).$$

En injectant maintenant cette égalité dans (1.14), on en déduit que

$$\begin{aligned} t_1(r,s) &= p(p^{r+s-2} - 2p^{2s-2}) + p^{2s-1} - \frac{p-1}{p+1}(p^{2s-1}+1) \\ &= p^{r+s-1} - \frac{p-1}{p+1}(p^{2s-1}+1) - p^{2s-1} \\ &= p^{r+s-1} - p^{2s} + \frac{p-1}{p+1}(p^{2s}-1). \end{aligned}$$

Ceci montre que (r,s) vérifie aussi *iii)* et *iv)*, ce qui contredit le fait que $(r,s) \notin \Lambda$. Le théorème s'ensuit. □

Nous allons maintenant prouver l'analogue du théorème 1.3.5 dans le cas où $p \nmid v_p(a)$.

Théorème 1.3.6. *Supposons que $p \nmid v_F(a)$. Soient r et s des entiers positifs. Alors*

i) si $r > s \geq 1$, $t_2(s,r) = p^{r+s-1} - \frac{p^{2s-1}-p^{2s-2}-p+1}{p+1}$;

ii) si $r > s \geq 1$, $t_2(r,s) = \frac{2p^{2s}+p-1}{p+1}$;

iii) si $r \geq 0$, $t_1(1,r) = 0$;

iv) si $r > s \geq 2$, $t_1(s,r) = p^{2s-3} - \frac{2p^{2s-3}-p+1}{p+1}$;

v) si $r > s+1$, $t_1(r,s) = p^{r+s-1} - \frac{2p^{2s+1}-p+1}{p+1}$;

vi) si $s \geq 1$, $t_1(s+1,s) = p^{2s-1} - \frac{2p^{2s-1}-p+1}{p+1}$;

vii) si $s \geq 1$, $t_2(s,s) = p^{2s-1} - \frac{p^{2s-1}-p^{2s-2}-p+1}{p+1}$;

viii) si $s \geq 2$, $t_1(s,s) = p^{2s-3} - \frac{2p^{2s-3}-p+1}{p+1}$.

Démonstration. Soit $r \geq 0$. Alors l'extension $F_{1,r}/F_{0,r}$ est totalement ramifiée de degré $p-1$ d'après la remarque 1.3.2. Par conséquent, $t_1(1,r) = 0$, ce qui montre *iii)*. Nous allons maintenant montrer les autres formules.

Supposons d'abord que $s = 0$. Remarquons que toutes les affirmations, sauf le *v)*, sont vides et le *v)* découle du lemme 1.3.3.

Supposons maintenant $s = 1$. Tout d'abord, *iv)* et *viii)* sont vides. Ensuite, *i)* et *vii)* découlent du *ii)* du lemme 1.3.4. Montrons que l'on a également *vi)*. D'après le *i)* de la proposition 1.2.11,

$$t_1(2,1) - t_2(2,1) = p(t_1(2,0) - t_2(1,1)) = -p < 0 \tag{1.15}$$

puisque $t_1(2,0) = p-1$ d'après le lemme 1.3.3 et que $t_2(1,1) = p$ d'après le *ii)* du lemme 1.3.4. Le *ii)* de la proposition 1.2.11 montre alors que

$$t_1(2,1) = t_1(2,0) = p - 1 = p - \frac{2p-p+1}{p+1}, \tag{1.16}$$

i.e. *vi)*.

Supposons toujours que $s = 1$ et montrons maintenant *ii)* et *v)* par récurrence sur $r \geq 2$. Si $r = 2$, remarquons que *v)* est vide. En injectant (1.16) dans (1.15), on en déduit que

$$t_2(2,1) = p - 1 + p = 2p - 1 = \frac{2p^2+p-1}{p+1},$$

ce qui montre *ii)* dans le cas $r = 2$. Ceci termine l'initialisation. Supposons maintenant que *ii)* et *v)* soient vérifiés pour un certain entier $r \geq 2$ et montrons qu'ils le sont encore pour l'entier $r+1$. D'après le lemme 1.3.3, on a $t_2(r+1,0) = p^r - 1$. Par hypothèse de récurrence, on déduit du *ii)* que

$$t_2(r,1) = 2p - 1 = \frac{2p^2+p-1}{p+1}. \tag{1.17}$$

D'après le *i)* de la proposition 1.2.11, on a alors que

$$\begin{aligned} t_2(r+1,1) - t_1(r+1,1) &= p(t_2(r,1) - t_1(r+1,0)) \\ &= p(2p - 1 - p^r + 1) = p(2p - p^r) < 0 \end{aligned} \tag{1.18}$$

car $r \geq 2$. Le *iii)* de la proposition 1.2.11, ainsi que (1.17), montrent donc que

$$t_2(r+1,1) = t_2(r,1) = 2p - 1 = \frac{2p^2+p-1}{p+1},$$

i.e. *ii)*. En injectant cette égalité dans (1.18), on obtient alors que

$$t_1(r+1,1) = p^{r+1} - 2p^2 + 2p - 1 = p^{r+1} - \frac{2p^3-p+1}{p+1},$$

i.e. v). Cela prouve donc le théorème dans le cas où $s = 1$.

Notons maintenant Λ l'ensemble des couples (r,s) de $\mathbb{N}^2$ tels que $r > s \geq 0$ et vérifiant les affirmations i) à $viii$) du théorème. Supposons par l'absurde qu'il existe $(r,s) \notin \Lambda$ avec $r > s \geq 0$. Choisissons le minimal pour l'ordre lexicographique. Par ce qui précède, $s \geq 2$.

Montrons dans un premier temps que (r,s) vérifie vii) et $viii$). Par minimalité de (r,s), on en déduit que $(s, s-1) \in \Lambda$. En utilisant le i),

$$t_2(s-1,s) = p^{2s-2} - \frac{p^{2s-3} - p^{2s-4} - p + 1}{p+1}. \tag{1.19}$$

En utilisant maintenant le vi), on en déduit, car $s \geq 2$, que

$$t_1(s,s-1) = p^{2s-3} - \frac{2p^{2s-3} - p + 1}{p+1}. \tag{1.20}$$

D'après le i) de la proposition 1.2.11, on en déduit, en utilisant (1.19) et (1.20), que

$$\begin{aligned} t_1(s,s) - t_2(s,s) &= p(t_1(s,s-1) - t_2(s-1,s)) \\ &= p\left(p^{2s-3} - p^{2s-2} - \frac{p^{2s-3} + p^{2s-4}}{p+1}\right) \\ &= p^{2s-3}(-p^2 + p - 1) < 0. \end{aligned} \tag{1.21}$$

Le ii) de la proposition 1.2.11, ainsi que (1.20), montrent donc que

$$t_1(s,s) = t_1(s,s-1) = p^{2s-3} - \frac{2p^{2s-3} - p + 1}{p+1}, \tag{1.22}$$

i.e. $viii$). En injectant maintenant cette égalité dans (1.21), il s'ensuit que

$$\begin{aligned} t_2(s,s) &= p^{2s-3}(p^2 - p + 1) + p^{2s-3} - \frac{2p^{2s-3} - p + 1}{p+1} \\ &= \frac{p^{2s-3}(p^2 - p + 2)(p+1) - 2p^{2s-3} + p - 1}{p+1} = \frac{p^{2s} + p^{2s-2} + p - 1}{p+1} \\ &= p^{2s-1} - \frac{p^{2s-1} - p^{2s-2} - p + 1}{p+1}, \end{aligned} \tag{1.23}$$

i.e. vii).

Montrons maintenant que (r,s) vérifie i) et iv). Comme $s \geq 2$, on a alors que

$$t_1(s,r-1) = p^{2s-3} - \frac{2p^{2s-3} - p + 1}{p+1}. \tag{1.24}$$

En effet, si $r = s+1$, alors cette égalité découle de (1.22). En revanche, si $r \geq s+2$, alors $(r-1,s) \in \Lambda$ et l'égalité découle de iv).

Comme $(r, s-1) \in \Lambda$ par minimalité, on déduit du i) que

$$t_2(s-1,r) = p^{r+s-2} - \frac{p^{2s-3} - p^{2s-4} - p + 1}{p+1}. \tag{1.25}$$

D'après le i) de la proposition 1.2.11, on en déduit, en utilisant (1.24) et (1.25), que

$$\begin{aligned} t_1(s,r) - t_2(s,r) &= p(t_1(s,r-1) - t_2(s-1,r)) \\ &= p\left(p^{2s-3} - \frac{p^{2s-3}+p^{2s-4}}{p+1} - p^{r+s-2}\right) \\ &= p(p^{2s-3} - p^{2s-4} - p^{r+s-2}) < 0 \end{aligned} \tag{1.26}$$

car $p^{2s-3} - p^{2s-4} - p^{r+s-2} \leq p^{2s-4}(-p^3+p-1) < 0$ (car $r > s$). Le ii) de la proposition 1.2.11, où l'on a permuté le rôle de r et s, ainsi que (1.24), montrent alors que

$$t_1(s,r) = t_1(s,r-1) = p^{2s-3} - \frac{2p^{2s-3}-p+1}{p+1},$$

i.e. iv). En injectant maintenant cette équation dans (1.26), on en déduit que

$$\begin{aligned} t_2(s,r) &= p(p^{r+s-2} + p^{2s-4} - p^{2s-3}) + p^{2s-3} - \frac{2p^{2s-3}-p+1}{p+1} \\ &= p^{r+s-1} - \frac{p^{2s-1}-p^{2s-2}-p+1}{p+1}, \end{aligned}$$

i.e. i).

Nous allons maintenant montrer que (r,s) vérifie $ii), v)$ et vi). Comme $r \geq s+1$, on en déduit que $(s+1, s-1) \in \Lambda$ par minimalité. Ainsi, en utilisant le v),

$$t_1(s+1,s-1) = p^{2s-1} - \frac{2p^{2s-1}-p+1}{p+1}. \tag{1.27}$$

D'après le i) de la proposition 1.2.11, on en déduit, en utilisant (1.23) et (1.27), que

$$\begin{aligned} t_1(s+1,s) - t_2(s+1,s) &= p(t_1(s+1,s-1) - t_2(s,s)) \\ &= p\left(p^{2s-1} - \frac{p^{2s}+2p^{2s-1}+p^{2s-2}}{p+1}\right) \\ &= p(p^{2s-1} - p^{2s-2}(p+1)) = -p^{2s-1} < 0. \end{aligned} \tag{1.28}$$

Le i) de la proposition 1.2.11, ainsi que (1.27), montrent donc que

$$t_1(s+1,s) = t_1(s+1,s-1) = p^{2s-1} - \frac{2p^{2s-1}-p+1}{p+1},$$

i.e. vi). En injectant maintenant cette équation dans (1.28), il s'ensuit que

$$t_2(s+1,s) = 2p^{2s-1} - \frac{2p^{2s-1}-p+1}{p+1} = \frac{2p^{2s}+p-1}{p+1},$$

i.e. ii) dans le cas $r = s+1$. Remarquons que iv) est vide pour $r = s+1$. On a ainsi montré que $(s+1,s) \in \Lambda$. Comme $(r,s) \notin \Lambda$, on en déduit que $r \geq s+2$.

Il nous reste plus qu'à montrer que (r,s) vérifie ii) et v) pour $r \geq s+2$. Par minimalité, $(r-1,s) \in \Lambda$. En utilisant le ii), on obtient que

$$t_2(r-1,s) = \frac{2p^{2s}+p-1}{p+1}. \tag{1.29}$$

De même, $(r, s-1) \in \Lambda$. En utilisant le v), on a ainsi que

$$t_1(r, s-1) = p^{r+s-2} - \frac{2p^{2s-1} - p + 1}{p+1}. \tag{1.30}$$

D'après le i) de la proposition 1.2.11, on en déduit, en utilisant (1.29) et (1.30) que

$$\begin{aligned} t_2(r,s) - t_1(r,s) &= p(t_2(r-1,s) - t_1(r,s-1)) \\ &= p\left(\frac{2p^{2s-1} + 2p^{2s}}{p+1} - p^{r+s-2}\right) \\ &= -p(p^{r+s-2} - 2p^{2s-1}) < 0 \end{aligned} \tag{1.31}$$

car $r \geq s+2$ et $p \geq 3$. Le ii) de la proposition 1.2.11, ainsi que (1.29), montrent alors que

$$t_2(r,s) = t_2(r-1,s) = \frac{2p^{2s} + p - 1}{p+1},$$

i.e. ii). En injectant cette égalité dans (1.31), il s'ensuit que

$$\begin{aligned} t_1(r,s) &= p(p^{r+s-2} - 2p^{2s-1}) + \frac{2p^{2s} + p - 1}{p+1} \\ &= p^{r+s-1} - \frac{2p^{2s+1} - p + 1}{p+1}, \end{aligned}$$

i.e. v).

On vient ainsi de montrer que $(r,s) \in \Lambda$, ce qui est absurde. Le théorème s'ensuit. □

Remarque 1.3.7. L'utilisation du théorème 1.2.8 (Hecke) semble plus adapté à ce problème que ne l'est le calcul explicite d'une uniformisante de $F_{1,s}/F_{1,s-1}$ [46, Lemma 5.7,Lemma 6.4]. Outre les généralisations évidentes (comme le fait que l'on considère une extension non ramifiée de $\mathbb{Q}_p$ plutôt que $\mathbb{Q}_p$ et un $a \in F^*$ à la place de $a \in \mathbb{Z} \subset \mathbb{Z}_p$ avec $v_p(a) \in \{0,1\}$), l'utilisation du théorème 1.2.8 nous permet de calculer des sauts que l'on ne peut calculer dans [46]. Dans [46, §5, §6], l'auteur ne peut calculer $t_1(r,s)$ et $t_2(r,s)$ que pour $r \geq s$ tandis que dans les théorèmes 1.3.5 et 1.3.6, on peut les calculer même si $r < s$. Par exemple, comme $v_p(2) = 0$, le i) du théorème 1.3.5 affirme que le saut de l'extension $\mathbb{Q}_p(\zeta_{p^2}, 2^{1/p^4})/\mathbb{Q}_p(\zeta_{p^2}, 2^{1/p^3})$ est égal à

$$t_2(2,4) = p^5 - \frac{p^3 - p^2 - p + 1}{p+1} = p^5 - p^2 + 2p - 1.$$

1.4 Calcul des groupes de ramification de $\mathrm{Gal}(F_{r,s}/F)$.

On se propose de calculer explicitement la suite des groupes de ramification de $\mathrm{Gal}(F_{r,s}/F)$ avec $r \geq s$. Commençons par le cas où $p \mid v_F(a)$. Nous avons besoin, au préalable, de quelques inégalités concernant les fonctions $t_1(.,.)$ et $t_2(.,.)$ et de quelques propriétés concernant deux suites que l'on définira dans le lemme 1.4.2. Ces suites nous serviront pour décrire les sauts de $\mathrm{Gal}(F_{r,s}/F)$ dans le cas où $p \mid v_F(a)$.

Lemme 1.4.1. *Pour tout entier $s \geq 1$, on a*

i) $t_1(s+1,s) < t_2(s+1,s+1)$;

ii) $t_2(s,s) < t_1(s+1,s)$.

Démonstration. D'après le i) et le iv) du théorème 1.3.5, on obtient que

$$t_1(s+1,s) - t_2(s+1,s+1) = \frac{p-1}{p+1}(p^{2s} + p^{2s+1}) - p^{2s+1} = -p^{2s} < 0$$

et

$$t_2(s,s) - t_1(s+1,s) = p^{2s-1} - \frac{p-1}{p+1}(p^{2s-1} + p^{2s}) = p^{2s-1}(2-p) < 0.$$

□

Lemme 1.4.2. *Soient $r \geq s \geq 0$ des entiers. Construisons par récurrence deux suites d'entiers positifs $(r^{(i)})_{i\geq 0}$ et $(s^{(i)})_{i\geq 0}$ comme suit : $r^{(0)} = s^{(0)} = 0$ et, pour $i \geq 0$,*

$$(r^{(i+1)}, s^{(i+1)}) = \begin{cases} (\min\{r, r^{(i)}+1\}, s^{(i)}) \text{ si } s^{(i)} = s \\ (r^{(i)}+1, s^{(i)}) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} = s^{(i)} \\ (r^{(i)}, s^{(i)}+1) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} \neq s^{(i)} \end{cases} . \tag{1.32}$$

On a alors les propriétés suivantes :

i) les suites $(r^{(i)})_i$ et $(s^{(i)})_i$ sont croissantes et stationnaires de limites respectives r et s. On note alors i_0 le plus petit entier i tel que $(r^{(i_0)}, s^{(i_0)}) = (r,s)$.

ii) soit $i \geq 0$ tel que $s^{(i)} \neq s$. Alors $r^{(i)} \in \{s^{(i)}, s^{(i)}+1\}$.

iii) pour tout $i \geq 0$, $r^{(i)} \geq s^{(i)}$.

Démonstration. i) Remarquons que par construction, la suite $(s^{(i)})_i$ est croissante et majorée par s ; elle est donc stationnaire. Notons s' sa limite. Notons i_1 le plus petit entier tel que $s^{(i_1)} = s'$.

Supposons par l'absurde que $s' < s$. Soit $i \geq i_1$. Alors, on ne peut pas avoir $r^{(i)} \neq s^{(i)} = s'$ car alors, cela signifierait que $s' = s'+1$ d'après (1.32), ce qui est absurde. Il s'ensuit donc que $r^{(i)} = s^{(i)} = s'$ pour tout $i \geq i_1$, ce qui est une nouvelle fois absurde puisque d'après (1.32), on obtiendrait une fois encore que $s' = s'+1$. On a ainsi montré que $s' = s$.

Montrons que la suite $(r^{(i)})_i$ est croissante. Par construction de $(r^{(i)})_i$, il est clair que $r^{(0)} \leq \cdots \leq r^{(i_1-1)}$ (car $s^{(i)} \neq s$ pour tout $i \leq i_1 - 1$). De plus, d'après (1.32), appliqué à $i = i_1 - 1$,

$$r^{(i_1)} = \begin{cases} r^{(i_1-1)} + 1 \geq r^{(i_1-1)} \text{ si } r^{(i_1-1)} = s^{(i_1-1)} \\ r^{(i_1-1)} \text{ si } r^{(i_1-1)} \neq s^{(i_1-1)} \end{cases} .$$

Ainsi, $r^{(i_1-1)} \leq r^{(i_1)}$. Enfin, soit $i \geq i_1$. Comme $s^{(i_1)} = s$ et que la suite $(s^{(i)})_i$ est croissante, il s'ensuit que $s^{(i)} = s$. D'après (1.32), on a alors que $r^{(i+1)} = \min\{r, r^{(i)}+1\}$. En particulier, $r^{(i)} \leq r^{(i+1)}$. La suite $(r^{(i)})_{i\geq i_1}$ est donc croissante. Par conséquent, la suite $(r^{(i)})_{i\geq 1}$ est donc elle aussi croissante.

Comme $s' = s$, il en résulte, d'après (1.32), que $r^{(i+1)} = \min\{r, r^{(i)} + 1\}$ pour tout i assez grand. Comme $(r^{(i)})_i$ est une suite croissante, on en déduit alors qu'elle est majorée par r. Elle est donc également stationnaire. Notons r' sa limite. On a alors la relation $r' = \min\{r, r' + 1\}$, d'où $r' = r$.

ii) Clairement, *ii*) est vide si $s = 0$ puisque $s^{(0)} = 0$. Supposons donc que $s > 0$. D'après *i*), il existe un plus grand entier $i_1 \geq 0$ tel que $s^{(i)} \neq s$ pour tout $i \leq i_1$.

Si $i_1 = 0$, alors *ii*) est clairement vérifié puisque $r^{(0)} = s^{(0)} = 0$. Supposons donc que $i_1 \geq 1$ et montrons *ii*) par récurrence pour $i \in \{0, \ldots, i_1\}$. Pour $i = 0$, c'est clair. Supposons maintenant que *ii*) soit satisfait pour un certain $i \in \{0, \ldots, i_1 - 1\}$ et montrons qu'il l'est encore au rang $i + 1$.

Supposons tout d'abord que $r^{(i)} = s^{(i)}$. Comme $s^{(i)} \neq s$, il s'ensuit alors, d'après (1.32), que $s^{(i+1)} = s^{(i)}$ et que

$$r^{(i+1)} = r^{(i)} + 1 = s^{(i)} + 1 = s^{(i+1)} + 1,$$

ce qui montre l'hérédité.

Supposons maintenant que $r^{(i)} = s^{(i)} + 1$. Comme $s^{(i)} \neq s$, il s'ensuit alors, d'après (1.32), que $s^{(i+1)} = s^{(i)} + 1$ et que

$$r^{(i+1)} = r^{(i)} = s^{(i)} + 1 = s^{(i+1)},$$

ce qui montre à nouveau l'hérédité. On en déduit ainsi *ii*).

iii) Procédons par récurrence sur $i \geq 0$. Pour $i = 0$, c'est clair. Supposons que *iii*) soit vrai au rang i et montrons qu'il est encore vrai au rang $i + 1$.

Si $s^{(i+1)} \neq s$, alors on a clairement que $r^{(i+1)} \geq s^{(i+1)}$ d'après *ii*). Si on suppose maintenant que $s^{(i)} = s$, alors d'après (1.32), on a que $s^{(i+1)} = s^{(i)}$ et que $r^{(i+1)} = \min\{r, r^{(i)} + 1\}$. Or, $r \geq s$ et $r^{(i)} \geq s^{(i)} = s$ par hypothèse de récurrence. Il s'ensuit donc que $r^{(i+1)} \geq s = s^{(i+1)}$, ce qui montre à nouveau l'hérédité dans ce cas.

Supposons enfin que $s^{(i+1)} = s$ et que $s^{(i)} \neq s$. Comme $s^{(i+1)} \neq s^{(i)}$, on déduit alors de (1.32) que l'on est dans la situation où $r^{(i)} \neq s^{(i)}$. Ainsi, $s^{(i+1)} = s^{(i)} + 1$ et $r^{(i+1)} = r^{(i)}$. Comme $s^{(i)} \neq s$ et que $r^{(i)} \neq s^{(i)}$, on déduit alors du *ii*) que $r^{(i)} = s^{(i)} + 1$. Des différentes formules que l'on a montrées, on obtient alors que

$$r^{(i+1)} = r^{(i)} = s^{(i)} + 1 = s^{(i+1)},$$

ce qui montre encore l'hérédité dans ce cas. On en déduit maintenant *iii*). □

On peut maintenant prouver le théorème 1.1.5. L'affirmation i) de ce théorème ayant été déjà prouvé dans le lemme 1.4.2, il nous reste à montrer :

Théorème 1.4.3. *Supposons que $p \mid v_F(a)$. Soient r, s des entiers positifs avec $r \geq s$ et $r \geq 1$. Reprenons les notations et les suites $(r^{(i)})_i$ et $(s^{(i)})_i$ définies dans le lemme 1.4.2. Alors les i_0 (cf lemme 1.4.2, ii)) sauts de $F_{r,s}/F$ sont les*

$$\tau_i = \begin{cases} t_1(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} = s \text{ ou si } r^{(i)} = s^{(i)} \\ t_2(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} \neq s^{(i)} \end{cases}$$

avec $i \in \{0, \ldots, i_0 - 1\}$. De plus, pour $i \in \{0, \ldots, i_0 - 1\}$, on a

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_i} = \mathrm{Gal}(F_{r,s}/F_{r^{(i)}, s^{(i)}}).$$

Démonstration. Par définition de i_0, on a pour tout $i < i_0$ que $(r^{(i)}, s^{(i)}) \neq (r, s) = (r^{(i_0)}, s^{(i_0)})$. Remarquons que si $i_0 = 1$, alors le théorème est vérifié. En effet, si $i_0 = 1$, alors $(r, s) = (r^{(1)}, s^{(1)}) = (1, 0)$. D'après le lemme 1.1.4, $F_{1,0}/F$ a un unique saut égal à $t_1(1, 0)$. D'après le lemme 1.3.3, ce saut est égal à 0. En particulier, 0 est le premier saut de $F_{1,0}/F$, i.e.

$$\mathrm{Gal}(F_{1,0}/F)_0 = \mathrm{Gal}(F_{1,0}/F).$$

On en déduit donc le théorème dans le cas où $i_0 = 1$ puisque $\tau_0 = t_1(1, 0) = 0$ et que $r^{(0)} = s^{(0)} = 0$ par construction des suites $(r^{(i)})_i$ et $(s^{(i)})_i$. Supposons donc à partir de maintenant que $i_0 \geq 2$.

Pour tout $i \geq 0$, notons $K_i := F_{r^{(i)}, s^{(i)}}$. Par définition des suites $(r^{(i)})_i$ et $(s^{(i)})_i$ et des sauts $t_1(.,.)$ et $t_2(.,.)$ (cf lemme 1.1.4), on remarque que τ_i est l'unique saut de K_{i+1}/K_i.

On souhaite montrer que $\tau_0 < \cdots < \tau_{i_0-1}$. Soit $i \in \{0, \ldots, i_0 - 2\}$ et montrons que $\tau_i < \tau_{i+1}$.

Supposons dans un premier temps que $s^{(i)} = s$. Comme $i \leq i_0 - 2$, on a alors, par définition de i_0, que $r^{(i)} < r$ et $r^{(i+1)} < r$. D'après le (1.32) du lemme 1.4.2, on obtient alors que

$$(r^{(i+1)}, s^{(i+1)}) = (r^{(i)} + 1, s) \text{ et } (r^{(i+2)}, s^{(i+2)}) = (r^{(i)} + 2, s).$$

Il en résulte donc que

$$\tau_i = t_1(r^{(i)} + 1, s) \text{ et } \tau_{i+1} = t_1(r^{(i)} + 2, s).$$

En appliquant la remarque 1.1.3 avec $r = 2, r' = 1$ et avec $s' = s$, on obtient alors que $F_{2,s}/F_{1,s}$ est totalement ramifié. Il s'ensuit, en appliquant la proposition 1.2.9 à $K = F_{1,s}$ et à $\alpha = \zeta_p$ (et donc, $K_1 = F_{2,s}$), que la suite $(t_1(j, s))_{j \geq 1}$ est strictement croissante. En particulier, $\tau_i < \tau_{i+1}$.

Supposons maintenant que $s^{(i)} \neq s$. Supposons également que $r^{(i)} = s^{(i)}$. Dans ce cas, en utilisant deux fois le (1.32) du lemme 1.4.2, on a que [3]

$$(r^{(i+1)}, s^{(i+1)}) = (s^{(i)} + 1, s^{(i)}) \text{ et } (r^{(i+2)}, s^{(i+2)}) = (s^{(i)} + 1, s^{(i)} + 1).$$

Par conséquent,

$$\tau_i = t_1(s^{(i)} + 1, s^{(i)}) \text{ et } \tau_{i+1} = t_2(s^{(i)} + 1, s^{(i)} + 1).$$

Le i) du lemme 1.4.1, appliqué à $s = s^{(i)}$, montre alors que $\tau_i < \tau_{i+1}$.

Enfin, supposons que $r^{(i)} \neq s^{(i)}$. Alors $r^{(i)} = s^{(i)} + 1$ d'après le i) du lemme 1.4.2. En utilisant le (1.32) du lemme 1.4.2, on obtient alors que

$$(r^{(i+1)}, s^{(i+1)}) = (s^{(i)} + 1, s^{(i)} + 1),$$

et donc, $r^{(i+1)} = s^{(i+1)}$.

[3] $s^{(i+1)} \neq s$ car $s^{(i+1)} = s^{(i)} \neq s$

Remarquons que $r^{(i+1)} \neq r$. En effet, si $r^{(i+1)} = r$, on aurait alors que $s^{(i+1)} = r$. Or, $r \geq s$ et $s \geq s^{(i+1)}$ d'après le i) du lemme 1.4.2. Il s'ensuit donc que $s^{(i+1)} = s$. D'où $(r^{(i+1)}, s^{(i+1)}) = (r, s)$, ce qui est absurde puisque $i + 1 \leq i_0 - 1 < i_0$.

Comme $r^{(i+1)} \neq r$ et que $r^{(i+1)} = s^{(i+1)}$, on déduit alors, que l'on aille $s^{(i)} = s$ ou $s^{(i)} \neq s$, de (1.32) que

$$(r^{(i+2)}, s^{(i+2)}) = (s^{(i)} + 2, s^{(i)} + 1).$$

On a alors que

$$\tau_i = t_2(s^{(i)} + 1, s^{(i)} + 1) \text{ et } \tau_{i+1} = t_1(s^{(i)} + 2, s^{(i)} + 1).$$

On déduit du ii) du lemme 1.4.1, appliqué à $s = s^{(i)} + 1$, que $\tau_i < \tau_{i+1}$.

On a donc montré que $\tau_0 < \cdots < \tau_{i_0-1}$. D'après le iii) du lemme 1.4.2, $r^{(i)} \geq s^{(i)}$ pour tout $i \geq 0$. L'extension K_i/F est donc galoisienne pour tout i. Comme τ_i est l'unique saut de K_{i+1}/K_i, le corollaire 1.2.3 montre donc que les sauts de $F_{r,s}/F$ sont les $\tau_0, \ldots, \tau_{i_0-1}$ et que $\mathrm{Gal}(F_{r,s}/F)_{\tau_i} = \mathrm{Gal}(F_{r,s}/K_i)$, ce qui correspond précisément aux sauts et aux groupes énoncés dans le théorème. □

Dans le corollaire ci-dessous, nous donnons explicitement la valeur du dernier saut de $F_{r,s}/F$, ainsi que son dernier groupe de ramification.

Corollaire 1.4.4. *Supposons que $p \mid v_F(a)$. Soient r, s deux entiers positifs tels que $r \geq s$ et $r \geq 1$. Alors le dernier saut de l'extension $F_{r,s}/F$ est*

$$\tau_{i_0-1} = \begin{cases} t_1(r,s) \text{ si } r > s \\ t_2(r,s) \text{ si } r = s \end{cases}.$$

De plus, le dernier groupe de ramification non trivial est égal à

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_{i_0-1}} = \begin{cases} \mathrm{Gal}(F_{r,s}/F_{r-1,s}) \text{ si } r > s \\ \mathrm{Gal}(F_{r,s}/F_{r,s-1}) \text{ si } r = s \end{cases}.$$

Démonstration. D'après le théorème 1.4.3, le dernier saut de $F_{r,s}/F$ est égal à

$$\tau_{i_0-1} = \begin{cases} t_1(r^{(i_0)}, s^{(i_0)}) \text{ si } s^{(i_0-1)} = s \text{ ou si } r^{(i_0-1)} = s^{(i_0-1)} \\ t_2(r^{(i_0)}, s^{(i_0)}) \text{ si } s^{(i_0-1)} \neq s \text{ et si } r^{(i_0-1)} \neq s^{(i_0-1)} \end{cases}$$

et le dernier groupe de ramification non trivial est égal à

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_{i_0-1}} = \mathrm{Gal}(F_{r,s}/F_{r^{(i_0-1)}, s^{(i_0-1)}}).$$

Par construction des suites $(r^{(i)})_i$ et $(s^{(i)})_i$, on remarque que

$$(r^{(i_0-1)}, s^{(i_0-1)}) \in \{(r-1, s), (r, s-1)\}. \tag{1.33}$$

Comme $(r^{(i_0)}, s^{(i_0)}) = (r, s)$, on en déduit que pour montrer l'affirmation concernant le dernier saut, il suffit de montrer que

$$r > s \Leftrightarrow s^{(i_0-1)} = s \text{ ou } r^{(i_0-1)} = s^{(i_0-1)}.$$

De plus, pour montrer l'affirmation concernant le dernier groupe de ramification, il suffit de montrer, d'après (1.33), que

$$r^{(i_0-1)} = r-1 \Leftrightarrow r > s.$$

En résumé, pour montrer le corollaire, il suffit de montrer que les assertions suivantes sont équivalentes :

i) $r^{(i_0-1)} = r-1$;

ii) $s^{(i_0-1)} = s$ ou $r^{(i_0-1)} = s^{(i_0-1)}$;

iii) $r > s$.

i) $\Rightarrow$ *ii)* : si $r^{(i_0-1)} = r-1$, alors d'après (1.33), on obtient que $s^{(i_0-1)} = s$, ce qui montre l'implication souhaitée.

ii) $\Rightarrow$ *iii)* : supposons que $s^{(i_0-1)} = s$. De (1.33), il s'ensuit alors que $r^{(i_0-1)} = r-1$. De plus, du *iii)* du lemme 1.4.2, on en déduit que $r^{(i_0-1)} \geq s^{(i_0-1)}$. On obtient donc que

$$r = r^{(i_0-1)} + 1 \geq s^{(i_0-1)} + 1 = s+1.$$

Supposons maintenant que $s^{(i_0-1)} \neq s$ et que $r^{(i_0-1)} = s^{(i_0-1)}$. D'après (1.32), on a alors que

$$r = r^{(i_0)} = r^{(i_0-1)} + 1 = s^{(i_0-1)} + 1 > s+1.$$

On en déduit ainsi l'implication souhaitée.

iii) $\Rightarrow$ *i)* : supposons par l'absurde que $r^{(i_0-1)} \neq r-1$, i.e. que $r^{(i_0-1)} = r$ d'après (1.33). Il s'ensuit alors que $s^{(i_0-1)} = s-1$. Comme $r \geq s$, on obtient alors que $r^{(i_0-1)} > s^{(i_0-1)}$. D'après le *ii)* du lemme 1.4.2, cela signifie que $r^{(i_0-1)} = s^{(i_0-1)} + 1$, i.e. $r = s$ ce qui est absurde par hypothèse. On en déduit ainsi l'implication souhaitée, et donc le corollaire. □

Traitons à présent le cas $p \nmid v_F(a)$. Nous avons besoin, au préalable, de quelques inégalités concernant les fonctions $t_1(.,.)$ et $t_2(.,.)$ et de quelques propriétés concernant deux nouvelles suites $(r^{(i)})_i$ et $(s^{(i)})_i$ que l'on définira dans le lemme 1.4.6. Ces suites nous servirons pour décrire les sauts de $F_{r,s}/F$ (avec $r \geq s$) dans le cas où $p \nmid v_F(a)$.

Lemme 1.4.5. *Pour tout entier $s \geq 1$, on a*

i) $t_1(s+2,s) > t_2(s+1,s)$;

ii) $t_2(s+1,s) > t_1(s+1,s-1)$.

Démonstration. En utilisant le $v)$ et le *iii)* du théorème 1.3.6, on a que

$$\begin{aligned} t_1(s+2,s) - t_2(s+1,s) &= p^{2s+1} - \frac{2p^{2s+1}-p+1}{p+1} - \frac{2p^{2s}+p-1}{p+1} \\ &= p^{2s+1} - 2p^{2s} > 0. \end{aligned}$$

et

$$t_2(s+1,s) - t_1(s+1,s-1) = \frac{2p^{2s}+p-1}{p+1} - p^{2s-1} + \frac{2p^{2s+1}-p+1}{p+1}$$
$$= 2p^{2s} - p^{2s-1} > 0.$$

□

Lemme 1.4.6. *Soient $r \geq s$ des entiers positifs tels que $r \geq 1$. Construisons par récurrence deux suites d'entiers positifs $(r^{(i)})_i$ et $(s^{(i)})_i$ comme suit : $r^{(0)} = s^{(0)} = 0, r^{(1)} = 1, s^{(1)} = 0$ et, pour tout $i \geq 1$,*

$$(r^{(i+1)}, s^{(i+1)}) = \begin{cases} (\min\{r, r^{(i)}+1\}, s^{(i)}) \text{ si } s^{(i)} = s \\ (r^{(i)}, s^{(i)}+1) \text{ si } s^{(i)} \neq s \text{ et si } r^{(i)} = r \\ (r^{(i)}+1, s^{(i)}) \text{ si } s^{(i)} \neq s, \text{ si } r^{(i)} \neq r \text{ et si } r^{(i)} = s^{(i)}+1 \\ (r^{(i)}, s^{(i)}+1) \text{ si } s^{(i)} \neq s, \text{ si } r^{(i)} \neq r \text{ et si } r^{(i)} \neq s^{(i)}+1 \end{cases} . \tag{1.34}$$

On a alors les propriétés suivantes :

i) les suites $(r^{(i)})_i$ et $(s^{(i)})_i$ sont croissantes et stationnaires de limites respectives r et s. On note alors i_0 le plus petit entier i tel que $(r^{(i_0)}, s^{(i_0)}) = (r, s)$;

ii) soit $i \geq 1$ tel que $r^{(i)} \neq r$ et $s^{(i)} \neq s$. Alors $r^{(i)} \in \{s^{(i)}+1, s^{(i)}+2\}$;

iii) soit $i \geq 1$ tel que $r^{(i)} \neq r$. Alors $r^{(i)} \geq s^{(i)}+1$;

iv) pour tout $i \geq 0$, on a que $r^{(i)} \geq s^{(i)}$;

v) soit $i \geq 0$ tel que $s^{(i)} \neq s$. Alors $r^{(i)} \leq s^{(i)}+2$.

Démonstration. *i)* Remarquons que les suites $(r^{(i)})_i$ et $(s^{(i)})_i$ sont croissantes et majorées respectivement par r et s. Elles sont donc stationnaires. Notons r' la limite de $(r^{(i)})_i$ et s' celle de $(s^{(i)})_i$. Notons i_1 le plus petit entier tel que $s^{(i_1)} = s'$.

Supposons par l'absurde que $s' < s$. Supposons également par l'absurde que $r' < r$. Soit $i \geq i_1$ un entier. On ne peut donc pas avoir $r^{(i)} \neq s^{(i)}+1$ car cela signifierait, d'après (1.34), que $s' = s'+1$, ce qui est absurde. Il s'ensuit donc que $r^{(i)} = s^{(i)}+1 = s'+1$ pour tout $i \geq i_1$, ce qui est une nouvelle fois absurde puisque d'après (1.34), on aurait que $s'+1 = s'+2$. On a ainsi montré que $r' = r$.

Comme $s' < s$ et $r' = r$, on déduit alors de (1.34) que $s' = s'+1$, ce qui est encore une fois absurde.

On a ainsi montré que $s' = s$. En utilisant une fois encore (1.34), on en déduit que $r' = \min\{r, r'+1\}$, et donc que $r' = r$, ce qui montre *i)*.

ii) Il est clair que *ii)* est vide si $s = 0$ puisque $s^{(0)} = 0$. Supposons donc que $s > 0$. Comme $r \geq 1$ et que $r^{(0)} = s^{(0)} = 0$, on déduit alors du *i)* qu'il existe un plus grand entier $i_1 \geq 0$ tel que $r^{(i)} \neq r$ pour tout $i \leq i_1$.

Remarquons que si $i_1 = 0$, alors *ii)* est vide. Si $i_1 = 1$, alors *ii)* est clair puisque $r^{(1)} = 1$ et $s^{(1)} = 0$. Nous allons maintenant montrer *ii)* dans le cas où $i_1 \geq 2$.

Montrons *ii*) par récurrence pour $i \in \{1, \ldots, i_1\}$. Pour $i = 1$, c'est clair car $r^{(1)} = 1$ et $s^{(1)} = 0$. Supposons maintenant que *ii*) soit satisfait pour un certain $i \in \{1, \ldots, i_1 - 1\}$ et montrons qu'il l'est encore au rang $i + 1$.

Supposons que $r^{(i)} = s^{(i)} + 1$. Comme $s^{(i)} \neq s$ et que $r^{(i)} \neq r$ par hypothèse, on déduit alors de (1.34) que $s^{(i+1)} = s^{(i)}$ et que

$$r^{(i+1)} = r^{(i)} + 1 = s^{(i)} + 2 = s^{(i+1)} + 2,$$

ce qui montre l'hérédité.

Supposons maintenant que $r^{(i)} = s^{(i)} + 2$. Comme $s^{(i)} \neq s$ et que $r^{(i)} \neq r$ par hypothèse, on déduit alors de (1.34) que $s^{(i+1)} = s^{(i)} + 1$ et que

$$r^{(i+1)} = r^{(i)} = s^{(i)} + 2 = s^{(i+1)} + 1,$$

ce qui montre à nouveau l'hérédité. On a ainsi montré *ii*).

iii) Comme $r \geq 1$, on déduit alors du *i*) qu'il existe un plus grand entier i_1 tel que $r^{(i)} \neq r$ pour tout $i \leq i_1$. Remarquons que *iii*) est vide si $i_1 = 0$. Si $i_1 = 1$, alors *iii*) est clair puisque $r^{(1)} = 1$ et $s^{(1)} = 0$. Nous allons maintenant montrer *iii*) dans le cas où $i_1 \geq 2$.

Montrons *iii*) par récurrence pour $i \in \{1, \ldots, i_1\}$. Pour $i = 1$, c'est clair puisque $r^{(1)} = 1$ et $s^{(0)} = 0$. Supposons maintenant que *iii*) soit vrai pour un certain entier $i \in \{1, \ldots, i_1 - 1\}$ et montrons que *iii*) est encore vérifié au rang $i + 1$.

Si $s^{(i+1)} \neq s$, alors comme $r^{(i+1)} \neq r$, on a que $r^{(i+1)} \geq s^{(i+1)} + 1$ d'après *ii*). Si on suppose maintenant que $s^{(i)} = s$, alors d'après (1.34), on obtient donc que $s^{(i+1)} = s^{(i)}$ et que $r^{(i+1)} = \min\{r, r^{(i)} + 1\}$. Or, $r^{(i)} \neq r$ et $r^{(i)} \geq s^{(i)} + 1$ par hypothèse de récurrence. Il s'ensuit donc que

$$r^{(i+1)} = r^{(i)} + 1 \geq s^{(i)} + 2 = s^{(i+1)} + 2 \geq s^{(i+1)} + 1,$$

ce qui montre, une fois encore, l'hérédité dans ce cas.

Supposons maintenant que $s^{(i+1)} = s$ et que $s^{(i)} \neq s$. Comme $s^{(i+1)} \neq s^{(i)}$, on déduit alors de (1.34) que $s^{(i+1)} = s^{(i)} + 1$ et que $r^{(i+1)} = r^{(i)}$. De plus, comme $r^{(i)} \neq r$, cette situation ne peut se produire que si $r^{(i)} \neq s^{(i)} + 1$. Comme $s^{(i)} \neq s$, on déduit alors du *ii*) que $r^{(i)} = s^{(i)} + 2$. Des différentes formules que l'on a montrées, on obtient alors que

$$r^{(i+1)} = r^{(i)} = s^{(i)} + 2 = s^{(i+1)} + 1,$$

ce qui montre à nouveau l'hérédité dans ce cas. On en déduit maintenant *iii*).

iv) Si $i = 0$, alors *iv*) est clair puisque $r^{(0)} = s^{(0)} = 0$. Supposons donc que $i \geq 1$. Si $r^{(i)} \neq r$, alors le fait que $r^{(i)} \geq s^{(i)}$ découle du *iii*) de ce lemme. En revanche, si $r^{(i)} = r$, alors comme $r \geq s$ et que $s \geq s^{(i)}$ d'après le *i*), on en déduit aussitôt que $r^{(i)} \geq s^{(i)}$ et *iv*) s'ensuit.

v) Clairement, *v*) est vide si $s = 0$ puisque $s^{(0)} = 0$. Supposons donc à partir de maintenant que $s \geq 1$. D'après *i*), il existe un plus grand entier i_1 tel que $s^{(i)} \neq s$ pour tout $i \leq i_1$.

Si $i_1 = 0$, alors $v)$ est clair puisque $r^{(0)} = 0$ et $s^{(0)} = 0$. De même, si $i_1 = 1$, alors $v)$ est clair puisque $r^{(1)} = 1$ et $s^{(1)} = 0$. Supposons donc que $i_1 \geq 2$.

Montrons $v)$ par récurrence pour $i \in \{0, \ldots, i_1\}$. Pour $i = 0$ et $i = 1$, c'est clair d'après le paragraphe précédent. Supposons maintenant que $v)$ soit vrai pour un certain entier $i \in \{1, \ldots, i_1 - 1\}$ et montrons que $v)$ est encore vérifié au rang $i + 1$.

Si $r^{(i+1)} \neq r$, alors, comme $s^{(i+1)} \neq s$, on a que $r^{(i+1)} \leq s^{(i+1)} + 2$ d'après le $ii)$ de ce lemme. Si on suppose maintenant que $r^{(i)} = r$, alors comme $s^{(i)} \neq s$, on déduit de (1.34) que $r^{(i+1)} = r^{(i)}$ et que $s^{(i+1)} = s^{(i)} + 1$. Comme $s^{(i)} + 2 \geq r^{(i)}$ par hypothèse de récurrence, on en déduit alors que

$$s^{(i+1)} + 2 = s^{(i)} + 3 \geq r^{(i)} + 1 = r^{(i+1)} + 1,$$

ce qui montre une fois encore l'hérédité dans ce cas.

Supposons maintenant que $r^{(i+1)} = r$ et que $r^{(i)} \neq r$. Comme $r^{(i+1)} \neq r^{(i)}$, on déduit alors de (1.34) que $r^{(i+1)} = r^{(i)} + 1$ et que $s^{(i+1)} = s^{(i)}$. De plus, comme $s^{(i)} \neq s$ et que $r^{(i)} \neq r$, alors d'après (1.34), cette situation ne peut se produire que si $r^{(i)} = s^{(i)} + 1$. Des différentes formules que l'on a montrées, on obtient alors que

$$s^{(i+1)} + 2 = s^{(i)} + 2 = r^{(i)} + 1 = r^{(i+1)},$$

ce qui montre à nouveau l'hérédité dans ce cas. On en déduit maintenant $v)$.

□

On peut maintenant prouver le théorème 1.1.6. L'affirmation i) de ce théorème ayant été déjà prouvé dans le lemme 1.4.6, il nous reste à montrer :

Théorème 1.4.7. *Supposons que $p \nmid v_F(a)$. Soient $r \geq s$ des entiers positifs tels que $r \geq 1$. Reprenons les suites $(r^{(i)})_i$ et $(s^{(i)})_i$ définies dans le lemme 1.4.6. Alors les i_0 (cf lemme 1.4.6, i)) sauts de $F_{r,s}/F$ sont $\tau_0 = t_1(1,0) = 0$ et les*

$$\tau_i = \begin{cases} t_1(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} = s \\ t_2(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s \text{ et } r^{(i)} = r \\ t_1(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s,\ r^{(i)} \neq r \text{ et } r^{(i)} = s^{(i)} + 1 \\ t_2(r^{(i+1)}, s^{(i+1)}) \text{ si } s^{(i)} \neq s,\ r^{(i)} \neq r \text{ et } r^{(i)} \neq s^{(i)} + 1 \end{cases},$$

avec $i \in \{1, \ldots, i_0 - 1\}$. De plus, pour $i \in \{0, \ldots, i_0 - 1\}$, on a :

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_i} = \mathrm{Gal}(F_{r,s}/F_{r^{(i)},s^{(i)}}).$$

Démonstration. Par définition de i_0, on a $(r^{(i)}, s^{(i)}) \neq (r, s) = (r^{(i_0)}, s^{(i_0)})$ pour tout $i < i_0$. Remarquons que si $i_0 = 1$, alors le théorème est vérifié. En effet, si $i_0 = 1$, alors $(r, s) = (r^{(1)}, s^{(1)}) = (1, 0)$. D'après le lemme 1.1.4, $F_{1,0}/F$ a un unique saut égal à $t_1(1, 0)$. D'après le lemme 1.3.3, ce saut vaut 0. En particulier, 0 est le premier saut de $F_{1,0}/F$, i.e.

$$\mathrm{Gal}(F_{1,0}/F)_0 = \mathrm{Gal}(F_{1,0}/F).$$

On en déduit donc le théorème dans le cas où $i_0 = 1$ puisque $\tau_0 = t_1(1, 0) = 0$ et que $r^{(0)} = s^{(0)} = 0$ par construction des suites $(r^{(i)})_i$ et $(s^{(i)})_i$. Supposons à

partir de maintenant que $i_0 \geq 2$.

Pour tout $i \geq 0$, notons $K_i = F_{r^{(i)},s^{(i)}}$. Par définition des suites $(r^{(i)})_i$ et $(s^{(i)})_i$ et des sauts $t_1(.,.)$ et $t_2(.,.)$ (cf. lemme 1.1.4), on remarque alors que τ_i est l'unique saut de K_{i+1}/K_i.

On souhaite montrer que $0 = \tau_0 < \cdots < \tau_{i_0-1}$. Soit $i \in \{0, \ldots, i_0 - 2\}$ et montrons que $\tau_i < \tau_{i+1}$.

Supposons $i = 0$. On déduit alors de (1.34) que

$$(r^{(2)}, s^{(2)}) = \begin{cases} (2,0) \text{ si } s^{(1)} = s \\ (1,1) \text{ si } s^{(1)} \neq s \text{ et si } \ r^{(1)} = r \\ (2,0) \text{ si } s^{(1)} \neq s, \text{ si } r^{(1)} \neq r \text{ et si } r^{(1)} = s^{(1)} + 1 \\ (1,1) \text{ si } s^{(1)} \neq s, \text{ si } r^{(1)} \neq r \text{ et si } r^{(1)} \neq s^{(1)} + 1 \end{cases}.$$

Comme $(r^{(1)}, s^{(1)}) = (1,0) \neq (r,s)$ car $i_0 \geq 2$, il en résulte donc que

$$\tau_1 = \begin{cases} t_1(2,0) \text{ si } s = 0 \text{ ou } r \neq 1 \\ t_2(1,1) \text{ si } s \neq 0 \text{ et } r = 1 \end{cases}.$$

Or, $t_1(2,0) = p-1$ d'après le lemme 1.3.3 et $t_2(1,1) = p$ d'après le $ii)$ du lemme 1.3.4. D'où $0 = \tau_0 < \tau_1$.

Supposons à partir de maintenant que $i \geq 1$. Supposons également que $s^{(i)} = s$. Comme $i \leq i_0 - 2$, on a alors, par définition de i_0, que $r^{(i)} < r$ et que $r^{(i+1)} < r$. De (1.34), on a alors que

$$(r^{(i+1)}, s^{(i+1)}) = (r^{(i)} + 1, s) \text{ et } (r^{(i+2)}, s^{(i+2)}) = (r^{(i)} + 2, s).$$

Ainsi,

$$\tau_i = t_1(r^{(i)} + 1, s) \text{ et } \tau_{i+1} = t_1(r^{(i)} + 2, s).$$

En appliquant la remarque 1.1.3 avec $r = 2, r' = 1$ et avec $s' = s$, on obtient alors que $F_{2,s}/F_{1,s}$ est totalement ramifié. Il s'ensuit, en appliquant la proposition 1.2.9 à $K = F_{1,s}$ et à $\alpha = \zeta_p$ (et donc, $K_1 = F_{2,s}$), que la suite $(t_1(j,s))_{j \geq 1}$ est strictement croissante. En particulier, $\tau_i < \tau_{i+1}$.

À partir de maintenant, supposons que $s^{(i)} \neq s$. Supposons également que $r^{(i)} = r$. Comme $i \leq i_0 - 2$, on a alors, par définition de i_0, que $s^{(i)} < s$ et que $s^{(i+1)} < s$. De (1.34), on a alors que

$$(r^{(i+1)}, s^{(i+1)}) = (r, s^{(i)} + 1) \text{ et } (r^{(i+2)}, s^{(i+2)}) = (r, s^{(i)} + 2).$$

Ainsi,

$$\tau_i = t_2(r, s^{(i)} + 1) \text{ et } \tau_{i+1} = t_2(r, s^{(i)} + 2).$$

En appliquant la remarque 1.1.3 avec $s = 1, r' = r$ et avec $s' = 0$, on obtient alors que $F_{r,1}/F_{r,0}$ est totalement ramifié. Il s'ensuit, en appliquant la proposition 1.2.9 à $K = F_{r,0}$ et à $\alpha = a$ (et donc, $K_1 = F_{r,1}$), que la suite $(t_2(r,j))_{j \geq 1}$ est strictement croissante. En particulier, $\tau_i < \tau_{i+1}$.

Supposons en plus à partir de maintenant que $r^{(i)} \neq r$. Supposons également que $r^{(i)} \neq s^{(i)}+1$. Du $ii)$ du lemme 1.34, il s'ensuit alors que $r^{(i)} = s^{(i)}+2$. De (1.34), on en déduit alors que

$$(r^{(i+1)}, s^{(i+1)}) = (s^{(i)}+2, s^{(i)}+1).$$

Remarquons que $r^{(i+1)} \neq r$ puisque $r^{(i+1)} = r^{(i)} \neq r$. Remarquons également que $r^{(i+1)} = s^{(i+1)}+1$. Ainsi, que l'on aille $s^{(i)} = s$ ou $s^{(i)} \neq s$, on déduit alors de (1.34) que

$$(r^{(i+2)}, s^{(i+2)}) = (r^{(i+1)}+1, s^{(i+1)}) = (s^{(i)}+3, s^{(i)}+1).$$

On obtient donc que

$$\tau_i = t_2(s^{(i)}+2, s^{(i)}+1) \text{ et } \tau_{i+1} = t_1(s^{(i)}+3, s^{(i)}+1).$$

Le $i)$ du lemme 1.4.5, appliqué à $s = s^{(i)}+1$, montre alors que $\tau_i < \tau_{i+1}$.

Enfin, supposons que $r^{(i)} = s^{(i)}+1$. De (1.34), on en déduit alors que

$$(r^{(i+1)}, s^{(i+1)}) = (s^{(i)}+2, s^{(i)}).$$

Remarquons que $s^{(i+1)} \neq s$ puisque $s^{(i+1)} = s^{(i)} \neq s$. Remarquons également que $r^{(i+1)} = s^{(i+1)}+2$. Ainsi, que l'on aille $r^{(i)} = r$ ou $r^{(i)} \neq r$, on déduit de (1.34) que

$$(r^{(i+2)}, s^{(i+2)}) = (r^{(i+1)}, s^{(i+1)}+1) = (s^{(i)}+2, s^{(i)}+1).$$

On obtient alors que

$$\tau_i = t_1(s^{(i)}+2, s^{(i)}) \text{ et } \tau_{i+1} = t_2(s^{(i)}+2, s^{(i)}+1).$$

Le $ii)$ du lemme 1.4.5, appliqué à $s = s^{(i)}+1$, montre alors que $\tau_i < \tau_{i+1}$.

On a donc montré que $\tau_0 < \cdots < \tau_{i_0-1}$. D'après le $iv)$ du lemme 1.4.6, $r^{(i)} \geq s^{(i)}$ pour tout $i \geq 0$. L'extension K_i/F est donc galoisienne pour tout i. Comme τ_i est l'unique saut de K_{i+1}/K_i, le corollaire 1.2.3 montre donc que les sauts de $F_{r,s}/F$ sont les $\tau_0, \ldots, \tau_{i_0-1}$ et que $\mathrm{Gal}(F_{r,s}/F)_{\tau_i} = \mathrm{Gal}(F_{r,s}/K_i)$, ce qui correspond précisément aux sauts et aux groupes énoncés dans le théorème. □

Dans le corollaire ci-dessous, nous donnons explicitement la valeur du dernier saut de $\mathrm{Gal}(F_{r,s}/F)$, ainsi que le dernier groupe de ramification non trivial.

Corollaire 1.4.8. *Supposons que $p \nmid v_F(a)$. Soient $r \geq s$ des entiers positifs tels que $r \geq 1$. Alors le dernier saut de l'extension $F_{r,s}/F$ est $\tau_0 = 0$ si $i_0 = 1$ (lemme 1.4.6, i)) et*

$$\tau_{i_0-1} = \begin{cases} t_1(r,s) \text{ si } r > s+1 \\ t_2(r,s) \text{ si } r \in \{s, s+1\} \end{cases}$$

si $i_0 \geq 2$. De plus, le dernier groupe de ramification non trivial est égal à $\mathrm{Gal}(F_{r,s}/F)$ si $i_0 = 1$ et

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_{i_0-1}} = \begin{cases} \mathrm{Gal}(F_{r,s}/F_{r-1,s}) \text{ si } r > s+1 \\ \mathrm{Gal}(F_{r,s}/F_{r,s-1}) \text{ si } r \in \{s, s+1\} \end{cases}$$

si $i_0 \geq 2$.

Démonstration. Rappelons que $r^{(0)} = s^{(0)} = 0$. Si $i_0 = 1$, alors d'après le théorème 1.4.7, $\tau_0 = 0$ est l'unique saut de $F_{r,s}/F$. De plus, comme $F_{r,s}/F$ est totalement ramifié d'après le lemme 1.1.2, il s'ensuit que

$$\mathrm{Gal}(F_{r,s}/F)_0 = \mathrm{Gal}(F_{r,s}/F).$$

Le corollaire est ainsi vérifié dans le cas où $i_0 = 1$. Supposons maintenant que $i_0 \geq 2$.

Par définition de i_0, on a que $(r^{(i_0)}, s^{(i_0)}) = (r, s)$. De plus, d'après le (1.34) du lemme 1.4.6, il est clair que

$$(r^{(i_0-1)}, s^{(i_0-1)}) \in \{(r-1, s), (r, s-1)\}. \tag{1.35}$$

Ainsi, on a soit $r^{(i_0-1)} = r$, soit $s^{(i_0-1)} = s$. Du théorème 1.4.7, on en déduit alors que

$$\tau_{i_0-1} = \begin{cases} t_1(r^{(i_0)}, s^{(i_0)}) = t_1(r, s) \text{ si } s^{(i_0-1)} = s \\ t_2(r^{(i_0)}, s^{(i_0)}) = t_2(r, s) \text{ si } s^{(i_0-1)} \neq s \end{cases}$$

et que le dernier groupe de ramification non trivial est

$$\mathrm{Gal}(F_{r,s}/F)_{\tau_{i_0-1}} = \mathrm{Gal}(F_{r,s}/F_{r^{(i_0-1)}, s^{(i_0-1)}}).$$

Ainsi, pour montrer l'affirmation concernant le dernier saut, il suffit de montrer que

$$r > s + 1 \Leftrightarrow s^{(i_0-1)} = s.$$

De plus, pour montrer l'affirmation concernant le dernier groupe de ramification, il suffit de montrer que

$$r^{(i_0-1)} = r - 1 \Leftrightarrow r > s + 1.$$

En résumé, pour montrer le corollaire, il suffit de montrer que les assertions suivantes sont équivalentes :

i) $r^{(i_0-1)} = r - 1$;

ii) $s^{(i_0-1)} = s$;

iii) $r > s + 1$.

i) $\Rightarrow$ *ii)* : c'est clair car si $r^{(i_0-1)} = r - 1$, alors $s^{(i_0-1)} = s$ d'après (1.35).

ii) $\Rightarrow$ *iii)* : supposons que $s^{(i_0-1)} = s$, et donc que $r^{(i_0-1)} = r - 1$ d'après (1.35). D'après le *iii)* du lemme 1.4.6, on en déduit alors que

$$r = r^{(i_0-1)} + 1 \geq s^{(i_0-1)} + 2 = s + 2,$$

ce qui montre l'implication souhaitée.

iii) $\Rightarrow$ *i)* : supposons par l'absurde que $r^{(i_0-1)} \neq r - 1$. D'après (1.35), cela signifie que $r^{(i_0-1)} = r$ et que $s^{(i_0-1)} = s - 1$. Comme $r > s + 1$, il s'ensuit que $r^{(i_0-1)} > s^{(i_0-1)} + 2$, ce qui contredit le *v)* du lemme 1.4.6. On a ainsi montré l'implication souhaitée, et donc le corollaire. □

Nous allons conclure cette section en montrant que le dernier saut de l'extension $F_{r,s}/F$ est proche de l'indice de ramification de cette extension. Plus précisément, nous avons :

Proposition 1.4.9. *Soient $r \geq s$ des entiers positifs avec $(r,s) \neq (1,0)$. Notons T le dernier saut de $F_{r,s}/F$. Alors $p^3 T \geq e(F_{r,s}|F)$.*

Démonstration. Comme $(r^{(i)}, s^{(i)}) = (1,0)$, l'hypothèse $(r,s) \neq (1,0)$ équivaut à dire que $i_0 \geq 2$ (lemme 1.4.6, i)). Rappelons, d'après le lemme 1.1.2, que $e(F_{r,s}|F) = (p-1)p^{r+s-1}$. Commençons par le cas où $p \mid v_F(a)$. D'après le corollaire 1.4.4, on a alors que

$$T = \begin{cases} t_1(r,s) \text{ si } r > s \\ t_2(s,s) \text{ sinon} \end{cases}.$$

D'après le théorème 1.3.5, il s'ensuit que

$$T = \begin{cases} p^{r+s-1} - p^{2s} + \frac{p-1}{p+1}(p^{2s}-1) \text{ si } r > s \\ \\ p^{2s-1} - \frac{p-1}{p+1}(p^{2s-1}-1) \text{ sinon} \end{cases}.$$

Remarquons que, à quelques calculs élémentaires près, T correspond précisément au nombre l de [2, Proposition 2.1 2)]. Comme $p^3 T \geq p^2(T+1)$, le [2, Lemma 2.2] permet alors de montrer l'inégalité souhaitée dans le cas où $p \mid v_F(a)$.

Supposons maintenant que $p \nmid v_F(a)$. D'après le corollaire 1.4.8, on a alors que

$$T = \begin{cases} t_1(r,s) \text{ si } r > s+1 \\ t_2(r,s) \text{ sinon} \end{cases}.$$

D'après le théorème 1.3.5, il s'ensuit alors que

$$T = \begin{cases} \frac{p^{2s}+p^{2s-2}+p-1}{p+1} \text{ si } r = s \\ \\ \frac{2p^{2s}+p-1}{p+1} \text{ si } r = s+1 \\ \\ p^{r+s-1} - p^{2s} - \frac{2p^{2s+1}-p+1}{p+1} \text{ si } r > s+1 \end{cases}.$$

Commençons par le cas $r = s$. Nous allons montrer l'inégalité ci-dessous, qui est plus forte que celle demandée,

$$p^2 T \geq (p-1)p^{2s} = e(F_{s+1,s}|F).$$

Par quelques calculs élémentaires, cette inégalité est équivalente à l'inégalité $2p^{2s} + p^3 - p^2 > 0$, qui est clairement satisfaite. Le lemme est donc vérifié dans le cas $r = s$.

Supposons maintenant que $r = s+1$. Comme

$$T > \frac{p^{2s} + p^{2s-2} + p - 1}{p+1},$$

on en déduit alors que $p^2T \geq (p-1)p^{2s}$ d'après le paragraphe précédent. L'inégalité du lemme est ainsi également satisfaite dans le cas où $r = s+1$.

Pour finir, supposons que $r > s+1$. Pour pouvoir conclure, il suffit de montrer que

$$p^3\left(p^{r+s-1} - p^{2s} - \frac{2p^{2s+1} - p + 1}{p+1}\right) \geq (p-1)p^{r+s-1}.$$

Cette inégalité équivaut à montrer

$$p^{r+s+2} - p^{r+s} + p^{r+s-1} \geq p^{2s+3} + \frac{2p^{2s+4} - p^4 + p^3}{p+1}.$$

Il est clair que si cette inégalité est vraie pour $r = s+2$, alors elle est vraie pour tout $r > s+2$. Montrons donc que

$$p^{2s+4} - p^{2s+3} - p^{2s+2} + p^{2s+1} \geq \frac{2p^{2s+4} - p^4 + p^3}{p+1}.$$

Par quelques opérations élémentaires, cette inégalité est équivalente à :

$$p^{2s+2}(p^3 - 2p^2 - 2p + 1) \geq -p^4 + p^3,$$

qui est clairement vérifiée puisque le terme de droite est négatif, tandis que celui de gauche est positif. Ceci prouve le lemme. □

Chapitre 2

Généralisation d'un théorème de Galateau

Ce chapitre est quasimment un copier-coller de l'article [34]. La seule différence entre [34] et ce chapitre est le texte introductif de la section 2.2 qui a été rajouté (et qui est lui aussi un copier-coller d'une partie de l'introduction de cette thèse).

2.1 Rappels et notations.

2.1.1 Hauteur de Weil.

Soient K un corps de nombres, $x \in K$ et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ au-dessus d'un premier $p \in \mathbb{Q}$. Notons $v_{\mathfrak{p}}(x)$ la valuation de x en $\mathfrak{p}$ (i.e. l'exposant de $\mathfrak{p}$ dans la décomposition en idéaux premiers de $x\mathcal{O}_K$) et $|x|_{\mathfrak{p}} = p^{-v_{\mathfrak{p}}(x)/v_{\mathfrak{p}}(p)}$. L'ensemble des places finies de K est noté $\mathcal{M}^0(K)$ et celui des places infinies $\mathcal{M}^\infty(K)$. Notons également $\mathcal{M}(K) = \mathcal{M}^0(K) \cup \mathcal{M}^\infty(K)$. Pour tout $\nu \in \mathcal{M}^0(K)$, on confond ν et son idéal premier associé. De même, pour tout $\nu \in \mathcal{M}^\infty(K)$, on confond ν et ses plongements associés.

Soit ν une place de K. On note K_ν le complété de K en ν. Si $\nu \in \mathcal{M}^0(K)$, on note d_ν le degré local $[K_\nu : \mathbb{Q}_p]$ où p est le premier au-dessous de ν. De la même façon, si $\nu \in \mathcal{M}^\infty(K)$, on note $d_\nu = [K_\nu : \mathbb{R}]$.

Avec ces différentes notations, on a :

Proposition 2.1.1 (Formule du produit, Proposition 1.4.4, [10])**.** *Pour tout $x \in K^*$,*

$$\sum_{\nu \in \mathcal{M}(K)} d_\nu \log |x|_\nu = 0.$$

Définissons maintenant la hauteur logarithmique et absolue de Weil.

Définition 2.1.2. *Soient $x \in \overline{\mathbb{Q}}^*$ et K un corps de nombres le contenant. On définit la hauteur logarithmique et absolue de Weil, notée* $\mathrm{h}(x)$*, par :*

$$\mathrm{h}(x) = \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in \mathcal{M}(K)} d_\nu \log \max\{1, |x|_\nu\}.$$

Remarque 2.1.3. Cette hauteur est appelée absolue car elle ne dépend pas du corps contenant x (cf [10, §1.5]).

Pour simplifier, on désigne par le mot "hauteur" la hauteur logarithmique et absolue de Weil. Cette hauteur possède d'autres propriétés importantes comme celles ci-dessous (cf [10, Proposition 1.5.17, Lemma 1.5.18]) :

Proposition 2.1.4. *Soient $x \in \overline{\mathbb{Q}}$ et $\lambda \in \mathbb{Z}$. Alors $\mathrm{h}(x^\lambda) = |\lambda|\mathrm{h}(x)$ et, pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, on a $\mathrm{h}(\sigma(x)) = \mathrm{h}(x)$.*

La hauteur est aussi utilisée pour prouver la finitude d'un ensemble de points algébriques via le théorème fondamental ci-dessous :

Théorème 2.1.5 (Northcott, §1.6, [10])**.** *Fixons $B, D > 0$. Alors l'ensemble*

$$\{\alpha \in \overline{\mathbb{Q}}^* \mid \mathrm{h}(\alpha) \leq B \text{ et } [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq D\}$$

est fini.

Soit $\alpha \in \overline{\mathbb{Q}}^*$ tel que $\mathrm{h}(\alpha) = 0$. Alors, pour tout entier $k \geq 1$,

$$\mathrm{h}(\alpha^k) = k\,\mathrm{h}(\alpha) = 0.$$

Par le théorème 2.1.5, la suite $(\alpha^k)_{k\geq 1}$ ne possède alors qu'un nombre fini de termes distincts. Ainsi, $\alpha \in \mu_\infty$. La réciproque étant triviale, on en déduit que :

Proposition 2.1.6. *Soit $\alpha \in \overline{\mathbb{Q}}^*$. Alors, $\mathrm{h}(\alpha) = 0$ si et seulement si $\alpha \in \mu_\infty$.*

2.1.2 Corps de rayons.

Dans toute cette sous-section, K désigne un corps de nombres. Nous allons rappeler quelques propriétés utiles sur les corps de classes de rayons.

Définition 2.1.7. *Un K- module est un produit formel $\mathfrak{m} = \mathfrak{m}_f\infty$ où ∞ désigne le produit formel de tous les plongements réels de K et $\mathfrak{m}_f$ (appelée la partie finie) est un idéal non-nul de $\mathcal{O}_K$.*

À partir de maintenant, $\mathfrak{m} = \mathfrak{m}_f\infty$ désigne un K-module et on confondra souvent $\mathfrak{m}$ et $\mathfrak{m}_f$. De ce module, on peut construire deux groupes importants. Le premier, est le groupe abélien $J_\mathfrak{m}(K)$ composé de tous les idéaux fractionnaires de K premiers à $\mathfrak{m}_f$ et le second, noté $P_\mathfrak{m}(K)$, est le sous-groupe des idéaux principaux de $J_\mathfrak{m}(K)$ engendrés par a/b où

i) $a, b \in \mathcal{O}_K\backslash\{0\}$ et $\mathrm{pgcd}((a),(b)) = 1$,

ii) $a \equiv b \mod \mathfrak{m}$,

iii) $\sigma\left(\frac{a}{b}\right) > 0$ pour tout plongement réel σ de K.

Un groupe H est appelé *groupe idéal de module* $\mathfrak{m}$ si $P_\mathfrak{m}(K) \subset H \subset J_\mathfrak{m}(K)$. Notons $Cl_\mathfrak{m}(K, H)$ le groupe quotient $J_\mathfrak{m}(K)/H$. Alors :

Théorème 2.1.8. *([32, chapter 6, Proposition 1.8]) Pour tout groupe idéal H de module $\mathfrak{m}$, $Cl_\mathfrak{m}(K, H)$ est fini.*

En particulier, le théorème 2.1.8 appliqué à $\mathfrak{m}_f = (1)$ et à $H = P_{(1)}(K)$ montre que le groupe des classes classique est fini.

Soient K un corps de nombres, L/K une extension finie et $\mathfrak{m}$ un K-module. Notons

$$N_{\mathfrak{m}}(L/K) = \{\mathfrak{a} \subset K | \mathfrak{a} = N_{L/K}(\mathcal{A}),\ \mathcal{A} \text{ un idéal fractionnaire de } L,\ \text{pgcd}(\mathfrak{a}, \mathfrak{m}_f) = 1\}$$

et

$$H_{\mathfrak{m}}(L/K) = P_{\mathfrak{m}}(K) N_m(L/K).$$

Si L/K est galoisienne alors, par un théorème de Weber (cf [23]),

$$[J_{\mathfrak{m}}(K) : H_{\mathfrak{m}}(L/K)] \leq [L : K]. \tag{2.1}$$

On dit que L est un *corps de classes* (au sens de Takagi) sur K s'il existe un K-module $\mathfrak{m}$ tel que (2.1) soit une égalité. Un tel K-module est appelé un *module admissible* pour L/K. On dit également qu'un groupe idéal H (associé au K-module $\mathfrak{m}$) admet un corps de classes L si $H = H_{\mathfrak{m}}(L/K)$ et si (2.1) est une égalité.

Théorème 2.1.9 (Takagi). *Soit H un groupe idéal d'un K-module $\mathfrak{m}$. Alors :*

i) (Existence) H admet un corps de classes L.

ii) (Isomorphisme) si H admet un corps de classes L, alors $\text{Gal}(L/K) \simeq Cl_{\mathfrak{m}}(K, H)$.

iii) (Complétude) toute extension abélienne de K est un corps de classes sur K.

iv) (Comparaison) si H_1 (resp. H_2) est un groupe idéal associé au K-module $\mathfrak{m}$ et admet un corps de classes L_1 (resp. L_2), alors

$$L_1 \subset L_2 \Leftrightarrow H_2 \subset H_1.$$

v) (Décomposition) si H admet un corps de classes L, alors tout premier $\mathfrak{p}$ de $\mathcal{O}_K$ ne divisant pas $\mathfrak{m}$ est non ramifié dans L et son degré résiduel $f_{\mathfrak{p}}(L|K)$ est égal à l'ordre de $\mathfrak{p}$ dans $J_{\mathfrak{m}}(K)/H$.

Soient $\mathfrak{m}$ un K- module et H un groupe idéal de module $\mathfrak{m}$. Le *i)* et le *iv)* du théorème 2.1.9 prouvent respectivement l'existence et l'unicité du corps de classes pour H. Si $H = P_{\mathfrak{m}}(K)$, le corps de classes pour H est appelé corps de rayon et est noté $K_{\mathfrak{m}}$.

Soit L/K une extension abélienne finie. Alors, par le *iii)* du théorème 2.1.9, on peut trouver un K-module $\mathfrak{m}_1$ et un groupe idéal H_1 de module $\mathfrak{m}_1$ tels que L est un corps de classes pour H_1. Or, $P_{\mathfrak{m}_1}(K) \subset H_1$ et donc $L \subset K_{\mathfrak{m}_1}$ d'après le *iv)* du théorème 2.1.9. Ainsi, les corps de rayons jouent le rôle des extensions cyclotomiques dans le sens où toute extension abélienne finie de K est contenue dans un corps de rayon de K.

Le cas $\mathfrak{m} = (1)$ fournit des résultats déjà connus sur les corps de Hilbert. Dans ce cas, le corps de rayon est le corps de Hilbert du corps K.

2.1.3 Majoration du degré d'inertie.

On s'intéresse maintenant à la majoration du degré d'inertie dans un compositum de corps. Jusqu'à la fin de cette sous-section, fixons un premier rationnel p et un corps local $F/\mathbb{Q}_p$. Rappelons d'abord un résultat de Krasner qui donne le nombre d'extensions et d'extensions totalement ramifiées de F de degré fixé.

Théorème 2.1.10 (Krasner, Théorème 2, [28]). *Notons $\mathcal{N}_{F,d}$ le nombre d'extensions K/F de degré $d = hp^m$ avec $(h,p) = 1$ et $D = d[F : \mathbb{Q}_p]$. Alors*

$$\mathcal{N}_{F,d} = \left(\sum_{l|h} l\right)\left(\sum_{s=0}^{m} \frac{p^{m+s+1} - p^{2s}}{p-1}(p^{\epsilon(s)D} - p^{\epsilon(s-1)D})\right),$$

où $\epsilon(s) = p^{-1} + p^{-2} + ... + p^{-s}$ si $s > 0$, $\epsilon(0) = 0$ et $p^{\epsilon(s-1)D} = 0$ si $s = 0$.

De plus, si $\mathcal{N}_{F,d}^{(r)}$ désigne le nombre d'extensions totalement ramifiées K/F de degré d, alors

$$\mathcal{N}_{F,d}^{(r)} = d\sum_{s=0}^{m} p^s(p^{\epsilon(s)D} - p^{\epsilon(s-1)D}).$$

Le théorème de Krasner donne en particulier une majoration de l'indice de ramification et du degré d'inertie du compositum d'une famille d'extensions de F.

Corollaire 2.1.11. *Soit $(K_i/F)_{i\in\mathbb{N}}$ une famille d'extensions finies telle que la suite $([K_i : F])_i$ est majorée. Notons $\Gamma = \{[K_i : F], i \in \mathbb{N}\}$ et K le compositum des K_i. Alors*

$$e(K|F), f(K|F) \leq e(K|F)f(K|F) = [K : F] \leq \prod_{d\in\Gamma} d^{\mathcal{N}_{F,d}}.$$

Nous nous proposons de donner une majoration plus fine qui sera prouvée dans l'appendice. Par le théorème 2.1.10, la famille $(K_i/F)_{i\in\mathbb{N}}$ qui intervient dans le corollaire 2.1.11 est une famille finie; on la note maintenant $\{K_1/F, \ldots, K_n/F\}$. Quitte à permuter les corps $K_1, \ldots, K_n$, on suppose que $K_1/F, ..., K_m/F$ sont non sauvagement ramifiés et que $K_{m+1}/F, ..., K_n/F$ sont sauvagement ramifiés. Notons $e_i = e(K_i|F)$ et $f_i = f(K_i|F)$. Pour tout $r \in \{1, \ldots, n\}$, posons

$$\Lambda_r = \{e_1, \ldots, e_r\}. \tag{2.2}$$

Soit $e \in \Lambda_n$. Notons $\mathcal{N}(e)$ le nombre d'extensions K_i/F d'indice de ramification e. Enfin, pour tout premier q, on note

$$a_r(q) := \left(\sum_{e\in\Lambda_r} v_q(e)\right) - \max_{e\in\Lambda_r}(v_q(e)). \tag{2.3}$$

Théorème 2.1.12. *Si $m = n$, alors $e(K_1 \ldots K_n|F) = \mathrm{ppcm}(e_1, \ldots, e_n)$. Si $m < n$, alors*

$$e(K_1 \ldots K_n|F) \leq \mathrm{ppcm}(e_1, \ldots, e_{m+1}) e_{m+1}^{\mathcal{N}(e_{m+1})-1} \prod_{e\in\Lambda_n\setminus\Lambda_{m+1}} e^{\mathcal{N}(e)}.$$

On a également

$$f(K_1...K_n|F) \leq \text{ppcm}(f_1, ..., f_n)E$$

où

$$E = \prod_{e \in \Lambda_n} e^{\mathcal{N}(e)-1} \prod_{q \in \mathcal{P}} q^{a_n(q)} \tag{2.4}$$

si $m \geq n-2$ *et*

$$E = \prod_{e \in \Lambda_{m+2}} e^{-1} \prod_{q \in \mathcal{P}} q^{a_{m+2}(q)} \prod_{e \in \Lambda_n} e^{\mathcal{N}(e)} \tag{2.5}$$

si $m < n-2$.

La valeur de $e(K_1 \dots K_n|F)$ dans le cas où $m = n$ dans le théorème ci-dessus découle immédiatement du lemme d'Abhyankar ci-dessous :

Théorème 2.1.13 (Lemme d'Abhyankar, Theorem 3, [17]). *Soit $F/\mathbb{Q}_p$ une extension finie. Soient L_1/F et L_2/F deux extensions finies telles que $p \nmid e(L_1|F)$ ou $p \nmid e(L_2|F)$. Alors*

$$e(L_1L_2|F) = \text{ppcm}(e(L_1|F), e(L_2|F)).$$

Il n'est pas toujours aisé de savoir si deux extensions de F sont égales. Le nombre $\mathcal{N}(e)$ n'est donc pas toujours facile à calculer. Si l'on veut une majoration plus explicite du degré résiduel $f(K_1 \dots K_n|F)$, on peut majorer $\mathcal{N}(e)$ comme suit : soient $e \in \Lambda_n$ et $f \in \mathbb{N}^*$ et cherchons le nombre d'extensions L/F telles que

$$\begin{cases} e(L|F) = e \\ f(L|F) = f \end{cases}.$$

Notons $F\{f\}$ l'unique extension non ramifiée de F de degré f (cf [24, Chapter III, Theorem 25]). Alors, le nombre d'extensions de F de degré ef et d'indice de ramification e est égal au nombre d'extensions totalement ramifiées de $F\{f\}$ de degré e, i.e. à $\mathcal{N}^{(r)}_{F\{f\},e}$ qui se calcule à l'aide du théorème 2.1.10. On en déduit donc que

$$\mathcal{N}(e) \leq \sum_{f \in \Lambda(e)} \mathcal{N}^{(r)}_{F\{f\},e}, \tag{2.6}$$

où $\Lambda(e) = \{f \in \mathbb{N}^* | \ \exists i \in \{1, \dots, n\},\ e = e_i \text{ et } f = f_i\}$.

Remarque 2.1.14. Pour d'autres résultats concernant l'indice de ramification dans un compositum d'extensions sauvages bien particulières, le lecteur intéressé pourra voir [12] ou [20].

2.2 Résultat principal.

Pour un corps de nombres K, on note $H(K)$ le corps de Hilbert de K. Récemment, Galateau a montré que :

Théorème 2.2.1 (Galateau, §5, [25]). *Soit $(K_n/\mathbb{Q})_n$ une suite d'extensions finies telle que la suite $([K_n : \mathbb{Q}])_n$ est majorée. Si :*

i) $K_n/\mathbb{Q}$ est galoisienne pour tout n ;

ii) il existe un premier p inerte dans tous les K_n ;

iii) les discriminants des K_n sont deux à deux premiers entre eux ;

alors le compositum L de tous les $H(K_n)$ satisfait la propriété (B).

La condition *iii)* est assez restrictive. Par un théorème de Dirichlet (cf [24, Chapter III, theorem 22]), cela implique que tout premier $q \in \mathbb{Q}$ doit être ramifié dans au plus un des K_n. Galateau a conjecturé qu'à l'aide d'une étude locale, on pouvait se passer de cette condition.

Notre résultat principal consiste à supprimer les conditions *i)* et *iii)* du théorème 2.2.1 ainsi qu' à affaiblir la condition *ii)* en supposant seulement qu'il existe un unique idéal premier de $\mathcal{O}_{K_n}$ au-dessus de p. En particulier, on autorise p à être ramifié dans K_n.

Théorème 2.2.2. *Soit $(K_n/\mathbb{Q})_n$ une suite d'extensions finies telle que la suite $([K_n : \mathbb{Q}])_n$ est majorée. Supposons qu'il existe un premier $p \in \mathbb{Q}$ tel que pour tout n, il existe un unique idéal premier $\mathfrak{p}_n$ de $\mathcal{O}_{K_n}$ au-dessus de p. Alors le compositum L de tous les $H(K_n)$ satisfait la propriété (B).*

Avec notre idée, il est en fait possible de généraliser le théorème 2.2.2 en considérant des corps de rayons plutôt que des corps de Hilbert. Dans cette section, on se propose de montrer le théorème suivant :

Théorème 2.2.3. *Soient K un corps de nombres et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Soit $(K_n/K)_{n\in\mathbb{N}}$ une suite d'extensions finies telle que la suite $([K_n : K])_n$ est majorée et telle que pour tout n, il existe un unique idéal premier $\mathfrak{p}_n$ de $\mathcal{O}_{K_n}$ au-dessus de $\mathfrak{p}$. Fixons $M \geq 1$ un entier. Pour $n \in \mathbb{N}$, notons*

$$\Omega_n = \{\text{idéaux } \mathfrak{m} \subset \mathcal{O}_{K_n} |\ \exists m \leq M,\ p \nmid m,\ \text{et } \mathfrak{m} \text{ au-dessus de } m\}.$$

Pour $\mathfrak{m} \in \Omega_n$, notons $K_{n,\mathfrak{m}}$ le corps de rayon de K_n associé à $\mathfrak{m}$. Alors le compositum L de tous les $K_{n,\mathfrak{m}}$ a la propriété (B).

Pour retrouver le théorème 2.2.2, il suffit de prendre $K = \mathbb{Q}$, $\mathfrak{p} = p\mathbb{Z}$ et $M = 1$.

La démonstration repose sur une méthode désormais classique et qui sera utilisée dans le lemme ci-dessous.

2.2.1 Preuve du résultat principal

Soient K un corps de nombres, L/K une extension algébrique et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ au-dessus d'un premier rationnel p.

Définition 2.2.4. *Pour $e \in \mathbb{N}^*$, on définit les réels $\lambda(e, \mathfrak{p})$ et $\beta(e, \mathfrak{p})$ de la façon suivante. Soit k l'unique entier tel que*

$$p^{k-1}(p-1) \leq e < p^k(p-1),$$

et notons, pour $\lambda \in \mathbb{N}$, $\beta_\lambda(e, p) = p^{\min\{\lambda,k\}}/e + \max\{0, \lambda - k\}$. Alors on note $\lambda(e, \mathfrak{p})$ le plus petit entier positif tel que

$$\beta_{\lambda(e,\mathfrak{p})}(e, p)\ [K_\mathfrak{p} : \mathbb{Q}_p] \log p > [K : \mathbb{Q}] \log 2,$$

et on note $\beta(e, \mathfrak{p}) := \beta_{\lambda(e,\mathfrak{p})}(e, p)$.

Lemme 2.2.5. *Soit $\nu \mid \mathfrak{p}$ une place finie de $\mathcal{O}_L$. Supposons que les familles de réels $(f_\nu(L|\mathbb{Q}))_{\nu|\mathfrak{p}}$ et $(e_\nu(L|\mathbb{Q}))_{\nu|\mathfrak{p}}$ soient majorées respectivement par f et e. Alors L a la propriété (B). De plus, pour tout $x \in L\backslash\mu_\infty$,*

$$\mathrm{h}(x) \geq \frac{1}{p^{f+\lambda}+p^\lambda}\left(\frac{\beta[K_\mathfrak{p}:\mathbb{Q}_p]}{[K:\mathbb{Q}]}\log p - \log 2\right) > 0$$

où $\lambda = \lambda(e,\mathfrak{p})$ et $\beta = \beta(e,\mathfrak{p})$.

Démonstration. Soit $M \subset L$ un corps de nombres contenant K. Soit w une place de $\mathcal{O}_M$ au-dessus de $\mathfrak{p}$. Notons $f_w = f_w(M|\mathbb{Q})$ et $e_w = e_w(M|\mathbb{Q})$. Comme $\mathcal{O}_M/w\mathcal{O}_M \simeq \mathcal{O}_{M_w}/w\mathcal{O}_{M_w}$ et $e_w \leq e$, on déduit du petit théorème de Fermat que

$$|x^{p^{f_w}} - x|_w \leq p^{-1/e}$$

pour tout $x \in \mathcal{O}_{M_w}$. D'après [3, Lemma 2.1] [1] avec $\rho = 1/e$, on a

$$|x^{p^{f_w+\lambda}} - x^{p^\lambda}|_w \leq p^{-\beta}.$$

Pour avoir une majoration sur tout M, on utilise un argument d'Habegger (cf [26, Lemma 4.2]). Soit $x \in M_w$ tel que $x \in \mathcal{O}_{M_w}$. Alors

$$|x^{p^{f_w+\lambda}} - x^{p^\lambda}|_w \leq p^{-\beta}.$$

Soit $x \in M_w$ tel que $x \notin \mathcal{O}_{M_w}$. Alors $x^{-1} \in \mathcal{O}_{M_w}$ car $\mathcal{O}_{M_w}$ est un anneau de valuation. Ainsi, $|x^{-p^{f_w+\lambda}} - x^{-p^\lambda}|_w \leq p^{-\beta}$ ou encore

$$|x^{p^{f_w+\lambda}} - x^{p^\lambda}|_w \leq p^{-\beta}|x|_w^{p^{f_w+\lambda}+p^\lambda}.$$

Il s'ensuit donc que pour tout $x \in M_w$, et par conséquent pour tout $x \in M$, que

$$\begin{aligned} |x^{p^{f_w+\lambda}} - x^{p^\lambda}|_w &\leq p^{-\beta}\max\{1,|x|_w\}^{p^{f_w+\lambda}+p^\lambda} \\ &\leq p^{-\beta}\max\{1,|x|_w\}^{p^{f+\lambda}+p^\lambda} \end{aligned} \tag{2.7}$$

car $f_w \leq f$.

Soit $x \in M^*\backslash\mu_\infty$. Alors $x^{p^{f_w+\lambda}} - x^{p^\lambda} \neq 0$ et, par la formule du produit, on obtient

$$\begin{aligned} 0 &= \sum_{w\in\mathcal{M}(M)} \frac{d_w}{[M:\mathbb{Q}]}\log|x^{p^{f_w+\lambda}} - x^{p^\lambda}|_w \\ &= \sum_{w|\mathfrak{p}} \frac{d_w}{[M:\mathbb{Q}]}\log|x^{p^{f_w+\lambda}} - x^{p^\lambda}|_w + \sum_{w\nmid\mathfrak{p}} \frac{d_w}{[M:\mathbb{Q}]}\log|x^{p^{f_w+\lambda}} - x^{p^\lambda}|_w. \end{aligned}$$

En utilisant la majoration (2.7) et la formule (cf [10, Corollaire 1.3.2])

$$\sum_{w|\mathfrak{p}} d_w = [M:K][K_\mathfrak{p}:\mathbb{Q}_p]$$

[1] Une imprécision s'est glissée dans ce lemme. La dernière formule de l'énoncé doit s'écrire

$$s_{p,\rho}(\lambda) = p^{\min\{\lambda,k\}}\rho + \max\{0,\lambda-k\}$$

sur les places divisant $\mathfrak{p}$, on obtient que

$$0 \leq -\beta \frac{[K_{\mathfrak{p}} : \mathbb{Q}_p]}{[K : \mathbb{Q}]} \log p + (p^{f+\lambda} + p^{\lambda}) \sum_{w|\mathfrak{p}} \frac{d_w}{[M : \mathbb{Q}]} \log \max\{1, |x|_w\} + \sum_{w \nmid \mathfrak{p}} \frac{d_w}{[M : \mathbb{Q}]} \log |x^{p^{f_w+\lambda}} - x^{p^{\lambda}}|_w. \tag{2.8}$$

En utilisant les inégalités ultramétriques et triangulaires ainsi que la formule

$$\forall\ a, b \in \mathbb{R}^{+*},\ \log(a+b) \leq \log \max\{1, a\} + \log \max\{1, b\} + \log 2,$$

il en résulte que

$$\sum_{w \nmid \mathfrak{p}} \frac{d_w}{[M : \mathbb{Q}]} \log |x^{p^{f_w+\lambda}} - x^{p^{\lambda}}|_w \leq \sum_{\substack{w \nmid \mathfrak{p}, \\ w \in \mathcal{M}^0(M)}} \frac{d_w}{[M : \mathbb{Q}]} \log \max\{|x^{p^{f_w+\lambda}}|_w, |x^{p^{\lambda}}|_w\}$$
$$+ \sum_{\sigma \in \mathcal{M}^{\infty}(M)} \frac{d_\sigma}{[M : \mathbb{Q}]} \big(\log \max\{1, |x^{p^{f_w+\lambda}}|_w\} + \log \max\{1, |x^{p^{\lambda}}|_w\} + \log 2 \big).$$

En injectant cette inégalité dans (2.8) et en utilisant le fait que $f_w \leq f$, on en déduit que

$$0 \leq (p^{f+\lambda} + p^{\lambda}) \mathrm{h}(x) - \beta \frac{[K_{\mathfrak{p}} : \mathbb{Q}_p]}{[K : \mathbb{Q}]} \log p + \log 2$$

et donc que

$$\mathrm{h}(x) \geq \frac{1}{p^{f+\lambda} + p^{\lambda}} \left(\frac{\beta [K_{\mathfrak{p}} : \mathbb{Q}_p]}{[K : \mathbb{Q}]} \log p - \log 2 \right) > 0$$

par définition de β.

□

Nous sommes maintenant en mesure de prouver notre théorème :

Démonstration du théorème 2.2.3 :

Fixons K un corps de nombres et $(K_n/K)_n$ une suite d'extensions finies telle que la suite $(d_n)_n$ avec $d_n = [K_n : K]$ est majorée. Fixons également un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ au-dessus d'un premier rationnel p. Fixons $M \geq 1$ un entier. Pour $n \in \mathbb{N}$, notons

$$\Omega_n = \{\text{idéaux } \mathfrak{m} \subset \mathcal{O}_{K_n} |\ \exists m \leq M,\ p \nmid m, \text{ et } \mathfrak{m} \text{ au-dessus de } m\}.$$

Pour $\mathfrak{m} \in \Omega_n$, notons $K_{n,\mathfrak{m}}$ le corps de rayon de K_n associé à $\mathfrak{m}$.

On suppose que pour tout n, il existe un unique idéal premier $\mathfrak{p}_n$ de $\mathcal{O}_{K_n}$ au-dessus de $\mathfrak{p}$. On se propose de montrer que le compositum L de tous les $K_{n,\mathfrak{m}}$ a la propriété (B). Comme K est un corps de nombres fixé, on déduit du lemme 2.2.5 qu'il suffit de montrer que les familles de réels $(e_\nu(L|K))_{\nu|\mathfrak{p}}$ et $(f_\nu(L|K))_{\nu|\mathfrak{p}}$ sont majorées.

Pour cela, fixons ν une place de L au-dessus de $\mathfrak{p}$. Pour $n \in \mathbb{N}$ et $\mathfrak{m} \in \Omega_n$, notons $\nu_{n,\mathfrak{m}}$ la place de $K_{n,\mathfrak{m}}$ au-dessous de ν. On va montrer que la famille des degrés locaux $[(K_{n,\mathfrak{m}})_{\nu_{n,\mathfrak{m}}} : K_{\mathfrak{p}}]$ est majorée (par un réel indépendant de ν, n

et $\mathfrak{m}$). Car alors, les complétés $(K_{n,\mathfrak{m}})_{\nu_{n,\mathfrak{m}}}$ ($(n,\mathfrak{m}) \in \mathbb{N} \times \Omega_n$) étant en nombre fini d'après le théorème 2.1.10, on aura que L_ν est égal au compositum de tous les $(K_{n,\mathfrak{m}})_{\nu_{n,\mathfrak{m}}}$ et le corollaire 2.1.11 donnera bien l'existence d'une constante C indépendante de $\nu, n, \mathfrak{m}$ telle que $e_\nu(L|K) \leq C$ et $f_\nu(L|K) \leq C$.

Comme $[(K_{n,\mathfrak{m}})_{\nu_{n,\mathfrak{m}}} : K_\mathfrak{p}] = e_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K) f_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K)$, il suffit alors de majorer $e_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K)$ et $f_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K)$ par un réel indépendant de $\nu, n, \mathfrak{m}$.

Commençons par $e_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K_n)$. Par hypothèse, $\mathfrak{m}$ et p sont premiers entre eux. Comme $\mathfrak{p}_n \mid p$, on en déduit que $\mathfrak{p}_n \nmid \mathfrak{m}$. Ainsi, d'après le v) du théorème 2.1.9,

$$e_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K_n) = 1. \tag{2.9}$$

Intéressons nous maintenant au degré d'inertie $f_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K_n)$. D'après le v) du théorème 2.1.9, $f_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K_n)$ est le plus petit entier h tel que $\mathfrak{p}_n^h \in P_\mathfrak{m}(K_n)$, i.e. tel que

i) $\mathfrak{p}_n^h$ est principal. Notons $\gamma \in \mathcal{O}_{K_n}$ un générateur de $\mathfrak{p}_n^h$.

ii) $\gamma \equiv 1 \mod \mathfrak{m}$,

iii) pour tout plongement réel $\sigma : K_n \hookrightarrow \mathbb{R}$, on a $\sigma(\gamma) > 0$.

Notons

$$N = \text{ppcm}(j \mid j = 1, \ldots, M \,, \text{pgcd}(j, p) = 1). \tag{2.10}$$

Notons également $f_\mathfrak{p}(K)$ l'ordre de $\mathfrak{p}$ dans $Cl(K)$ (le groupe des classes de K) et (α) l'idéal $\mathfrak{p}^{f_\mathfrak{p}(K)}$.

Si $N \neq 1$, alors comme $\mathfrak{p}$ est au-dessus de p et que $p \nmid N$, on a

$$\alpha \in (\mathcal{O}_K / N\mathcal{O}_K)^\times .$$

Ainsi, pour tout N, il existe un plus petit entier strictement positif g tel que $\alpha^g \equiv 1 \mod N\mathcal{O}_K$ (on a $g = 1$ si $N = 1$).

Par hypothèse, il existe un unique idéal $\mathfrak{p}_n$ de $\mathcal{O}_{K_n}$ au-dessus de $\mathfrak{p}$. Par conséquent, $\mathfrak{p}\mathcal{O}_{K_n} = \mathfrak{p}_n^{e_{\mathfrak{p}_n}(K_n|K)}$. Ainsi, $\mathfrak{p}_n^{h_n}$ avec

$$h_n := 2 f_\mathfrak{p}(K) e_{\mathfrak{p}_n}(K_n|K) g \tag{2.11}$$

vérifie les conditions i), ii) et iii) ci-dessus. En effet, un rapide calcul montre que $\mathfrak{p}_n^{h_n} = (\alpha^{2g})$. Ainsi, i) est vérifié. Comme $\alpha^g \equiv 1 \mod N\mathcal{O}_K$ et que $\mathfrak{m} \mid N\mathcal{O}_{K_n}$, il s'ensuit que $\alpha^{2g} \equiv 1 \mod \mathfrak{m}$, ce qui montre ii). Enfin, iii) est vérifié car si $\sigma : K_n \hookrightarrow \mathbb{R}$, alors $\sigma(\alpha^{2g}) = (\sigma(\alpha))^{2g} > 0$. Ainsi, $\mathfrak{p}_n^{h_n} \in P_\mathfrak{m}(K_n)$.

On a donc montré l'inégalité $f_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K_n) \leq h_n$. Par ailleurs, la suite $(d_n)_n$ est majorée par hypothèse. Par conséquent, la suite $(e_{\mathfrak{p}_n}(K_n|K))_n$ est majorée. De (2.11), il devient alors clair que la suite $(h_n)_n$ est majorée. On a ainsi majoré $f_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K_n)$ par une constante ne dépendant pas de ν, n et $\mathfrak{m}$. Ceci prouve le théorème. □

Remarquons que si $M = 1$, alors $K_{n,\mathfrak{m}}$ correspond au corps de Hilbert de K_n. Ainsi, le cas $M = 1$ et $K = \mathbb{Q}$ de ce théorème correspond au théorème 2.2.2.

Remarque 2.2.6. En utilisant le théorème 2.1.12 à la place du corollaire 2.1.11, il est possible de donner une majoration explicite plus précise des familles $(e_\nu(L|\mathbb{Q}))_{\nu|\mathfrak{p}}$ et $(f_\nu(L|\mathbb{Q}))_{\nu|\mathfrak{p}}$. Puis, en utilisant le lemme 2.2.5, on en déduit une minoration explicite de la hauteur.

On reprend les notations du théorème 2.2.3. Pour $n \in \mathbb{N}$, posons $e_n = e_{\mathfrak{p}_n}(K_n|K)$. Soit $\nu \in \mathcal{M}(L)$ au-dessus de $\mathfrak{p}$. De (2.9), on a $e_n = e_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K)$ pour tout $\mathfrak{m} \in \Omega_n$.

Notons Λ l'ensemble des entiers e_n divisibles par p. Si $\Lambda = \emptyset$, alors d'après le théorème 2.1.12, un majorant de $e_\nu(L|\mathbb{Q})$ est

$$e := e_{\mathfrak{p}}(K|\mathbb{Q})\mathrm{ppcm}_{n\in\mathbb{N}}(e_n) \tag{2.12}$$

(car nous n'avons pas d'extensions sauvagement ramifiées et donc $m = n$). Remarquons que dans ce cas, e ne dépend pas de ν.

Supposons maintenant que $\Lambda \neq \emptyset$. Soit $\tilde{e} \in \Lambda$. Alors d'après le théorème 2.1.12, un majorant de $e_\nu(L|K)$ est

$$e := e_{\mathfrak{p}}(K|\mathbb{Q}) \operatorname*{ppcm}_{m\in\mathbb{N},\, p\nmid e_m} (e_m, \tilde{e})\, \tilde{e}^{\mathcal{N}(\tilde{e})-1} \prod_{\substack{e'\in\Lambda \\ e'\neq\tilde{e}}} e'^{\mathcal{N}(e')} \tag{2.13}$$

où $\mathcal{N}(e')$ désigne le nombre d'extensions $\{(K_{n,\mathfrak{m}})_{\nu_{n,\mathfrak{m}}}/K_{\mathfrak{p}}|\ n \in \mathbb{N}, \mathfrak{m} \in \Omega_n\}$ dont l'indice de ramification est précisément e'. Comme $e_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K_n) = 1$ (cf (2.9)), cela implique que $\mathcal{N}(e')$ est aussi le nombre d'extensions $\{K_n/K, n \in \mathbb{N}\}$ dont l'indice de ramification est précisément e'. Ainsi, $\mathcal{N}(e')$, et donc e, ne dépend pas de ν.

Calculons maintenant un majorant de la famille $(f_\nu(L|K))_{\nu|\mathfrak{p}}$. Notons, comme dans la preuve du théorème 2.2.3, α un générateur de $\mathfrak{p}^{f_{\mathfrak{p}}(K)}$. Notons $g_{\mathfrak{m}}$ le plus petit entier strictement positif tel que $\alpha^{g_{\mathfrak{m}}} \equiv 1 \mod \mathfrak{m}$. Définissons également $\epsilon_{\mathfrak{m}}$ comme suit : $\varepsilon_{\mathfrak{m}}$ vaut 1 si $\sigma(\alpha^{g_{\mathfrak{m}}}) > 0$ pour tout plongement réel $\sigma : K_n \hookrightarrow \mathbb{R}$ et 2 sinon. Par un calcul similaire à celui effectué dans la preuve du théorème 2.2.3, on en déduit que

$$f_{\nu_{n,\mathfrak{m}}}(K_{n,\mathfrak{m}}|K_n) \mid \varepsilon_{\mathfrak{m}}\ f_{\mathfrak{p}}(K)\ e_n g_{\mathfrak{m}}.$$

Comme $d_n = e_n f_{\mathfrak{p}_n}(K_n|K)$, le théorème 2.1.12 montre qu'un majorant de $f_\nu(L|\mathbb{Q})$ est

$$f := f_{\mathfrak{p}}(K|\mathbb{Q}) f_{\mathfrak{p}}(K) \operatorname*{ppcm}_{n\in\mathbb{N},\mathfrak{m}\in\Omega_n} (\varepsilon_{\mathfrak{m}}\, g_{\mathfrak{m}} d_n) E \tag{2.14}$$

pour un certain E explicitement calculable (cf (2.4) et (2.5)) ne dépendant pas de ν.

En reprenant les notations de la définition 2.2.4, on déduit du lemme 2.2.5 que pour tout $x \in L^*\backslash\mu_\infty$,

$$\mathrm{h}(x) \geq \frac{1}{p^{f+\lambda} + p^\lambda} \left(\frac{\beta[K_{\mathfrak{p}} : \mathbb{Q}_p]}{[K : \mathbb{Q}]} \log p - \log 2 \right) > 0$$

où $\lambda = \lambda(e, \mathfrak{p})$ et $\beta = \beta(e, \mathfrak{p})$.

Remarquons que la minoration de la hauteur ci-dessus reste strictement positive si, à la place de e, on prend un majorant quelconque de la famille $(e_\nu(L|\mathbb{Q}))_{\nu|\mathfrak{p}}$.

2.2.2 Exemples.

Dans cette sous-section, on donne quatre exemples de corps ayant la propriété (B) ainsi qu'une minoration explicite de la hauteur. Les deux premiers sont des généralisations d'exemples déjà illustrés dans [25].

Dans ces quatre exemples, on se place dans le cas particulier où $M = 1$ et $K = \mathbb{Q}$. Par conséquent, $f_{\mathfrak{p}}(K) = 1$. Il s'ensuit donc que $(\alpha) = \mathfrak{p} = p\mathbb{Z}$. On peut ainsi supposer que $\alpha = p$. Comme $M = 1$, il s'ensuit que $\Omega_n = \{\mathcal{O}_{K_n}\}$ et donc que $\mathfrak{m} = (1)$. Ainsi, $K_{n,\mathfrak{m}} = H(K_n)$. De plus, par définition de $g_{\mathfrak{m}}$ et de $\epsilon_{\mathfrak{m}}$, il s'ensuit que $g_{\mathfrak{m}} = \epsilon_{\mathfrak{m}} = 1$. De (2.14), il en résulte, dans cette situation, que $f = \mathrm{ppcm}_{n\in\mathbb{N}}(d_n)E$ où $d_n = [K_n : \mathbb{Q}]$ et où E est défini comme dans (2.4) ou (2.5).

Pour un corps de nombres K, notons Δ_K son discriminant.

Exemple 2.2.7. Fixons un premier $p > 3$. Pour un entier D non nul et sans facteur carré, notons $K_D = \mathbb{Q}(\sqrt{D})$. Notons également

$$\mathcal{D} = \{D \in \mathbb{Z}\backslash\{0\} \mid p\mathcal{O}_{K_D} \text{ est premier ou totalement ramifié}\}$$

et L le compositum des $H(K_D)$ avec $D \in \mathcal{D}$. On souhaite minorer la hauteur des éléments de $L^*\backslash\mu_\infty$.

Le théorème 2.1.10 montre qu'il y a deux extensions quadratiques de $\mathbb{Q}_p$ totalement ramifiées (que l'on note K_1 et K_2) et une seule non ramifiée (que l'on note K_3). Il s'ensuit donc que $a_3(q) = 0$ (cf (2.3)) pour tout premier q. Comme aucune extension n'est sauvagement ramifiée, on en déduit alors que $E = 2$ (cf (2.4)) et que $e = 2$. On a également $d_n = 2$ pour tout n. Par conséquent, $f = 4$. Avec les notations de la définition 2.2.4, on obtient $\lambda(e, p) = 0$ car $p \geq 5$ et $\beta(e, p) = 1/2$. La minoration de la hauteur que l'on a obtenue dans la remarque 2.2.6 montre donc que pour tout $x \in L^*\backslash\mu_\infty$,

$$\mathrm{h}(x) \geq \frac{\log(p/4)}{2(p^4+1)}.$$

Dans [25, § 5], l'auteur obtenait la minoration $(\log(p/2))/(p^2+1)$. Cependant, il montra que cette minoration est valable non pas pour L, mais pour le compositum des $H(K_D)$ avec $D \in \mathcal{D}_0$ où

$$\mathcal{D}_0 = \{D \in \mathbb{N}^* \mid D \text{ est premier, } p\mathcal{O}_{K_{-D}} \text{ est premier et } D \equiv 3 \mod 4\}.$$

Il doit supposer en plus que $D \equiv 3 \mod 4$ afin que $\Delta_{\mathbb{Q}(\sqrt{-D})} = -D$ et que $D = p$ est premier afin que les $\Delta_{\mathbb{Q}(\sqrt{-p})}$ soient deux à deux premiers entre eux.

La différence entre nos deux minorations provient du fait que dans notre situation, p se ramifie. Si p ne se ramifie pas (comme c'est le cas si on considère l'ensemble des entiers D non nuls et sans facteur carré tels que $p\mathcal{O}_{K_D}$ est premier), on a $e = 1$, $E = 1$ et $\beta(e, p) = 1$. On obtient ainsi $(\log(p/2))/(p^2+1)$ comme minoration au lieu de $(\log(p/4))/(2(p^4+1))$. Cette minoration a également été obtenue par Pottmeyer dans [35, Theorem 2.3].

Exemple 2.2.8. Dans [41], l'auteur étudie le corps de décomposition (« simplest cubic field ») K_m du polynôme

$$P_m(X) = X^3 - mX^2 - (m+3)X - 1$$

avec $m \in \mathbb{N}$. Pour tout m, l'extension $K_m/\mathbb{Q}$ est galoisienne de degré 3. Ainsi, $K_m = \mathbb{Q}(x_m)$ où x_m est une racine de P_m. On a également que le discriminant $\mathrm{disc}(\mathrm{P_m})$ du polynôme P_m vaut $(m^2+3m+9)^2$.

Montrons que 2 est inerte dans tous les K_m. Il est clair que P_m, vu comme un polynôme de $\mathbb{F}_2[X]$, est irréductible (c'est un polynôme de degré 3 ne possédant pas de racine dans $\mathbb{F}_2$). Par conséquent, P_m est irréductible dans $\mathbb{Z}_2[X]$. Comme $K_m = \mathbb{Q}(x_m)$, on déduit d'un lemme de Kummer (cf [13, Chapter 2, section 10]) qu'il n'y a qu'un seul idéal premier au-dessus de 2. Comme 2 ne se ramifie pas dans K_m (car $\mathrm{disc}(\mathrm{P_m})$ est impair et que l'on a $\mathrm{disc}(\mathrm{P_m}) = [\mathcal{O}_{\mathrm{K_m}} : \mathbb{Z}[\mathrm{x_m}]]^2 \Delta_{\mathrm{K_m}}$), il s'ensuit que 2 est bien inerte dans K_m.

D'après le théorème 2.2.3, le compositum L de tous les $H(K_m)$ a la propriété (B). Nous pouvons être plus explicite. Ici, on est dans le cas où $p = 2$. Comme il n'y a pas de ramification, on a $e = 1$ d'après (2.12) et $E = 1$ d'après (2.4). On a également $d_n = 3$ pour tout n. Par conséquent, $f = 3$. Enfin, avec les notations de la définition 2.2.4, on a $\lambda(e,p) = 1$ et donc $\beta(e,p) = 2$. La minoration de la hauteur que l'on a obtenue montre donc que pour tout $x \in L^* \backslash \mu_\infty$,

$$\mathrm{h}(x) \geq \frac{\log 2}{18}.$$

À cause des restrictions nécessaires pour appliquer son théorème, Galateau s'intéresse aux corps K_m dont l'anneau des entiers est $\mathbb{Z}[x_m]$, ce qui permet d'en déduire la relation $\mathrm{disc}(\mathrm{P_m}) = \Delta_{\mathrm{K_m}}$ et donc que $\Delta_{K_m} = (m^2+3m+9)^2$. Il a ensuite montré qu'il existe un ensemble infini $\mathcal{N}$ tel que l'anneau des entiers de K_m, pour $m \in \mathcal{N}$, est $\mathbb{Z}[x_m]$ et tel que les $(\Delta_{K_m})_{m\in\mathcal{N}}$ sont deux à deux premiers entre eux. Il peut ainsi appliquer son théorème et obtenir que le compositum L_0 des $H(K_m)$ avec $m \in \mathcal{N}$ a la propriété (B). Pour ce corps, il obtient la même minoration que la nôtre.

Notre théorème permet d'obtenir d'autres exemples. Nous allons en voir deux. Le premier ne contient que des extensions non sauvagement ramifiées tandis que le second en contiendra.

Le lecteur pourra remarquer que la minoration de la hauteur dans l'exemple 2.2.9 est de bien meilleure qualité que dans l'exemple 2.2.10.

Exemple 2.2.9. Plaçons nous dans le cas où $p = 3$. Soit S l'ensemble des corps de degrés 2, 4 ou 5 tel que pour tout $K \in S$, il existe un unique idéal premier $\mathfrak{p}_K$ de $\mathcal{O}_K$ au-dessus de 3. Notons L le compositum de tous les $H(K)$ pour $K \in S$.

Comme la suite $([K_{\mathfrak{p}_K} : \mathbb{Q}_3])_{K\in S}$ est majorée par 5, le théorème 2.1.10 montre que l'ensemble $\{K_{\mathfrak{p}_K}, K \in S\}$ est fini. Notons $K_1, \ldots, K_n$ les localisés $K_{\mathfrak{p}_K}$ avec $K \in S$.

Soit ν une place de $\mathcal{O}_L$ au-dessus de 3 (ν est donc au-dessus de chacun des $\mathfrak{p}_K$ par unicité de l'idéal premier au-dessus de 3). Comme $K_j/\mathbb{Q}_3$ est non sauvagement ramifié pour tout $j \leq n$, il découle de (2.12) que

$$e = \mathrm{ppcm}(1,2,4,5) = 20.$$

Comme $2\ 3^{3-1} \leq 20 < 2\ 3^3$, on en déduit, avec les notations de la définition 2.2.4, que $\lambda(e,p) = 3$ et donc que $\beta(e,p) = 1,35$.

Enfin, $f(K_j|\mathbb{Q}_3)e(K_j|\mathbb{Q}_3) \leq 5$. On obtient donc que

$$\begin{cases} f(K_j|\mathbb{Q}_3) = 1 \text{ si } e(K_j|\mathbb{Q}_3) \geq 3 \\ f(K_j|\mathbb{Q}_3) \in \{1,2\} \text{ si } e(K_j|\mathbb{Q}_3) = 2 \\ f(K_j|\mathbb{Q}_3) \leq 5 \text{ si } e(K_j|\mathbb{Q}_3) = 1 \end{cases}.$$

On déduit alors de (2.6) et du théorème 2.1.10 que $\mathcal{N}(2) \leq 2+2 = 4$; $\mathcal{N}(4) \leq 4$ et $\mathcal{N}(5) \leq 5$. Enfin, $a_n(2) = 1$ et $a_n(q) = 0$ pour les premiers impairs (cf (2.3)). On en déduit que

$$f \leq \text{ppcm}(2,4,5)\ 2^3\ 4^3\ 5^4\ 2 = 20\ 2^3\ 4^3\ 5^4\ 2 = 1.28\ 10^7.$$

Ainsi, pour tout $x \in L^*\backslash\mu_\infty$, on a

$$\text{h}(x) \geq \frac{0.78}{3^{f+3}+3^3} \geq e^{-1.41\ 10^7}.$$

Exemple 2.2.10. Plaçons nous de nouveau dans le cas où $p = 3$. Soit S l'ensemble des corps de degré ≤ 5 tel que pour tout $K \in S$, il existe un unique idéal premier $\mathfrak{p}_K$ de $\mathcal{O}_K$ au-dessus de 3. Notons L le compositum de tous les $H(K)$ pour $K \in S$.

Comme la suite $([K_{\mathfrak{p}_K} : \mathbb{Q}_3])_{K\in S}$ est majorée par 5, le théorème 2.1.10 montre que l'ensemble $\{K_{\mathfrak{p}_K}, K \in S\}$ est fini. Notons $K_1, \ldots, K_n$ les localisés $K_{\mathfrak{p}_K}$ avec $K \in S$.

Notons m le nombre d'extensions $K_j/\mathbb{Q}_3$ non sauvagement ramifiées. Quitte à renuméroter, on peut supposer que ces m extensions sont $K_1/\mathbb{Q}_3, \ldots, K_m/\mathbb{Q}_3$. Les extensions sauvagement ramifiées ont un indice de ramification égal à 3. Ainsi, (cf (2.2) pour la définition de Λ_r)

$$\Lambda_{m+1} = \Lambda_{m+2} = \Lambda_n = \{1, \ldots, 5\}.$$

Comme $f(L_j|\mathbb{Q}_3)e(L_j|\mathbb{Q}_3) \leq 5$, on en déduit que

$$\begin{cases} f(K_j|\mathbb{Q}_3) = 1 \text{ si } e(K_j|\mathbb{Q}_3) \geq 3 \\ f(K_j|\mathbb{Q}_3) \in \{1,2\} \text{ si } e(K_j|\mathbb{Q}_3) = 2 \\ f(K_j|\mathbb{Q}_3) \leq 5 \text{ si } e(K_j|\mathbb{Q}_3) = 1 \end{cases}.$$

Par conséquent, le (2.6) et le théorème 2.1.10 montrent que $\mathcal{N}(2) \leq 2+2 = 4$, $\mathcal{N}(3) \leq 21$, $\mathcal{N}(4) \leq 4$ et $\mathcal{N}(5) \leq 5$. Enfin, $a_{m+2}(2) = 1$ et $a_{m+2}(q) = 0$ pour les premiers impairs q. Par conséquent,

$$f \leq \text{ppcm}(1,2,\ldots,5)\frac{1}{5!}\ 2\ 2^4\ 3^{21}\ 4^4\ 5^5.$$

De plus, d'après (2.13), $\text{ppcm}(1,2,\ldots,5)\ 3^{\mathcal{N}(3)-1}$ est un majorant de la famille $(e_\nu(L|\mathbb{Q}))_{\nu|3}$. Il s'ensuit donc que $e_1 = 60\ 3^{20}$ est un majorant de la famille $(e_\nu(L|\mathbb{Q}))_{\nu|3}$.

Avec les notations de la définition 2.2.4, on a $\lambda(e_1, p) = 24$. Ainsi, $\beta(e_1, p) = 1,35$ et donc, pour tout $x \in L^*\backslash\mu_\infty$, on a

$$\text{h}(x) \geq \frac{0.78}{3^{f+24}+3^{24}} \geq e^{-3.6\ 10^{18}}.$$

2.3 Un problème de densité.

Fixons un premier q. Pour un corps K, on notera Δ_K son discriminant. Dans [25], Galateau s'est intéressé à la densité de corps quadratiques tels que q est inerte dans chacun de ces corps et tels que leurs discriminants sont deux à deux premiers entre eux, conditions nécessaires dans sa preuve. Comme un corps quadratique est de la forme $\mathbb{Q}(\sqrt{D})$ pour un certain entier D non nul sans facteur carré, cela revient à déterminer la densité naturelle d'ensembles d'entiers sans facteur carré D vérifiant les conditions de l'hypothèse ci-dessous, pour q un premier fixé :

Hypothèse 2.3.1.

i) q est inerte dans $\mathbb{Q}(\sqrt{D})$;

ii) les $\Delta_{\mathbb{Q}(\sqrt{D})}$ sont deux à deux premiers entre eux.

Cette densité valant 0 puisque les D doivent être deux à deux premiers entre eux, l'auteur considère plutôt la densité de Dirichlet des premiers D vérifiant les conditions de l'hypothèse 2.3.1.

Notons $\mathcal{P}$ l'ensemble des nombres premiers. Soit X un sous-ensemble de $\mathcal{P}$. Si la limite

$$\lim_{s\to 1^+} \frac{-1}{\log(s-1)} \sum_{p\in X} \frac{1}{p^s}$$

existe, alors on dira que X admet une densité de Dirichlet, notée $\mathcal{D}(X)$, égale à la valeur de cette limite. Par exemple, si X est fini, alors $\mathcal{D}(X) = 0$ et $\mathcal{D}(\mathcal{P}) = 1$ (théorème de Dirichlet).

Galateau a montré :

Proposition 2.3.2. *([25, Lemma 3.1]) Il existe un ensemble de premiers $\mathcal{P}_q$, de densité de Dirichlet égale à $\frac{1}{4}$, tel que les entiers $D := -p$ avec $p \in \mathcal{P}_q$ vérifient les conditions de l'hypothèse 2.3.1.*

Dans notre situation, nous n'avons plus la condition *ii)* de l'hypothèse 2.3.1 qui était nécessaire dans [25]. Cela nous permet de considérer la densité naturelle dont on rappelle ci-dessous la définition en toute généralité.

Le but de cette section est de montrer que dans certains cas, cette densité peut être strictement positive. Même si cela semble naturel, cela repose sur des résultats profonds.

Pour $d \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$, notons $N_n(d)$ le nombre de corps de degré n sur $\mathbb{Q}$ et de discriminants bornés, en valeur absolue, par d.

Définition 2.3.3. *Soit E_n un ensemble de corps de degré n fixé. On note $E_n(d)$ l'ensemble des corps de E_n de discriminants bornés, en valeur absolue, par d. On dira que E_n a une densité naturelle si $\frac{\#E_n(d)}{N_n(d)}$ a une limite quand d tend vers $+\infty$ et on la notera, si elle existe, $d(E_n)$.*

Notons $\mathcal{I}(p,n)$ (resp. $\mathcal{R}(p,n)$) l'ensemble de tous les corps de degré n dans lesquels p est inerte (resp. totalement ramifié).

Supposons maintenant $p > 2$. L'existence (et donc le calcul) de $d(\mathcal{R}(p,n))$ et de $d(\mathcal{I}(p,n))$ est un problème non-trivial sauf pour le cas $n = 2$ qui a été traité par Gauss. Pour le cas $n = 3$, la preuve repose sur une propriété propre

aux corps cubiques (cf [18]). Les cas $n = 4$ et $n = 5$ ont été traités par Bhargava et reposent sur des résultats très profonds (cf [7] et [8]). Pour la commodité du lecteur, nous rappelons ces résultats.

Théorème 2.3.4 (Gauss). *Pour $n = 2$, on a*

$$d(\mathcal{R}(p,2)) = \frac{1}{p+1}$$

et

$$d(\mathcal{I}(p,2)) = \frac{p}{2(p+1)}.$$

Théorème 2.3.5 (Davenport-Heilbronn). *Pour $n = 3$, on a*

$$d(\mathcal{R}(p,3)) = \frac{1}{p^2+1}$$

et

$$d(\mathcal{I}(p,3)) = \frac{p(p-1)}{3(p^2+1)}.$$

Théorème 2.3.6 (Bhargava). *Pour $n = 4$,*

$$d(\mathcal{I}(p,4)) = \frac{1}{4}\left(1 - \frac{(p+1)^2}{p^3+p^2+2p+1}\right).$$

Pour $n = 5$,

$$d(\mathcal{I}(p,5)) = \frac{1}{5}\left(1 - \frac{(p+1)(p^2+p+1)}{p^4+p^3+2p^2+2p+1}\right).$$

Ces différents théorèmes montrent que la densité de corps K_m de degré $n \leq 5$ fixé sur $\mathbb{Q}$ tel qu'il existe un unique idéal premier $\mathfrak{p}_m$ de $\mathcal{O}_{K_m}$ au-dessus de p est strictement positive. Cela montre que notre théorème principal permet de considérer beaucoup plus de corps que le théorème 2.2.1.

De ces résultats, nous pouvons conjecturer que :

Conjecture 2.3.7. *Pour tout n, pour tout p, $\mathcal{I}(p,n)$ a une densité naturelle et*

$$\lim_{p\to+\infty} d(\mathcal{I}(p,n)) = \frac{1}{n}.$$

Il n'existe pas de résultats connus pour $n \geq 6$. Del Corso et Dvornicich ont étudié dans [19] un autre type de densité.

Notons $\Phi_n(N) \subset \mathbb{Z}[X]$ l'ensemble des polynômes irréductibles de degré n fixé dont les coefficients sont majorés en valeur absolue par $N > 0$. Soit $\Phi_n \subset \mathbb{Z}[X]$ un ensemble de polynômes irréductibles de degré n. Si la limite

$$\lim_{N\to+\infty} \frac{\mid \Phi_n \cap \Phi_n(N) \mid}{\mid \Phi_n(N) \mid}$$

existe, on dit que Φ_n admet une densité naturelle, notée $D(\Phi_n)$, égale à la valeur de cette limite.

Soient $e, f \in \mathbb{N}^*$. Notons $\mathcal{A}(p;(e,1))$ (resp. $\mathcal{A}(p;(1,f))$), l'ensemble des polynômes unitaires et irréductibles g de degré e (resp. f) tels que p est totalement ramifié (resp. inerte) dans $\mathbb{Q}[X]/(g(X))$. On a alors

Théorème 2.3.8 ([19], Main Theorem)**.** *Il existe deux fonctions rationnelles* $\phi_e(X),\ \phi_f(X) \in \mathbb{Q}(X)$ *telles que* $D(\mathcal{A}(p,(e,1))$ *existe et vaut* $\phi_e(p)$ *pour tout premier* p *premier à* e *et telles que* $D(\mathcal{A}(p,(1,f))$ *existe et vaut* $\phi_f(p)$ *pour tout premier* p*.*

Le lecteur intéressé pourra consulter [19] pour des résultats plus généraux.

2.4 Appendice.

Dans cet appendice, nous allons montrer le théorème 2.1.12. Pour une extension L/K de corps locaux, les deux diagrammes

$$\begin{array}{ccc} L & & L \\ \Big| e & & \Big| d \\ \Big| f & & \\ K & & K \end{array} \quad \text{et}$$

signifient que $e = e(L|K)$, $f = f(L|K)$ et $d = [L : K]$.

Fixons un nombre premier p et une extension finie $F/\mathbb{Q}_p$. Soient $n \geq 2$ et $K_1/F, \ldots, K_n/F$ des extensions deux à deux distinctes. Posons $e_i = e(K_i|F)$ et $f_i = f(K_i|F)$.

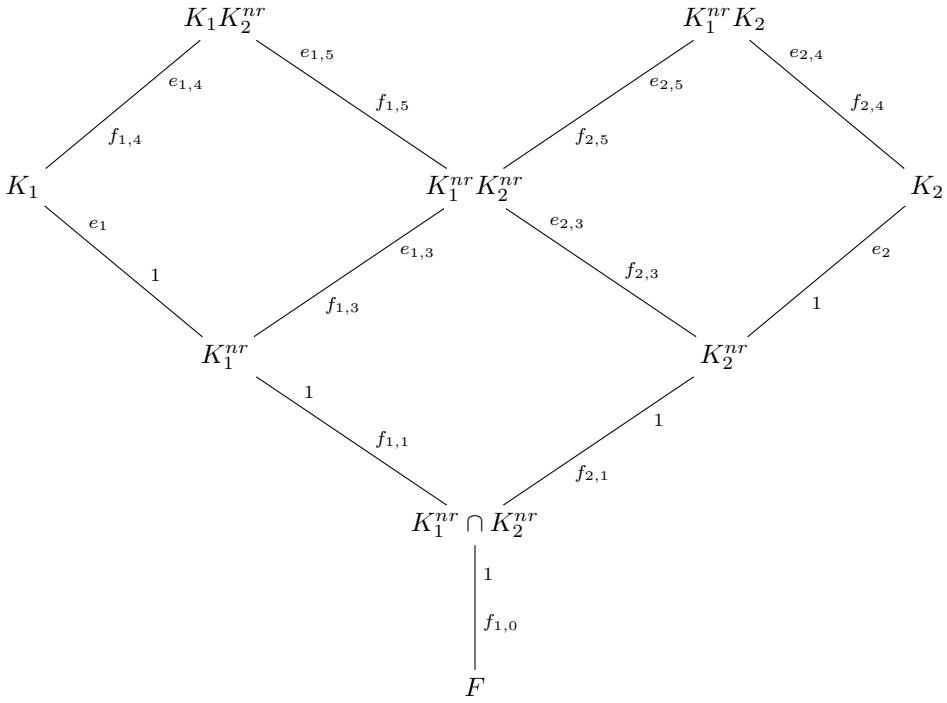
Commençons par majorer le degré d'inertie d'un compositum de deux corps.

Proposition 2.4.1. *On a*

$$f(K_1K_2|F) \leq \mathrm{ppcm}(f_1, f_2)\ \mathrm{pgcd}(e_1, e_2).$$

Démonstration. Notons K_i^{nr} l'extension maximale non-ramifiée de F incluse dans K_i. Par [24, chapitre 3, théorème 25], K_i/K_i^{nr} est totalement ramifiée de degré $e(K_i|K_i^{nr}) = e_i$ et donc $f(K_i|K_i^{nr}) = 1$. Par conséquent, $f(K_i^{nr}|F) = f_i$.

Considérons le diagramme suivant :



Comme le compositum de deux extensions non ramifiées est non ramifié, on a $e_{1,3} = e_{2,3} = 1$. Comme l'extension $K_1^{nr}K_2^{nr}/K_i^{nr}$ est non ramifiée, on déduit du théorème 2.1.13 que $K_1K_2^{nr}/K_1$ est non ramifié et donc $e_{1,4} = 1$. Par conséquent,

$$e_{1,5} = e_{1,5}\, e_{1,3} = e_{1,4}\, e_1 = e_1.$$

De même, $e_{2,4} = 1$ et $e_{2,5} = e_2$.

Calculons maintenant les f_i. Cela se fait en utilisant le lemme suivant :

Fait. *On a* $\mathrm{pgcd}(f_{1,1}, f_{2,1}) = 1$.

Démonstration. Les trois extensions

$$K_1^{nr}/K_1^{nr} \cap K_2^{nr},\ K_2^{nr}/K_1^{nr} \cap K_2^{nr} \text{ et } K_1^{nr}K_2^{nr}/K_1^{nr} \cap K_2^{nr}$$

sont non-ramifiées. Ce sont donc des extensions cycliques. Or,

$$\mathrm{Gal}(K_1^{nr}K_2^{nr}/K_1^{nr} \cap K_2^{nr}) \simeq \mathrm{Gal}(K_1^{nr}/K_1^{nr} \cap K_2^{nr}) \times \mathrm{Gal}(K_2^{nr}/K_1^{nr} \cap K_2^{nr}). \tag{2.15}$$

On a donc un groupe cyclique qui est isomorphe à un produit cartésien de deux groupes cycliques. Il en résulte donc que le cardinal de $\mathrm{Gal}(K_1^{nr}/K_1^{nr} \cap K_2^{nr})$ et de $\mathrm{Gal}(K_2^{nr}/K_1^{nr} \cap K_2^{nr})$ sont premiers entre eux. Ceci prouve le fait.

□

Comme $f_1 = f_{1,1}f_{1,0}$ et $f_2 = f_{2,1}f_{1,0}$, on déduit du fait que $f_{1,0} = \mathrm{pgcd}(f_1, f_2)$ et $\mathrm{ppcm}(f_{1,1}, f_{2,1}) = f_{1,1}f_{2,1}$. En passant aux cardinaux dans (2.15), on en déduit que $f_{1,3}f_{1,1} = f_{1,1}f_{2,1}$ et donc que $f_{1,3} = f_{2,1}$.

De l'inégalité $[K_1K_2^{nr} : K_1^{nr}K_2^{nr}] \leq [K_1 : K_1^{nr}]$, il en résulte que

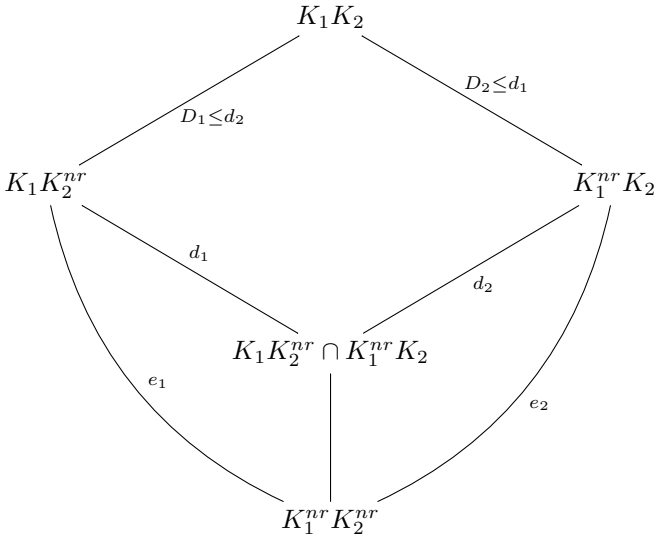
$$e_1\ f_{1,5} = e_{1,5}\ f_{1,5} \leq e_1$$

et donc $f_{1,5} = 1$. Enfin,

$$f_{1,4} = f_{1,3}\ f_{1,5} = f_{2,1}.$$

Par symétrie, on a également $f_{2,4} = f_{2,3} = f_{1,1}$ et $f_{2,5} = 1$.

Á l'aide des valeurs calculées, on peut maintenant majorer le degré d'inertie $f(K_1K_2|K_1^{nr}K_2^{nr})$. Considérons le diagramme ci-dessous :



On remarque que $[K_1K_2 : K_1^{nr}K_2^{nr}] \leq d_2\ e_1$. Il s'ensuit donc que :

$$f(K_1K_2|K_1^{nr}K_2^{nr}) \leq \frac{d_2\ e_1}{e(K_1K_2|K_1^{nr}K_2^{nr})}.$$

Or, $\mathrm{ppcm}(e_1, e_2) \leq e(K_1K_2|K_1^{nr}K_2^{nr})$ et $d_2 \leq e_2$. Ainsi,

$$f(K_1K_2|K_1^{nr}K_2^{nr}) \leq \frac{e_1\ e_2}{\mathrm{ppcm}(e_1, e_2)} = \mathrm{pgcd}(e_1, e_2).$$

Donc, $f(K_1K_2|F) \leq f_{1,1}f_{2,1}\mathrm{pgcd}(e_1, e_2)$ et la proposition s'ensuit puisque

$$\begin{aligned}\mathrm{pgcd}(f_1, f_2)\ f_{1,1}\ f_{2,1} &= f_{1,0}f_{1,1}f_{2,1} \\ &= \frac{f_1f_2}{\mathrm{pgcd}(f_1, f_2)} = \mathrm{ppcm}(f_1, f_2).\end{aligned}$$

Ceci termine la preuve de la proposition 2.4.1. □

Pour prouver le théorème 2.1.12, nous avons également besoin du lemme arithmétique élémentaire suivant.

Lemme 2.4.2. *Soient $l \geq 2$ un entier et $a_1, ..., a_l \in \mathbb{N}^*$. Alors*

$$\prod_{i=1}^{l-1} \mathrm{pgcd}(\mathrm{ppcm}(a_1, ..., a_i), a_{i+1}) = \underset{j=1,...,l}{\mathrm{pgcd}} \left(\prod_{\substack{i=1 \\ i \neq j}}^{l} a_i \right). \tag{2.16}$$

Démonstration. Soit q un nombre premier. Afin d'alléger les notations, notons $P(i) = \max\{v_q(a_1), \ldots, v_q(a_i)\}$ pour tout entier i. En passant à la valuation v_q dans (2.16), on en déduit que pour montrer le lemme, il suffit de montrer que

$$\sum_{i=1}^{l-1} \min\{P(i), v_q(a_{i+1})\} = \sum_{i=1}^{l} v_q(a_i) - P(l) \tag{2.17}$$

Il est clair que

$$\min\{P(i), v_q(a_{i+1})\} + \max\{P(i), v_q(a_{i+1})\} = P(i) + v_q(a_{i+1}). \tag{2.18}$$

Or, $\max\{P(i), v_q(a_{i+1})\} = P(i+1)$. Ainsi, en sommant chaque terme de l'égalité (2.18) pour i allant de 1 à $l-1$, il s'ensuit que

$$\sum_{i=1}^{l-1} \min\{P(i), v_q(a_{i+1})\} + \sum_{i=1}^{l-1} (P(i+1) - P(i)) = \sum_{i=1}^{l-1} v_q(a_{i+1}).$$

Comme $P(1) = v_q(a_1)$, un rapide calcul permet d'en déduire (2.17). Ceci termine la preuve du lemme.

□

Quitte à permuter les corps $K_1, \ldots, K_n$, on peut supposer que $K_1/F, ..., K_m/F$ sont non sauvagement ramifiés et que $K_{m+1}/F, ..., K_n/F$ sont sauvagement ramifiés.

Montrons maintenant la proposition suivante :

Proposition 2.4.3. *On a*

$$f(K_1...K_n|F) \leq \text{ppcm}(f_1, f_2, ..., f_n)E$$

où

$$E = \operatorname*{pgcd}_{j=1,\ldots,n} \left(\prod_{\substack{i=1 \\ i \neq j}}^{n} e_i \right)$$

si $m \geq n-2$ *et*

$$E = \operatorname*{pgcd}_{j=1,\ldots,m+2} \left(\prod_{\substack{i=1 \\ i \neq j}}^{m+2} e_i \right) \prod_{i=m+3}^{n} e_i$$

si $m < n-2$.

Démonstration. Pour tout i, notons $F_i := f(K_1K_2...K_i|F)$ et $E_i := e(K_1K_2...K_i|F)$. D'après la proposition 2.4.1 où l'on prend le compositum $K_1 \ldots K_{i-1}$ pour corps K_1 et K_i pour corps K_2, on a, pour tout $i \geq 2$,

$$F_i = \text{ppcm}(F_{i-1}, f_i)F_i'$$

avec

$$F_i' \in \{1, ..., \text{pgcd}(E_{i-1}, e_i)\}.$$

Ainsi,

$$\begin{aligned} F_n &\leq \mathrm{ppcm}(F_{n-1}, f_n)\mathrm{pgcd}(E_{n-1}, e_n) \\ &= \mathrm{ppcm}(\mathrm{ppcm}(F_{n-2}, f_{n-1})\ F'_{n-1}, f_n)\mathrm{pgcd}(E_{n-1}, e_n). \end{aligned}$$

De plus, pour tous entiers n et $a, a_1, ..., a_n \in \mathbb{N}^*$,

$$\mathrm{ppcm}(a\ a_1, a_2, ..., a_n) \leq a\ \mathrm{ppcm}(a_1, ..., a_n).$$

On en déduit alors que

$$\begin{aligned} F_n &\leq F'_{n-1}\ \mathrm{ppcm}(F_{n-2}, f_{n-1}, f_n)\mathrm{pgcd}(E_{n-1}, e_n) \\ &\leq \mathrm{ppcm}(F_{n-2}, f_{n-1}, f_n)\mathrm{pgcd}(E_{n-2}, e_{n-1})\mathrm{pgcd}(E_{n-1}, e_n) \end{aligned}$$

car $F'_{n-1} \leq \mathrm{pgcd}(E_{n-2}, e_{n-1})$. Par récurrence descendante,

$$F_n \leq \mathrm{ppcm}(f_1, ..., f_n) \prod_{i=2}^{n} \mathrm{pgcd}(E_{i-1}, e_i).$$

Supposons $m \geq n-2$. Par le théorème 2.1.13, $E_k = \mathrm{ppcm}(e_1, ..., e_k)$ pour tout $k \leq n-1$. Il s'ensuit que

$$F_n \leq \mathrm{ppcm}(f_1, ..., f_n) \prod_{i=2}^{n} \mathrm{pgcd}(\mathrm{ppcm}(e_1, ..., e_{i-1}), e_i)$$

et la première assertion du théorème se déduit du lemme 2.4.2.

Supposons maintenant que $m < n-2$. Remarquons que

$$\prod_{i=2}^{n} \mathrm{pgcd}(E_{i-1}, e_i) = \prod_{i=2}^{m+2} \mathrm{pgcd}(E_{i-1}, e_i) \prod_{i=m+3}^{n} \mathrm{pgcd}(E_{i-1}, e_i).$$

D'après le théorème 2.1.13, on a $E_k = \mathrm{ppcm}(e_1, \ldots, e_k)$ pour tout $k \leq m+1$. On déduit ainsi du lemme 2.4.2 que

$$F_n \leq \mathrm{ppcm}(f_1, ..., f_n) \underset{j=1,...,m+2}{\mathrm{pgcd}} \left(\prod_{\substack{i=1 \\ i \neq j}}^{m+2} e_i \right) \prod_{i=m+3}^{n} \mathrm{pgcd}(E_{i-1}, e_i)$$

et la seconde assertion du théorème s'ensuit car $\mathrm{pgcd}(E_{i-1}, e_i) \leq e_i$. □

Pour la commodité du lecteur, rappelons les différentes notations utilisées pour le théorème 2.1.12.

Pour tout $r \in \{1, \ldots, n\}$, notons

$$\Lambda_r = \{e_1, \ldots, e_r\}.$$

Pour $e \in \Lambda_n$, notons $\mathcal{N}(e)$ le nombre d'extensions K_i/F d'indice de ramification e. Enfin, pour tout premier q, notons

$$a_r(q) := \left(\sum_{e \in \Lambda_r} v_q(e) \right) - \max_{e \in \Lambda_r} \{v_q(e)\}.$$

Théorème. *Si $n = m$, alors $e(K_1 \dots K_n|F) = \mathrm{ppcm}(e_1, \dots, e_n)$. Si $m < n$, alors*

$$e(K_1 \dots K_n|F) \leq \mathrm{ppcm}(e_1, \dots, e_{m+1}) e_{m+1}^{\mathcal{N}(e_{m+1})-1} \prod_{e \in \Lambda_n \setminus \Lambda_{m+1}} e^{\mathcal{N}(e)}.$$

On a également

$$f(K_1 ... K_n|F) \leq \mathrm{ppcm}(f_1, f_2, ..., f_n) E$$

où

$$E = \prod_{e \in \Lambda_n} e^{\mathcal{N}(e)-1} \prod_{q \in \mathcal{P}} q^{a_n(q)}$$

si $m \geq n-2$ et

$$E = \prod_{e \in \Lambda_{m+2}} e^{-1} \prod_{q \in \mathcal{P}} q^{a_{m+2}(q)} \prod_{e \in \Lambda_n} e^{\mathcal{N}(e)}$$

si $m < n-2$.

Démonstration. Rappelons que la valeur de $e(K_1 \dots K_n|F)$ dans le cas $n = m$ a déjà été montrée juste après l'énoncé du théorème 2.1.12.

Montrons la majoration de l'indice de ramification dans le cas où $m < n$. Par le théorème 2.1.13, l'indice de ramification du compositum de toutes les extensions K_i/F non-sauvagement ramifiées et de K_{m+1} est

$$\mathrm{ppcm}(e_1, \dots, e_{m+1}).$$

Par ailleurs, l'indice de ramification d'un compositum de corps est majoré par le produit des indices de ramification. Ainsi, l'indice de ramification du compositum de toutes les extensions sauvagement ramifiées sauf K_{m+1} est majoré par

$$e_{m+1}^{\mathcal{N}(e_{m+1})-1} \prod_{e \in \Lambda_n \setminus \Lambda_{m+1}} e^{\mathcal{N}(e)}, \tag{2.19}$$

ce qui montre la majoration souhaitée de $e(K_1 \dots K_n|F)$.

Montrons maintenant la majoration du degré d'inertie. Le théorème 2.1.12 devient maintenant une réécriture de la proposition précédente.

Pour tout $e \in \mathbb{N}$ et tout $r \in \{1, \dots, n\}$, notons $\mathcal{N}_r(e)$ le nombre d'extensions $K_1/F, \dots K_r/F$ dont l'indice de ramification vaut e.

Fixons r et $e \in \Lambda_r$. Soit q un nombre premier. Posons $A = \underset{j=1,\dots,r}{\mathrm{pgcd}} \left(\prod_{\substack{i=1 \\ i \neq j}}^{r} e_i \right)$. Alors $v_q(A) = \sum_{i=1}^{r} v_q(e_i) - \max\{v_q(e_1), \dots, v_q(e_r)\}$. Par définition de $\mathcal{N}_r(e)$, on obtient que

$$\sum_{i=1}^{r} v_q(e_i) = \sum_{e \in \Lambda_r} \mathcal{N}_r(e) v_q(e).$$

Un rapide calcul montre que $v_q(A) = \sum_{e \in \Lambda_r} (\mathcal{N}_r(e) - 1) v_q(e) + a_r(q)$. Il en résulte donc que

$$\underset{j=1,\dots,r}{\mathrm{pgcd}} \left(\prod_{\substack{i=1 \\ i \neq j}}^{r} e_i \right) = \prod_{e \in \Lambda_r} e^{\mathcal{N}_r(e)-1} \prod_{q \in \mathcal{P}} q^{a_r(q)}. \tag{2.20}$$

Supposons que $m \geq n-2$. De le proposition 2.4.3, on a $E = \underset{j=1,\dots,n}{\text{pgcd}} \left(\prod_{\substack{i=1 \\ i \neq j}}^{n} e_i \right)$. En prenant $r = n$ dans (2.20), on en déduit la majoration de $f(K_1 \dots K_n|F)$ souhaitée.

Supposons maintenant que $m < n-2$. Dans ce cas, on a

$$E = \underset{j=1,\dots,m+2}{\text{pgcd}} \left(\prod_{\substack{i=1 \\ i \neq j}}^{m+2} e_i \right) \prod_{i=m+3}^{n} e_i.$$

En prenant cette fois-ci $r = m+2$ dans (2.20), on en déduit que

$$E = \prod_{e \in \Lambda_{m+2}} e^{\mathcal{N}_{m+2}(e)-1} \prod_{q \in \mathcal{P}} q^{a_{m+2}(q)} \prod_{i=m+3}^{n} e_i.$$

Comme $\prod_{e \in \Lambda_{m+2}} e^{\mathcal{N}_{m+2}(e)} \prod_{i=m+3}^{n} e_i = \prod_{e \in \Lambda_n} e^{\mathcal{N}(e)}$, cela montre la majoration souhaitée de $f(K_1 \dots K_n|F)$, ce qui achève la preuve du théorème 2.1.12. □

Remarque 2.4.4. Si on suppose en plus que les extensions $(K_i/F)_{i=1}^n$ soient galoisiennes, alors on peut remplacer "inférieur ou égal" par "divise" dans le théorème 2.1.12 du fait que l'indice de ramification d'un compositum fini d'extensions galoisiennes de F divise le produit des indices de ramification.

Soient $K_1/F, \dots, K_n/F$ comme dans le théorème 2.1.12. Pour un entier $i \leq n$, notons $e_i = e(K_i|F)$ et $f_i = f(K_i|F)$. Supposons que

i) $K_1 \dots K_i/F$ et K_{i+1}/F sont linéairement disjoints pour tout i ;

ii) K_i/F est non sauvagement ramifié pour tout i ;

iii) $e_i = e_j$ ou $\text{pgcd}(e_i, e_j) = 1$ pour tous i, j.

Alors dans le théorème 2.1.12, notre majoration du degré d'inertie est une égalité. En effet, il s'ensuit de la condition $i)$ que

$$[K_1 \dots K_n : F] = \prod_{i=1}^{n} [K_i : F] = \prod_{i=1}^{n} e_i f_i.$$

De plus, les extensions K_i/F sont non sauvagement ramifiées. Le théorème 2.1.13 permet donc d'en déduire que

$$e(K_1 \dots K_n|F) = \text{ppcm}(e_1, \dots, e_n). \tag{2.21}$$

De la condition $iii)$, on obtient que $a_n(q) = 0$ pour tout premier q. De plus, la condition $iii)$ et (2.21) permettent d'en déduire que

$$e(K_1 \dots K_n|F) = \prod_{e \in \Lambda_n} e.$$

Comme $[K_1 \dots K_n : F] = e(K_1 \dots K_n|F) f(K_1 \dots K_n|F)$, on en déduit que

$$f(K_1 \dots K_n|F) = \prod_{e \in \Lambda_n} e^{\mathcal{N}(e)-1} \prod_{i=1}^{n} f_i.$$

Le théorème 2.1.12 permet d'en déduire que

$$\prod_{i=1}^{n} f_i \leq \text{ppcm}(f_1, \dots, f_n).$$

Cela montre donc que $\prod_{i=1}^{n} f_i = \text{ppcm}(f_1, \dots, f_n)$. Ainsi, la majoration du degré d'inertie du théorème 2.1.12 est, dans ce cas, une égalité.

Nous terminons cet appendice avec deux exemples où l'on compare les bornes obtenues en utilisant d'un côté le corollaire 2.1.11 et de l'autre le théorème 2.1.12. L'un contiendra de la ramification sauvage et l'autre non.

Exemple 2.4.5. Prenons $p = 11$ et $\{K_1, \dots, K_n\}$ l'ensemble des extensions de $\mathbb{Q}_{11}$ de degré plus petit que 10 (c'est bien un ensemble fini d'après le théorème 2.1.10). Notons K le compositum des K_n. Pour $i \in \{2, ..., 10\}$, le théorème 2.1.10 montre que $\mathcal{N}_{\mathbb{Q}_{11},i} = \sum_{d|i} d$. Ainsi, la majoration donnée par le corollaire 2.1.11 montre que

$$f(K|\mathbb{Q}_{11}) \leq \prod_{i=1}^{10} i^{\sum_{d|i} d} \leq 1,9.10^{71}.$$

Calculons, avec le théorème 2.1.12, une majoration plus précise de $f(K|\mathbb{Q}_{11})$. Comme il n'y a pas de ramification sauvage, on est dans le cas où $m = n > m-2$. Comme il existe une unique extension non ramifiée de $\mathbb{Q}_{11}$ de degré f, que l'on note $\mathbb{Q}_{11}\{f\}$, il s'ensuit que le nombre d'extensions de $\mathbb{Q}_{11}$ de degré ef et de degré d'inertie f est, d'après le théorème 2.1.10, $\mathcal{N}^{(r)}_{\mathbb{Q}_{11}\{f\},e} = e$. Dans notre situation, $f \leq 10e^{-1}$ et donc, le nombre d'extensions dont le degré de ramification vaut e est $e\lfloor 10/e \rfloor$. Rappelons que pour tout premier q,

$$a_n(q) = -\max\{v_q(1), \dots, v_q(10)\} + \sum_{e=1}^{10} v_q(e).$$

Ainsi, $a_n(2) = 5$, $a_n(3) = 2$, $a_n(5) = 1$ et $a_n(q) = 0$ pour les autres valeurs de q. Il en résulte donc que

$$f(K|\mathbb{Q}_{11}) \leq \text{ppcm}(1, \dots, 10)\ 2^5\ 3^2\ 5 \prod_{e=1}^{10} e^{e\ \lfloor \frac{10}{e} \rfloor - 1} \leq 3,3.10^{56}.$$

Traitons le second exemple.

Exemple 2.4.6. Prenons $p = 5$ et $\{K_1, \dots, K_n\}$ l'ensemble des extensions de $\mathbb{Q}_5$ de degré plus petit que 10. Notons K le compositum des K_n. Le théorème 2.1.10 montre que $\mathcal{N}_{\mathbb{Q}_5,5} = 106$ et $\mathcal{N}_{\mathbb{Q}_5,10} = 1818$. Ainsi, en utilisant la majoration donnée par le corollaire 2.1.11, on en déduit que

$$f(K|\mathbb{Q}_5) \leq 5^{106}\ 10^{1818} \prod_{\substack{i=1 \\ i \neq 5}}^{9} i^{\sum_{d|i} d} \leq 1,5.10^{1941}.$$

Calculons maintenant un majorant de $f(K|\mathbb{Q}_5)$ à l'aide du théorème 2.1.12. Notons m le nombre d'extensions $K_j/\mathbb{Q}_5$ non sauvagement ramifiées. On a $m < n-2$. D'après l'exemple précédent, $\mathcal{N}(e) = e\lfloor 10/e \rfloor$ si $e \notin \{5, 10\}$. Pour $e = 5$, on a $f = 1$ ou $f = 2$. Ainsi, d'après (2.6), on a $\mathcal{N}(5) \leq 105 + 605 = 710$. De même, si $e = 10$, alors $f = 1$ et on en déduit que $\mathcal{N}(10) \leq 1210$. On en déduit donc (en prenant $e_{m+1} = e_{m+2} = 10$) que $a_{m+2}(2) = 8 - 3 = 5$, $a_{m+2}(3) = 4 - 2 = 2$ et $a_{m+2}(q) = 0$ pour les autres valeurs de q. On en conclut donc que :

$$f(K|\mathbb{Q}_5) \leq \mathrm{ppcm}(1, \ldots, 10)\ (10!)^{-1}\ 5\ 2^5\ 3^2\ 5^{710}\ 10^{1210} \prod_{\substack{e=1 \\ e \neq 5}}^{9} e^{e\ \lfloor \frac{10}{e} \rfloor} \leq 6,2.10^{1745}.$$

Chapitre 3

Autour d'une conjecture de Rémond

Notons $\mathbb{G}$ le groupe multiplicatif $\mathbb{G}_m^n$ de dimension n ou une variété abélienne définie sur un corps de nombres k. Notons $\hat{\mathrm{h}}$ une hauteur sur $\mathbb{G}(\overline{k})$ définie de la manière suivante : dans le cas où $\mathbb{G} = \mathbb{G}_m^n$, la hauteur $\hat{\mathrm{h}}(P)$ d'un point $P = (a_1, \ldots, a_n)$ est la somme des hauteurs de Weil $\mathrm{h}(a_1) + \ldots \mathrm{h}(a_n)$. Dans le cas où $\mathbb{G}$ est une variété abélienne, $\hat{\mathrm{h}}$ désignera la hauteur canonique associée à un fibré en droite ample et symétrique L que l'on fixe. Notons $[n] : \mathbb{G} \to \mathbb{G}$ la multiplication par un entier n. Pour un sous-groupe Γ de $\mathbb{G}(\overline{k})$, notons

$$\Gamma_{\mathrm{sat}} = \{g \in \mathbb{G}(\overline{k}) \mid \exists n \in \mathbb{N}\backslash\{0\}, [n].g \in \mathrm{End}(\mathbb{G}).\Gamma\}$$

(où $\mathrm{End}(\mathbb{G}).\Gamma$ désigne le groupe engendré par les éléments de la forme $\phi(\gamma)$ avec $\phi \in \mathrm{End}(\mathbb{G})$ et $\gamma \in \Gamma$) le groupe saturé de Γ. Si $\mathrm{End}(\mathbb{G}) = \mathbb{Z}$ (comme c'est le cas si, par exemple, $\mathbb{G} = \mathbb{G}_m$ ou $\mathbb{G} = E$ est une courbe elliptique non CM) alors, Γ_{sat} est le groupe de division de Γ, i.e. $\{g \in \mathbb{G}(\overline{k}) \mid \exists n \in \mathbb{N}\backslash\{0\}, [n].g \in \Gamma\}$. On définit aussi le rang de Γ comme étant égal à $\dim_{\mathbb{Q}} \Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$.

Récemment, Rémond a énoncé une conjecture très générale [36, Conjecture 3.4] sur la minoration de la hauteur $\hat{\mathrm{h}}$. Un cas particulier de cette conjecture prédit l'énoncé ci-dessous :

Conjecture 3.0.1. *Soit $\Gamma \subset \mathbb{G}(\overline{k})$ un groupe de rang fini. Alors, il existe une constante $c_\Gamma > 0$ telle que $\hat{\mathrm{h}}(P) \geq c_\Gamma$ pour tout $P \in \mathbb{G}(k(\Gamma))\backslash\Gamma_{\mathrm{sat}}$.*

Cette conjecture donne un énoncé apparemment plus fort que celui qu'on peut déduire directement de [36, Conjecture 3.4], où la condition "$P \notin \Gamma_{\mathrm{sat}}$" est remplacée par la condition logiquement plus forte "P est Γ-transverse" (rappelons que, en suivant [36], une sous-variété V de $\mathbb{G}$ est dite Γ-transverse si elle n'est contenue dans aucun translaté d'un sous-groupe algébrique connexe B de A tel que $B \neq A$ par un point de Γ_{sat}). Cependant, [36, Théorème 3.7] avec $\varepsilon = 0$ (ce qui est possible d'après le dernier paragraphe de [36, section 3]) montre que l'on peut affaiblir la condition sur P.

3.1 Cas $\mathbb{G} = \mathbb{G}_m$

Dans cette section, on va s'intéresser à la conjecture 3.0.1 dans le cas où $\mathbb{G} = \mathbb{G}_m$. Dans ce cas particulier, elle se réécrit comme suit :

Conjecture 3.1.1. *Soit $\Gamma \subset \mathbb{G}_m(\overline{\mathbb{Q}})$ un groupe de rang fini. Alors il existe une constante $c_\Gamma > 0$ telle que $\mathrm{h}(\alpha) \geq c_\Gamma$ pour tout $\alpha \in \mathbb{G}_m(\mathbb{Q}(\Gamma))\backslash\Gamma_{\mathrm{sat}}$.*

On ne connaît que peu de résultats non-triviaux dans la direction de cette conjecture, même dans des cas très particuliers. Le cas où $\Gamma = \{1\}_{\mathrm{sat}}$ est le groupe des racines de l'unité a été traité dans [4] et les auteurs ont montré que $c_\Gamma = (\log 5)/12$ convenait.

Cependant, on ne sait toujours pas si cette conjecture est vraie pour tout autre groupe de la forme $\Gamma = \langle b\rangle_{\mathrm{sat}}$ avec $b \in \mathbb{Z}\backslash\{-1, 0, 1\}$. En particulier, on ne sait pas si les points de petite hauteur de $\mathbb{Q}^{ab}(2^{1/2}, 2^{1/3}, \dots)$ sont dans $\langle 2\rangle_{\mathrm{sat}}$.

Pour un nombre premier p, on définit le groupe p-saturé de Γ comme étant le groupe :

$$\Gamma_{\mathrm{sat},p} = \left\{ g \in \overline{\mathbb{Q}}^* \mid \exists n \in \mathbb{N}^*, g^{p^n} \in \Gamma \right\}.$$

Il y a peu, Amoroso a montré que la conjecture 3.1.1 est vérifiée pour le groupe $\Gamma = \langle 2\rangle_{\mathrm{sat},3}$. Plus généralement, il a montré [2, Theorem 3.3] :

Théorème 3.1.2 (Amoroso)**.** *Soient $b \geq 2$ un entier et $p \geq 3$ un nombre premier. Supposons que $p \nmid b$ et que $p^2 \nmid (b^{p-1}-1)$. Alors $\mathrm{h}(\alpha) \geq \min\left\{\frac{1}{3\mathrm{h}(b)}, \frac{\log(p/2)}{2p^2}\right\}$ pour tout $\alpha \in \mathbb{G}_m\left(\mathbb{Q}(\langle b\rangle_{\mathrm{sat},p})\right)\backslash\langle b\rangle_{\mathrm{sat}}$.*

Un ingrédient indispensable dans la preuve de ce théorème repose sur l'étude du dernier saut de la suite des groupes de ramification de $\mathrm{Gal}\big(\mathbb{Q}_p(\zeta_{p^r}, b^{1/p^s})/\mathbb{Q}_p\big)$ avec $r \geq s$ deux entiers positifs. Remarquons que cette étude a déjà été faite par Viviani. Comme on a déjà généralisé les résultats de Viviani (cf les théorèmes 1.1.5 et 1.1.6), cela nous permet de supprimer les conditions techniques du théorème 3.1.2 et de pouvoir considérer des corps de nombres à la place de $\mathbb{Q}$. On montrera le résultat suivant :

Théorème 3.1.3. *Soient F un corps de nombres, $a \in F^*\backslash(F^*)^p$ et p un nombre premier impair ne divisant pas le discriminant de F. Alors il existe $c > 0$ tel que $\mathrm{h}(\alpha) \geq c$ pour tout $\alpha \in \mathbb{G}_m\left(F(\langle a\rangle_{\mathrm{sat},p})\right)\backslash\langle a\rangle_{\mathrm{sat}}$.*

Remarquons que dans le cas $F = \mathbb{Q}$, la condition technique "p ne divise pas le discriminant de F" est vide puisque le discriminant de $\mathbb{Q}$ vaut 1. Le théorème 3.1.3 est donc bien une généralisation du théorème 3.1.2.

3.1.1 Résultats auxiliaires

Dans ce paragraphe, nous allons montrer comment l'étude des groupes de ramification faite dans le chapitre 1 permet d'obtenir des renseignements sur la minoration de la hauteur (cf proposition 3.1.9). Une fois cette proposition prouvée, on pourra alors, à l'aide d'une méthode de la descente, et du lemme 3.1.10, (que l'on peut voir comme une "initialisation" de la méthode de la descente) montrer le théorème 3.1.3.

Nous allons d'abord donner quelques définitions et établir quelques résultats préliminaires.

Pour un corps de nombres ou un corps local K, notons $\mathcal{O}_K$ son anneau des entiers.

Soient L/K une extension galoisienne de corps de nombres et $\mathfrak{p}_L$ un idéal premier de $\mathcal{O}_L$. Pour un entier $i \geq -1$, notons

$$\mathrm{Gal}(L/K)_i(\mathfrak{p}_L) = \{\sigma \in \mathrm{Gal}(L/K) \mid \forall x \in \mathcal{O}_L,\ \sigma x \equiv x \mod \mathfrak{p}_L^{i+1}\}$$

le i-ième groupe de ramification de $\mathrm{Gal}(L/K)$ associé à $\mathfrak{p}_L$.

Lemme 3.1.4. *Soient K un corps de nombres et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Soient $a \in K$ et r, s des entiers positifs tels que $r \geq s$. Alors pour tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_{K(\zeta_{p^r}, a^{1/p^s})}$ au-dessus de $\mathfrak{p}$, on a*

$$K(\zeta_{p^r}, a^{1/p^s})_{\mathfrak{P}} = K_{\mathfrak{p}}(\zeta_{p^r}, a^{1/p^s}).$$

Démonstration. Quitte à multiplier a par un bon élément de K^*, on peut se réduire à montrer le théorème dans le cas où $a \in \mathcal{O}_K$. D'après un lemme de Kummer [13, Chapter 2, section 10], on a que $K(a^{1/p^s})_{\mathfrak{P} \cap K(a^{1/p^s})} = K_{\mathfrak{p}}\big(\zeta_d a^{1/p^s}\big)$ pour un certain diviseur d de p^s. Toujours d'après ce lemme de Kummer, on obtient que $K(\zeta_{p^r})_{\mathfrak{P} \cap K(\zeta_{p^r})} = K_{\mathfrak{p}}(\zeta_{p^r})$. Ainsi, $K(\zeta_{p^r}, a^{1/p^s})_{\mathfrak{P}} = K_{\mathfrak{p}}\big(\zeta_{p^r}, a^{1/p^s}\big)$ puisque $d \mid p^r$ $(r \geq s)$, ce qui montre le lemme. □

On dira qu'une extension L/K est radicale s'il existe $a \in K^*$ et des entiers r, s tels que $L = K(\zeta_{p^r}, a^{1/p^s})$. Remarquons qu'une telle extension est galoisienne si $r \geq s$. Le lemme 3.1.4 affirme donc que l'extension complétée d'une extension galoisienne et radicale de corps de nombres est aussi galoisienne et radicale.

Notons μ_∞ l'ensemble des racines de l'unité. Dans cette sous-section, et uniquement dans celle ci, fixons un corps de nombres F, un $a \in \mathcal{O}_F \backslash \mu_\infty$ tel que $a \in F^* \backslash (F^*)^p$ et un nombre premier p impair ne divisant pas le discriminant de F. Fixons également un idéal premier $\mathfrak{p}$ de $\mathcal{O}_F$ au-dessus de p. Notons ρ l'unique entier tel que $a \in F_{\mathfrak{p}}^{p^\rho} \backslash F_{\mathfrak{p}}^{p^{\rho+1}}$ et $b \in F_{\mathfrak{p}} \backslash F_{\mathfrak{p}}^p$ tel que $b^{p^\rho} = a$. Remarquons que l'on peut identifier b avec un élément de $\langle a \rangle_{\mathrm{sat},p} \subset \overline{F}$, que l'on note encore b. Enfin, posons $F' = F(b)$ et, pour des entiers positifs r et s,

$$F_{r,s} = F(\zeta_{p^r}, b^{1/p^s}), \qquad (F_{\mathfrak{p}})_{r,s} = F_{\mathfrak{p}}(\zeta_{p^r}, b^{1/p^s}).$$

Lemme 3.1.5. *Il existe un idéal premier $\mathfrak{p}'$ de $\mathcal{O}_{F'}$ au-dessus de $\mathfrak{p}$ de telle sorte que $F'_{\mathfrak{p}'} = F_{\mathfrak{p}}$.*

Démonstration. Comme $a \in F^* \backslash (F^*)^p$, un lemme de Capelli [29, Chapter 6, Theorem 9.1] montre que le polynôme $X^{p^\rho} - a \in F[X]$ est irréductible sur F. C'est donc le polynôme minimal de b sur F. Comme $b \in F_{\mathfrak{p}}$ et que $a = b^{p^\rho}$, il existe alors un polynôme $P(X) \in F_{\mathfrak{p}}[X]$ tel que

$$X^{p^\rho} - a = (X - b)P(X).$$

D'après un lemme de Kummer [13, Chapter 2, section 10], appliqué à $K = F$ et à $\beta = b \in \mathcal{O}_{F'}$ (car $a \in \mathcal{O}_F$), on en déduit qu'il existe un idéal premier $\mathfrak{p}'$ de $\mathcal{O}_{F'}$ au-dessus de $\mathfrak{p}$ tel que

$$F'_{\mathfrak{p}'} = F_{\mathfrak{p}}(b) = F_{\mathfrak{p}}.$$

□

Dans la suite de cette section, choisissons un tel idéal $\mathfrak{p}'$. Remarquons que $F_{\mathfrak{p}}/\mathbb{Q}_p$ est une extension finie non ramifiée puisque par hypothèse, p ne divise pas le discriminant de F.

Lemme 3.1.6. *Il existe une unique place de $F(\langle b\rangle_{\mathrm{sat},p})$ au-dessus de $\mathfrak{p}'$.*

Démonstration. Clairement,

$$F(\langle b\rangle_{\mathrm{sat},p}) = \bigcup_{r\geq 0} F_{r,r}.$$

Ainsi, pour montrer le lemme, il suffit de montrer que le nombre c_r d'idéaux premiers de $F_{r,r}$ au-dessus de $\mathfrak{p}'$ est égal à 1.

En appliquant le lemme 3.1.4 avec $K = F$, le complété de $F_{r,r}$ par rapport à un idéal premier quelconque au-dessus de $\mathfrak{p}'$ est égal à $(F_{\mathfrak{p}})_{r,r}$. Comme $b \in F_{\mathfrak{p}}^*\backslash(F_{\mathfrak{p}}^*)^p$, on déduit du lemme 1.1.2, où l'on a remplacé a par b, que

$$[(F_{\mathfrak{p}})_{r,r} : F_{\mathfrak{p}}] = (p-1)p^{2r-1}.$$

Comme $c_r = [F_{r,r} : F]/[(F_{\mathfrak{p}})_{r,r} : F_{\mathfrak{p}}]$ et que

$$[F_{r,r} : F] \leq [F_{r,0} : F][F_{0,r} : F] \leq (p-1)p^{r-1}p^r = (p-1)p^{2r-1},$$

on en déduit que $c_r \leq 1$, et donc que $c_r = 1$, ce qui prouve le lemme. □

Par ce lemme, il existe alors un unique idéal premier de $\mathcal{O}_{F_{r,s}}$, avec r, s deux entiers positifs, au-dessus de $\mathfrak{p}'$ que l'on notera $\mathfrak{P}_{r,s}$. D'après le lemme 3.1.4, appliqué à $K = F$, $\mathfrak{p} = \mathfrak{p}'$ et à $\mathfrak{P} = \mathfrak{P}_{r,s}$, on a que

$$(F_{r,s})_{\mathfrak{P}_{r,s}} = (F_{\mathfrak{p}})_{r,s}. \tag{3.1}$$

Ainsi, si $r \geq s$, alors $(F_{r,s})_{\mathfrak{P}_{r,s}}/F_{\mathfrak{p}}$ est une extension galoisienne, radicale et finie. L'étude des groupes de ramification d'une telle extension a déjà été traitée dans le chapitre 1. Ici, on souhaite obtenir des renseignements sur les groupes de ramification d'une extension globale. C'est l'objet de la proposition suivante.

Introduisons d'abord une notation que nous permettra d'unifier les deux cas $p \mid v_{\mathfrak{p}'}(b)$ et $p \nmid v_{\mathfrak{p}'}(b)$. Posons

$$\delta = \begin{cases} 0 \text{ si } p \mid v_{\mathfrak{p}'}(b) \\ 1 \text{ si } p \nmid v_{\mathfrak{p}'}(b) \end{cases}.$$

Proposition 3.1.7. *Soient r, s des entiers tels que $r \geq s \geq 2$. Notons T le dernier saut de* $\mathrm{Gal}((F_{r,s-\delta})_{\mathfrak{P}_{r,s-\delta}}/F_{\mathfrak{p}})$. *Alors* $\mathrm{Gal}(F_{r,s-\delta}/F')_T(\mathfrak{P}_{r,s-\delta}) \simeq \mathbb{Z}/p\mathbb{Z}$ *et*

$$F_{r,s-\delta}^{\mathrm{Gal}(F_{r,s-\delta}/F')_T(\mathfrak{P}_{r,s-\delta})} = \begin{cases} F_{r-1,s-\delta} \text{ si } r > s \\ F_{r,s-\delta-1} \text{ si } r = s \end{cases}.$$

Démonstration. Afin d'alléger les notations, notons $N = F_{r,s-\delta}$ et $\mathfrak{Q} = \mathfrak{P}_{r,s-\delta}$. On sait que pour tout $i \geq 0$,

$$\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_i \simeq \mathrm{Gal}(N/F')_i(\mathfrak{Q}), \tag{3.2}$$

où l'isomorphisme est donné par le morphisme de restriction. Plus précisément, si

$$N_{\mathfrak{Q}}^{\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_i} = N_{\mathfrak{Q}}^{\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_0}\left(\zeta_{p^{r^{(i)}}}, b^{1/p^{s^{(i)}}}\right) \tag{3.3}$$

pour certains entiers positifs $r^{(i)}$ et $s^{(i)}$, alors

$$N^{\mathrm{Gal}(N/F')_i(\mathfrak{Q})} = N^{\mathrm{Gal}(N/F')_0(\mathfrak{Q})}\left(\zeta_{p^{r^{(i)}}}, b^{1/p^{s^{(i)}}}\right). \tag{3.4}$$

Commençons par supposer que $p \mid v_{\mathfrak{p}'}(b)$, i.e. $\delta = 0$. Ainsi, $N = F_{r,s}$ et donc, $N_{\mathfrak{Q}} = (F_{\mathfrak{p}})_{r,s}$ par (3.1). D'après le corollaire 1.4.4, appliqué à $F = F_{\mathfrak{p}}$, on a

$$N_{\mathfrak{Q}}^{\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_T} = \begin{cases} (F_{\mathfrak{p}})_{r-1,s} \text{ si } r > s \\ (F_{\mathfrak{p}})_{r,s-1} \text{ si } r = s \end{cases}.$$

Remarquons également que $\#\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_T = [N_{\mathfrak{Q}} : N_{\mathfrak{Q}}^{\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_T}] = p$ d'après la remarque 1.1.3 appliquée à $r' = r-1$ et à $s' = s$ si $r > s$ ou à $r' = r$ et à $s' = s-1$ si $r = s$.

Supposons maintenant que $p \nmid v_{\mathfrak{p}'}(b)$, i.e. $\delta = 1$. Ainsi, $N = F_{r,s-1}$ et $N_{\mathfrak{Q}} = (F_{\mathfrak{p}})_{r,s-1}$ par la (3.1). D'après le corollaire 1.4.8, appliqué à $F = F_{\mathfrak{p}}$, on a

$$N_{\mathfrak{Q}}^{\mathrm{Gal}(L_{\mathfrak{Q}}/F_{\mathfrak{p}})_T} = \begin{cases} (F_{\mathfrak{p}})_{r-1,s-1} \text{ si } r > s \\ (F_{\mathfrak{p}})_{r,s-2} \text{ si } r = s \end{cases}.$$

Remarquons également que $\#\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_T = [N_{\mathfrak{Q}} : N_{\mathfrak{Q}}^{\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_T}] = p$ d'après la remarque 1.1.3 appliquée à $r' = r-1$ et à $s' = s-1$ si $r > s$ ou à $r' = r$ et à $s' = s-2$ si $r = s$.

On a ainsi montré que dans les deux cas, $\#\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_T = p$ et

$$N_{\mathfrak{Q}}^{\mathrm{Gal}(L_{\mathfrak{Q}}/F_{\mathfrak{p}})_T} = \begin{cases} (F_{\mathfrak{p}})_{r-1,s-\delta} \text{ si } r > s \\ (F_{\mathfrak{p}})_{r,s-\delta-1} \text{ si } r = s \end{cases}.$$

Rappelons que $N_{\mathfrak{Q}} = (F_{\mathfrak{p}})_{r,s-\delta}$ par (3.1). Ainsi, d'après le lemme 1.1.2, $N_{\mathfrak{Q}}/F_{\mathfrak{p}}$ est totalement ramifié, et donc, $\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_0 = \mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})$. Dit autrement, $N_{\mathfrak{Q}}^{\mathrm{Gal}(N_{\mathfrak{Q}}/F_{\mathfrak{p}})_0} = F_{\mathfrak{p}}$. Comme $\mathfrak{Q}$ est l'unique idéal premier de $\mathcal{O}_N$ au-dessus de $\mathfrak{p}'$ et que l'extension complétée $N_{\mathfrak{Q}}/F'_{\mathfrak{p}'} = N_{\mathfrak{Q}}/F_{\mathfrak{p}}$ est totalement ramifiée, il s'ensuit que $\mathrm{Gal}(N/F')_0(\mathfrak{Q}) = \mathrm{Gal}(N/F')$, i.e. $N^{\mathrm{Gal}(N/F')_0(\mathfrak{Q})} = F'$.

De (3.3) et (3.4), il s'ensuit alors que

$$N^{\mathrm{Gal}(N/F')_T(\mathfrak{Q})} = \begin{cases} F'(\zeta_{p^{r-1}}, b^{1/p^{s-\delta}}) = F_{r-1,s-\delta} \text{ si } r > s \\ F'(\zeta_{p^r}, b^{1/p^{s-1-\delta}}) = F_{r,s-1-\delta} \text{ si } r = s \end{cases}$$

et, d'après (3.2), que $\#\mathrm{Gal}(N/F')_T(\mathfrak{Q}) = p$, i.e. $\mathrm{Gal}(N/F')_T(\mathfrak{Q}) \simeq \mathbb{Z}/p\mathbb{Z}$. □

Pour un entier $m \geq 1$, notons μ_m l'ensemble des racines m-ième de l'unité. Le lemme suivant servira uniquement pour prouver la proposition 3.1.9.

Lemme 3.1.8. *Soient r, s des entiers tels que $r \geq s \geq 2$. Notons T le dernier saut de $\mathrm{Gal}((F_{r,s-\delta})_{\mathfrak{P}_{r,s-\delta}}/F_{\mathfrak{p}})$. Soient $\alpha \in F_{r,s-\delta}$ et σ un générateur du groupe cyclique $\mathrm{Gal}(F_{r,s-\delta}/F')_T(\mathfrak{P}_{r,s-\delta})$ tels que $\sigma\alpha/\alpha \in \mu_\infty$. Alors $\sigma\alpha/\alpha \in \mu_{p^r}$.*

Démonstration. Afin d'alléger les notations, notons $N = F_{r,s-\delta}$ et $\mathfrak{Q} = \mathfrak{P}_{r,s-\delta}$. Posons $m = p^\beta d$ l'ordre de $\sigma\alpha/\alpha \in N$ avec $p \nmid d$. Posons également $\omega = (\sigma\alpha/\alpha)^{p^\beta} \in N$. Par conséquent, ω est d'ordre d.

Comme $p \nmid d$, on a, d'après [32, Chapter II, Proposition 7.12], que $\mathfrak{Q} \cap N^{\langle\sigma\rangle}$ est non ramifié dans $N^{\langle\sigma\rangle}(\omega)$.

Par la théorie des groupes de ramification, $\mathfrak{Q} \cap N^{\mathrm{Gal}(N/F')_0(\mathfrak{Q})}$ est totalement ramifié dans N. Comme $N^{\langle\sigma\rangle}(\omega) \subset N$ et que $\langle\sigma\rangle = \mathrm{Gal}(N/F')_T(\mathfrak{Q})$, il s'ensuit que $\mathfrak{Q} \cap N^{\langle\sigma\rangle}$ est totalement ramifié dans $N^{\langle\sigma\rangle}(\omega)$.

Comme $\mathfrak{Q} \cap N^{\langle\sigma\rangle}$ est à la fois totalement ramifié et non ramifié dans $N^{\langle\sigma\rangle}(\omega)$, on en déduit alors que $N^{\langle\sigma\rangle}(\omega) = N^{\langle\sigma\rangle}$, ou encore que $\omega \in N^{\langle\sigma\rangle}$. D'où $\sigma\omega = \omega$. Comme $\sigma\alpha^{p^\beta} = \omega\alpha^{p^\beta}$, il s'ensuit alors que $\sigma^i\alpha^{p^\beta} = \omega^i\alpha^{p^\beta}$ pour tout $i \geq 1$. D'après la proposition 3.1.7, σ est d'ordre p. Par conséquent, $\sigma^p = id$ et donc, $\omega^p = 1$. Or, ω est aussi d'ordre d et $p \nmid d$. D'où $d = 1$. Ainsi, $\sigma\alpha/\alpha \in \mu_{p^\infty}$ et donc, $\sigma\alpha/\alpha \in \mu_{p^\infty} \cap N = \mu_{p^r}$. □

Proposition 3.1.9. *Soient r, s des entiers tels que $r \geq s$. Notons T le dernier saut de $\mathrm{Gal}((F_{r,s-\delta})_{\mathfrak{P}_{r,s-\delta}}/F_{\mathfrak{p}})$. Soient $\alpha, \tilde{g} \in \overline{\mathbb{Q}}^*$ tels que $\alpha/\tilde{g} \in F_{r,s-\delta}$. Supposons que :*

i) il existe $d \in \mathbb{N}^*$ tel que $\tilde{g}^d \in F_{r,s-\delta}^{\mathrm{Gal}(F_{r,s-\delta}/F')_T(\mathfrak{P}_{r,s-\delta})}$;

ii) $|\tilde{g}^d|_{\mathfrak{P}_{r,s-\delta}} \leq 1$;

iii) $r \geq 3$ et $s \geq 2$.

Alors soit il existe $g \in \langle\zeta_{p^r}, b^{1/p^s}\rangle$ tel que $\alpha/(\tilde{g}g) \in F_{r,s-\delta}^{\mathrm{Gal}(F_{r,s-\delta}/F')_T(\mathfrak{P}_{r,s-\delta})}$, soit

$$\mathrm{h}(\alpha) + \max\left\{0, \frac{1}{[\mathbb{Q}(\gamma):\mathbb{Q}]} \sum_{\tau:\mathbb{Q}(\gamma)\hookrightarrow\mathbb{C}} \log|\tau\gamma - 1|\right\} \geq \max\left\{0; \frac{\log p + p^3 \log|\tilde{g}|_{\mathfrak{P}_{r,s-\delta}}}{2p^4[F':\mathbb{Q}]}\right\}$$

où $\gamma = ((\sigma\alpha)/(\zeta\alpha))^{p^3}$ avec $\zeta \in \mu_\infty$ et avec $\sigma \in \mathrm{Gal}(F_{r,s-\delta}/F')$. De plus, $\gamma \notin \mu_\infty$.

Démonstration. Afin d'alléger les notations, notons $N = F_{r,s-\delta}$ et $\mathfrak{Q} = \mathfrak{P}_{r,s-\delta}$. D'après l'hypothèse *iii*), on obtient que $r \geq s \geq 2$. En utilisant la proposition 3.1.7, on en déduit alors que $\zeta_{p^{r-1}}, b^{1/p^{s-\delta-1}} \in N^{\mathrm{Gal}(N/F')_T(\mathfrak{Q})}$ et que $\mathrm{Gal}(N/F')_T(\mathfrak{Q})$ est cyclique d'ordre p. Notons σ un générateur de ce groupe.

Si $\log p + p^3 \log|\tilde{g}|_{\mathfrak{Q}} \leq 0$, alors l'inégalité de la proposition est clairement vérifiée. Supposons donc que $\log p + p^3 \log|\tilde{g}|_{\mathfrak{Q}} > 0$.

Posons

$$h = \zeta_{p^r} \text{ si } r = s \text{ et } h = b^{1/p^{s-\delta}} \text{ si } r > s.$$

Remarquons que $\sigma h/h \in \mu_p \backslash \{1\}$ (car $h^p \in \{\zeta_{p^{r-1}}; b^{1/p^{s-\delta-1}}\} \subset N^{\langle\sigma\rangle}$) et que $h \in \langle\zeta_{p^r}, b^{1/p^s}\rangle$ puisque $s - \delta \leq s$.

Notons $\beta = \alpha/\tilde{g}$. Supposons dans un premier temps que $\sigma\beta/\beta \in \mu_\infty$. D'après le lemme 3.1.8, il s'ensuit que $\omega := \sigma\beta/\beta \in \mu_{p^r}$. Montrons que $\omega \in \mu_p$. Tout d'abord, $\sigma\beta^p = \omega^p\beta^p$. Ensuite, on a aussi que $\sigma\omega^p = \omega^p$ puisque $\omega^p \in \mu_{p^{r-1}} \subset N^{\langle\sigma\rangle}$. Des deux dernières égalités, on en déduit aisément que $\sigma^j\beta^p = \omega^{pj}\beta^p$ pour tout $j \geq 1$. Comme σ est d'ordre p, on obtient alors que $\beta^p = \sigma^p\beta^p = \omega^{p^2}\beta^p$ et donc que $\omega \in \mu_{p^2}$. Or, $r \geq 3$ d'après l'hypothèse $iii)$, ce qui implique que $\mu_{p^2} \subset N^{\langle\sigma\rangle}$. Comme $\sigma\beta = \omega\beta$ et que $\sigma\omega = \omega$, on en déduit alors que $\beta = \sigma^p\beta = \omega^p\beta$, et donc que $\omega \in \mu_p$.

Comme $\sigma h/h \in \mu_p\backslash\{1\}$, il existe alors un entier l tel que $\sigma\beta/\beta = (\sigma h/h)^l$. D'où $\sigma\left(\alpha/(\tilde{g}h^l)\right) = \alpha/(\tilde{g}h^l)$ et donc que $\alpha/(\tilde{g}h^l) \in N^{\langle\sigma\rangle} = N^{\mathrm{Gal}(N/F')_T(\mathfrak{Q})}$.

Supposons maintenant que $\sigma\beta/\beta \notin \mu_\infty$. En particulier, $\sigma\beta^{p^3} \neq \beta^{p^3}$. Soit E la clôture galoisienne de $N(\alpha) = N(\tilde{g})$ sur $N^{\langle\sigma\rangle}$ (cela a bien un sens puisque d'après l'hypothèse $i)$, $\tilde{g}^d \in N^{\langle\sigma\rangle}$). Notons encore σ une extension de σ à E. Par $i)$, il existe une racine de l'unité $\zeta \in E$ telle que $\sigma\tilde{g} = \zeta\tilde{g}$. Ainsi, $\sigma\beta = (\sigma\alpha)/(\zeta\tilde{g})$ et

$$\sigma\beta^{p^3} - \beta^{p^3} = (\sigma\alpha^{p^3} - (\zeta\alpha)^{p^3})/(\zeta\tilde{g})^{p^3}. \tag{3.5}$$

Montrons que que pour tout $x \in N$,

$$|\sigma x^{p^3} - x^{p^3}|_{\mathfrak{Q}} \leq p^{-1}\max\{1, |\sigma x|_{\mathfrak{Q}}\}^{p^3}\max\{1, |x|_{\mathfrak{Q}}\}^{p^3}. \tag{3.6}$$

Pour tout $x \in \mathcal{O}_{N_{\mathfrak{Q}}}$, on a $\sigma x \equiv x \mod \mathfrak{Q}^{T+1}$ et donc,

$$\sigma x^{p^3} \equiv x^{p^3} \mod \mathfrak{Q}^{p^3(T+1)}.$$

Ainsi, pour tout $x \in \mathcal{O}_{N_{\mathfrak{Q}}}$, on déduit de la proposition 1.4.9 que

$$|\ \sigma x^{p^3} - x^{p^3}\ |_{\mathfrak{Q}} \leq p^{-p^3(T+1)/e(N_{\mathfrak{Q}}|\mathbb{Q}_p)} \leq p^{-e(N_{\mathfrak{Q}}|F_{\mathfrak{p}})/e(N_{\mathfrak{Q}}|\mathbb{Q}_p)} = p^{-1},$$

car $F_{\mathfrak{p}}/\mathbb{Q}_p$ est non ramifié. Ceci montre (3.6) dans le cas où $x \in \mathcal{O}_{N_{\mathfrak{Q}}}$.

En revanche, si $x \notin \mathcal{O}_{N_{\mathfrak{Q}}}$, alors $x^{-1} \in \mathcal{O}_{N_{\mathfrak{Q}}}$ puisque $\mathcal{O}_{N_{\mathfrak{Q}}}$ est un anneau de valuation. Ainsi,

$$|\sigma x^{-p^3} - x^{-p^3}|_{\mathfrak{Q}} \leq p^{-1}$$

ou encore que

$$|\sigma x^{p^3} - x^{p^3}|_{\mathfrak{Q}} \leq p^{-1}|\sigma x|_{\mathfrak{Q}}^{p^3}\ |x|_{\mathfrak{Q}}^{p^3},$$

ce qui montre de nouveau (3.6) dans le cas où $x \notin \mathcal{O}_{N_{\mathfrak{Q}}}$.

Posons $y = \sigma\alpha^{p^3} - (\zeta\alpha)^{p^3}$. Remarquons que $y \neq 0$ car $\zeta = \sigma\tilde{g}/\tilde{g}$ et $\sigma\beta^{p^3} \neq \beta^{p^3}$. En appliquant (3.6) à $x = \beta = \alpha/\tilde{g}$, on déduit de (3.5) que

$$|y|_{\mathfrak{Q}}\ |\tilde{g}|_{\mathfrak{Q}}^{-p^3} \leq p^{-1}\max\{1, |\sigma\left(\alpha/\tilde{g}\right)|_{\mathfrak{Q}}\}^{p^3}\max\{1, |\alpha/\tilde{g}|_{\mathfrak{Q}}\}^{p^3}.$$

Comme $\sigma\tilde{g} = \zeta\tilde{g}$ et $|\tilde{g}|_{\mathfrak{Q}} \leq 1$ d'après l'hypothèse $ii)$, il s'ensuit alors que :

$$|y|_{\mathfrak{Q}} \leq p^{-1}\max\{1, |\sigma\alpha|_{\mathfrak{Q}}\}^{p^3}\max\{1, |\alpha|_{\mathfrak{Q}}\}^{p^3}|\tilde{g}|_{\mathfrak{Q}}^{-p^3}. \tag{3.7}$$

Pour toute place ν de N, notons $n_\nu = [N_\nu : \mathbb{Q}_\nu]/[N : \mathbb{Q}]$ si ν est finie et $n_\nu = [N_\nu : \mathbb{R}]/[N : \mathbb{Q}]$ sinon. Notons $\mathcal{M}^0(N)$ l'ensemble des places finies de N

et $\mathcal{M}^\infty(N)$ celui des places infinies. En appliquant la formule du produit à y, on a

$$0 = n_{\mathfrak{Q}} \log |y|_{\mathfrak{Q}} + \sum_{\substack{\nu \in \mathcal{M}^0(N) \\ \nu \neq \mathfrak{Q}}} n_\nu \log |y|_\nu + \sum_{\nu \in \mathcal{M}^\infty(N)} n_\nu \log |y|_\nu. \tag{3.8}$$

Dans (3.8), on majore $|y|_{\mathfrak{Q}}$ en utilisant l'inégalité (3.7). On majore également $|y|_\nu$, pour $\nu \in \mathcal{M}^0(N)$ et $\nu \neq \mathfrak{Q}$, en utilisant l'inégalité ultramétrique. On obtient alors

$$\begin{aligned} 0 \leq & \left(-\log p - p^3 \log |\tilde{g}|_{\mathfrak{Q}}\right) n_{\mathfrak{Q}} \\ & + p^3 \sum_{\nu \in \mathcal{M}^0(N)} n_\nu \left(\log \max\{1, |\sigma\alpha|_\nu\} + \log \max\{1, |\zeta\alpha|_\nu\}\right) + \sum_{\nu \in \mathcal{M}^\infty(N)} n_\nu \log |y|_\nu. \end{aligned} \tag{3.9}$$

Posons $\gamma = (\sigma\alpha/\zeta\alpha)^{p^3}$. Supposons par l'absurde que $\gamma \in \mu_\infty$. Alors $\sigma\alpha/\alpha \in \mu_\infty$. Comme $\zeta = \sigma\tilde{g}/\tilde{g} \in \mu_\infty$ et que $\beta = \alpha/\tilde{g}$, il s'ensuit que $\sigma\beta/\beta \in \mu_\infty$, ce qui est absurde par hypothèse. Par conséquent, $\gamma \notin \mu_\infty$.

Clairement, $y = (\zeta\alpha)^{p^3}(\gamma - 1)$. Ainsi,

$$\sum_{\nu \in \mathcal{M}^\infty(N)} n_\nu \log |y|_\nu = \frac{1}{[\mathbb{Q}(\gamma) : \mathbb{Q}]} \sum_\tau \log |\tau\gamma - 1| + p^3 \sum_{\nu \in \mathcal{M}^\infty(N)} n_\nu \log |\zeta\alpha|_\nu \tag{3.10}$$

où τ parcourt l'ensemble des plongements $\mathbb{Q}(\gamma) \hookrightarrow \mathbb{C}$. En injectant (3.10) dans (3.9), il en résulte, car $\mathrm{h}(\sigma\alpha) = \mathrm{h}(\zeta\alpha) = \mathrm{h}(\alpha)$, que

$$0 \leq \left(-\log p - p^3 \log |\tilde{g}|_{\mathfrak{Q}}\right) n_{\mathfrak{Q}} + 2p^3 \mathrm{h}(\alpha) + \frac{1}{[\mathbb{Q}(\gamma) : \mathbb{Q}]} \sum_\tau \log |\tau\gamma - 1|.$$

Comme $\mathfrak{Q}$ est l'unique idéal premier de $\mathcal{O}_N$ au-dessus de $\mathfrak{p}'$ et que $F'_{\mathfrak{p}'} = F_{\mathfrak{p}}$ (cf lemme 3.1.5), il s'ensuit que $[N_{\mathfrak{Q}} : F_{\mathfrak{p}}] = [N : F']$. D'où

$$n_{\mathfrak{Q}} = [N_{\mathfrak{Q}} : \mathbb{Q}_p]/[N : \mathbb{Q}] = [F_{\mathfrak{p}} : \mathbb{Q}_p]/[F' : \mathbb{Q}] \geq 1/[F' : \mathbb{Q}].$$

Enfin, comme $\log p + p^3 \log |\tilde{g}|_{\mathfrak{Q}} > 0$, il s'ensuit que

$$\mathrm{h}(\alpha) + \max\left\{0, \frac{1}{[\mathbb{Q}(\gamma) : \mathbb{Q}]} \sum_\tau \log |\tau\gamma - 1|\right\} \geq \frac{\log p + p^3 \log |\tilde{g}|_{\mathfrak{Q}}}{2p^4 [F' : \mathbb{Q}]}.$$

□

Lemme 3.1.10. *Soient K un corps de nombres et $r, c \in K^* \backslash \mu_\infty$. Supposons que pour tout $m > 0$, on a $r^m \notin \langle c \rangle$. Soit $(x, n) \in \mathbb{Z} \times \mathbb{Z}^*$ et posons $\alpha = rc^{x/n}$. Alors*

$$\mathrm{h}(\alpha) \geq \frac{1}{5\mathrm{h}(c)[K : \mathbb{Q}]^4}.$$

Démonstration. Comme $r, c \notin \mu_\infty$, les vecteurs $(v_{\mathfrak{p}}(r))_{\mathfrak{p}}$ (où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de $\mathcal{O}_K$) et $(v_{\mathfrak{p}}(c))_{\mathfrak{p}}$ sont non nuls. De plus, $r^m \notin \langle c \rangle$

pour tout m. Cela implique donc que le vecteur $(v_{\mathfrak{p}}(r))_{\mathfrak{p}}$ ne peut être une combinaison linéaire, à coefficient dans $\mathbb{Q}$, des vecteurs $(v_{\mathfrak{p}}(c))_{\mathfrak{p}}$. Il existe donc deux idéaux premiers distincts $\mathfrak{p}_1$ et $\mathfrak{p}_2$ tels que

$$v_{\mathfrak{p}_1}(r)v_{\mathfrak{p}_2}(c) - v_{\mathfrak{p}_2}(r)v_{\mathfrak{p}_1}(c) \neq 0.$$

Comme $\alpha^n = r^n c^x \in K^*$, il s'ensuit que pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$,

$$v_{\mathfrak{p}}(\alpha^n) = nv_{\mathfrak{p}}(r) + xv_{\mathfrak{p}}(c).$$

Un rapide calcul montre donc que

$$|v_{\mathfrak{p}_1}(\alpha^n)v_{\mathfrak{p}_2}(c) - v_{\mathfrak{p}_2}(\alpha^n)v_{\mathfrak{p}_1}(c)| = n|v_{\mathfrak{p}_1}(r)v_{\mathfrak{p}_2}(c) - v_{\mathfrak{p}_2}(r)v_{\mathfrak{p}_1}(c)| \geq n. \quad (3.11)$$

Soient $\beta \in K^*$ et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Notons p le générateur positif de $\mathfrak{p} \cap \mathbb{Z}$. Alors

$$\mathrm{h}(\beta) \geq \frac{1}{[K:\mathbb{Q}]} \log \max\{1, p^{-v_{\mathfrak{p}}(\beta)/v_{\mathfrak{p}}(p)}\} = \frac{|v_{\mathfrak{p}}(\beta)|}{[K:\mathbb{Q}]v_{\mathfrak{p}}(p)} \log p \quad (3.12)$$

si $v_{\mathfrak{p}}(\beta) \leq 0$. Dans le cas où $v_{\mathfrak{p}}(\beta) > 0$, alors $v_{\mathfrak{p}}(\beta^{-1}) < 0$ et donc,

$$\mathrm{h}(\beta^{-1}) \geq \frac{|v_{\mathfrak{p}}(\beta^{-1})|}{[K:\mathbb{Q}]v_{\mathfrak{p}}(p)} \log p.$$

Comme $\mathrm{h}(\beta) = \mathrm{h}(\beta^{-1})$, on en déduit que (3.12) est vérifié pour tout $\beta \in K^*$ et tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$. On obtient ainsi, car $v_{\mathfrak{p}}(p) \leq [K:\mathbb{Q}]$ et $p \geq 2$, que

$$|v_{\mathfrak{p}}(\beta)| \leq [K:\mathbb{Q}]v_{\mathfrak{p}}(p)\mathrm{h}(\beta)/\log p \leq [K:\mathbb{Q}]^2\mathrm{h}(\beta)/\log 2. \quad (3.13)$$

En appliquant l'inégalité triangulaire dans (3.11), puis deux fois (3.13), avec $\beta = \alpha^N$ et avec $\beta = c$, on en conclut alors que

$$\begin{aligned} n &\leq |v_{\mathfrak{p}_1}(\alpha^n)|\,|v_{\mathfrak{p}_2}(c)| + |v_{\mathfrak{p}_2}(\alpha^n)|\,|v_{\mathfrak{p}_1}(c)| \\ &\leq \frac{2\mathrm{h}(c)[K:\mathbb{Q}]^4\mathrm{h}(\alpha^n)}{(\log 2)^2} \leq 5n\mathrm{h}(c)\mathrm{h}(\alpha)[K:\mathbb{Q}]^4 \end{aligned}$$

car $2/(\log 2)^2 \leq 5$ et le lemme s'ensuit. □

3.1.2 Preuve du théorème.

Dans cette section, nous allons prouver le théorème 3.1.3, que l'on rappelle ci-dessous pour la commodité du lecteur.

Théorème. *Soient F un corps de nombres, $a \in F^*\backslash(F^*)^p$ et p un nombre premier impair ne divisant pas le discriminant de F. Alors il existe $c > 0$ tel que $\mathrm{h}(\alpha) \geq c$ pour tout $\alpha \in \mathbb{G}_m\left(F(\langle a\rangle_{\mathrm{sat},p})\right)\backslash\langle a\rangle_{\mathrm{sat}}$.*

Démonstration. Supposons tout d'abord que $a \in \mu_\infty$. Comme $F(\mu_\infty)/F$ est une extension abélienne, on déduit de [5] qu'il existe $c > 0$ tel que $\mathrm{h}(\alpha) \geq c$ pour tout $\alpha \in F(\mu_\infty)^*\backslash\mu_\infty$, ce qui montre le théorème dans le cas où $a \in \mu_\infty$ puisque $\langle a\rangle_{\mathrm{sat}} \subset \mu_\infty$.

Supposons maintenant que $a \notin \mu_\infty$. Soit $\alpha \in F(\langle a \rangle_{\mathrm{sat},p})$. Il existe alors un entier positif t, que l'on suppose assez grand, tel que $\alpha \in F(\zeta_{p^{t-1}}, a^{1/p^{t-1}})$. Quitte à multiplier a par un bon élément de F^*, on peut supposer que $a \in \mathcal{O}_F$.

Rappelons quelques notations que l'on a introduites dans la sous-section 3.1.1. Fixons un idéal premier $\mathfrak{p}$ de $\mathcal{O}_F$ au-dessus de p. Notons ρ l'unique entier tel que $a \in F_{\mathfrak{p}}^{p^\rho} \backslash F_{\mathfrak{p}}^{p^{\rho+1}}$ et $b \in F_{\mathfrak{p}}$ tels que $b^{p^\rho} = a$. Remarquons que l'on peut identifier b avec un élément de $\langle a \rangle_{\mathrm{sat},p} \subset \overline{F}$, que l'on note encore b. Notons $F' = F(b)$. D'après le lemme 3.1.5, il existe un idéal premier $\mathfrak{p}'$ de $\mathcal{O}_{F'}$ au-dessus de $\mathfrak{p}$ de telle sorte que $F'_{\mathfrak{p}'} = F_{\mathfrak{p}}$. Notons

$$\delta = \begin{cases} 0 \text{ si } p \mid v_{\mathfrak{p}'}(b) \\ 1 \text{ sinon} \end{cases} .$$

Enfin, pour des entiers positifs r et s, posons

$$F_{r,s} = F(\zeta_{p^r}, b^{1/p^s}) \text{ et } (F_{\mathfrak{p}})_{r,s} = F_{\mathfrak{p}}(\zeta_{p^r}, b^{1/p^s}).$$

Comme $t - 1 \leq t - \delta$ et que $\alpha \in F(\zeta_{p^{t-1}}, a^{1/p^{t-1}}) = F_{t-1,t-1-\rho}$, on a alors que

$$\alpha \in F_{t-1,t-1-\rho} \subset F_{t,t-\delta}.$$

Notons Λ l'ensemble des couples (r,s) tel que $t \geq r \geq s \geq 2$ et tel qu'il existe $\tilde{f} \in \left\langle \zeta_{p^t}, b^{1/p^t} \right\rangle$ avec $\alpha/\tilde{f} \in F_{r,s-\delta}$. Remarquons que $(t,t) \in \Lambda$. Fixons (r,s) un élément minimal de Λ pour l'ordre lexicographique et $\tilde{f} \in \left\langle \zeta_{p^t}, b^{1/p^t} \right\rangle$ avec $\alpha/\tilde{f} \in F_{r,s-\delta}$. Pour finir, posons

$$\kappa = \max\left\{ \lceil \log\left(-\log|b|_{\mathfrak{p}}\right) / \log p \rceil + 6;\ 3 \right\}.$$

Supposons que $r \leq \kappa$. Comme $r \geq s$, on en déduit que $s \leq \kappa$ et donc que $\alpha/\tilde{f} \in F_{\kappa,\kappa}$. En appliquant le lemme 3.1.10 avec $K = F_{\kappa,\kappa}, r = \alpha/\tilde{f}$ et avec $c = b$, on en conclut que soit

$$\mathrm{h}(\alpha) \geq \frac{1}{5\mathrm{h}(b)[F_{\kappa,\kappa} : \mathbb{Q}]^4},$$

soit que $\alpha \in \langle b \rangle_{\mathrm{sat}} = \langle a \rangle_{\mathrm{sat}}$. Le théorème est ainsi prouvé dans le cas où $r \leq \kappa$.

À partir de maintenant, supposons que $r \geq \kappa$. Comme r est "assez grand", on va pouvoir minorer, grâce à la proposition 3.1.9, $\mathrm{h}(\alpha)$ par une constante indépendante de α.

Notons $\mathfrak{Q} = \mathfrak{P}_{r,s-\delta}$ l'unique idéal premier de $\mathcal{O}_{F_{r,s-\delta}}$ au-dessus de $\mathfrak{p}'$. Par définition de $\tilde{f}$, il existe des entiers u et x tels que $\tilde{f} = \zeta_{p^t}^u b^{x/p^t}$. On pourrait appliquer la proposition 3.1.9 avec r, s et $\tilde{g} = \tilde{f}$. Mais, si c'est la seconde conclusion qui est satisfaite, on ne peut garantir que $\log p + p^3 \log|\tilde{f}|_{\mathfrak{Q}} > 0$ car on n'a aucun contrôle sur $|\tilde{f}|_{\mathfrak{Q}}$. Ceci est dû au fait que x/p^t peut être très proche de 1.

Pour contourner ce problème, posons $x = Qp^{t-r+2} + R$ la division euclidienne de x par p^{t-r+2}. Posons alors

$$\tilde{g} = \zeta_{p^t}^u b^{R/p^t}.$$

Comme $\alpha/\tilde{f} \in F_{r,s-\delta}$ et que $\max\{r-2, s-\delta\} \leq \max\{r-1, s\} - \delta$, on en déduit alors que

$$\alpha/\tilde{g} = (\alpha/\tilde{f})b^{Q/p^{r-2}} \in F_{r,\max\{r-2,s-\delta\}} \subset F_{r,s'-\delta},$$

où l'on a noté, pour abréger, $s' = \max\{r-1, s\}$.

Comme on a un "bon contrôle" de R/p^t, cela nous permettra de montrer plus tard, avec le fait que $r \geq \kappa$, que $\log p + p^3 \log|\tilde{g}|_{\mathfrak{Q}} > 0$. Cependant, le couple $(r, s') \in \Lambda$ n'est plus nécessairement minimal pour l'ordre lexicographique. Mais, il est quand même "suffisamment petit" pour pouvoir contredire la minimalité de (r, s) si c'est la première conclusion de la proposition 3.1.9, appliquée à r et à s', qui est satisfaite.

Remarquons tout d'abord que les hypothèses de la proposition 3.1.9 sont vérifiées. Clairement, $r \geq 3$ puisque $r \geq \kappa$ et $s' \geq 2$ puisque $s \geq 2$ par construction de Λ. De plus, par définition de $\tilde{g}$, il existe un entier d tel que $\tilde{g}^d \in \langle a \rangle \subset F^*$. Enfin, comme $b \in \mathcal{O}_{F'}$, il s'ensuit que $|\tilde{g}^d|_{\mathfrak{Q}'} = |b|_{\mathfrak{p}'}^{dR/p^t} \leq 1$ où $\mathfrak{Q}'$ désigne l'unique idéal premier de $F_{r,s'-\delta}$ au-dessus de $\mathfrak{p}'$.

Notons T le dernier saut de $\mathrm{Gal}((F_{r,s'-\delta})_{\mathfrak{Q}}/F_{\mathfrak{p}})$. Supposons par l'absurde que c'est la première conclusion qui soit vérifiée. Il existe alors $g \in \langle \zeta_{p^t}, b^{1/p^t} \rangle$ tel que

$$\alpha/(\tilde{g}g) \in F_{r,s'-\delta}^{\mathrm{Gal}(F_{r,s'-\delta}/F')_T(\mathfrak{Q}')}. \tag{3.14}$$

Il s'ensuit donc que $\tilde{g}g \in \langle \zeta_{p^t}, b^{1/p^t} \rangle$ et, d'après la proposition 3.1.7, appliquée à r et à s', que

$$F_{r,s'-\delta}^{\mathrm{Gal}(F_{r,s'-\delta}/F')_T(\mathfrak{Q}')} = \begin{cases} F_{r-1,s'-\delta} \text{ si } r > s' \\ F_{r,s'-1-\delta} \text{ si } r = s' \end{cases}. \tag{3.15}$$

Rappelons que $s' = \max\{r-1, s\}$. Si $r > s'$, alors d'après (3.14) et (3.15), $(r-1, s') \in \Lambda$ car $r - 1 \geq s' \geq 2$, ce qui contredit la minimalité de (r, s). Si $r = s'$, alors $r = s$ et donc, $s' = s$. D'après (3.14) et (3.15), on a alors que $(r, s-1) \in \Lambda$ puisque $s - 1 = r - 1 \geq 2$. Ceci contredit à nouveau la minimalité de (r, s).

On a ainsi montré que la première conclusion de la proposition 3.1.9 ne peut être satisfaite. C'est donc la seconde conclusion qui est satisfaite. On en déduit donc que

$$\mathrm{h}(\alpha) + \max\left\{0; \frac{1}{[\mathbb{Q}(\gamma):\mathbb{Q}]} \sum_{\tau} \log|\tau(\gamma) - 1|\right\} \geq \frac{\log p + p^3 \log|\tilde{g}|_{\mathfrak{Q}}}{2p^4[F':\mathbb{Q}]} =: c(\tilde{g}). \tag{3.16}$$

où

$$\gamma = ((\sigma\alpha)/(\zeta\alpha))^{p^3} \notin \mu_\infty \tag{3.17}$$

pour une certaine racine de l'unité ζ et un certain $\sigma \in \mathrm{Gal}(F_{r,s-\delta}/F')$.

Comme $\log|\tilde{g}|_{\mathfrak{Q}} = R/p^t \log|b|_{\mathfrak{p}'}$, que $|b|_{\mathfrak{p}'} \leq 1$ et que $R < p^{t-r+2}$, il s'ensuit que $\log|\tilde{g}|_{\mathfrak{Q}} > p^{-(r-2)} \log|b|_{\mathfrak{p}'}$. D'où

$$c(\tilde{g}) > \frac{\log p + p^{-(r-5)} \log|b|_{\mathfrak{p}'}}{2p^4[F' : \mathbb{Q}]}.$$

Enfin, comme $r \geq \kappa \geq \lceil \log(-\log|b|_{\mathfrak{p}'})/\log p) \rceil + 6$, on en déduit que

$$p^{-(r-5)} \log|b|_{\mathfrak{p}'} < (\log p)/p$$

et donc que $c(\tilde{g}) \geq c := \frac{(1-1/p)\log p}{2p^4[F':\mathbb{Q}]} > 0$.

Nous allons maintenant utiliser une variante de l'argument de [26, § 7] pour montrer que :

$$\max\left\{0; \frac{1}{[\mathbb{Q}(\gamma) : \mathbb{Q}]} \sum_{\tau} \log|\tau(\gamma) - 1|\right\} \leq (p^3+1)\mathrm{h}(\alpha) + c/2. \tag{3.18}$$

Cela nous permettra, avec (3.16), d'obtenir une minoration de $\mathrm{h}(\alpha)$ indépendante de α et ainsi en déduire le théorème.

Pour $m \in \mathbb{N}^*$, notons

$$\begin{array}{rccl} f_m & : & \mathbb{C}^* & \to & \mathbb{R} \\ & & z & \mapsto & \begin{cases} \min\{m, \max\{-m, \log|z-1|\}\}, \text{ si } z \neq 1 \\ -m, \text{ sinon} \end{cases} \end{array}.$$

Notons $z = \tau(\gamma) \neq 1$ et montrons que

$$\log|z-1| \leq c/4 + \log\max\{1, |z|\} + f_m(z). \tag{3.19}$$

Commençons par le cas où $|z-1| < e^m$. Alors, $f_m(z) = \max\{-m, \log|z-1|\}$. On obtient alors que $\log|z-1| \leq f_m(z)$, ce qui montre (3.19) dans cette situation.

Enfin, supposons que $|z-1| \geq e^m$. Alors, $f_m(z) = m \geq 0$. De plus, $|z| \geq e^m - 1 \geq e^m/2$ car $m \geq 1$. Ainsi,

$$\frac{|z-1|}{|z|} \leq 1 + 1/|z| \leq 1 + 2e^{-m}.$$

Comme $\lim_{m\to+\infty}(1+2e^{-m}) = 1$, on en déduit, pour tout m assez grand, $\log(1+2e^{-m}) < c/4$. Par conséquent,

$$\log|z-1| \leq \log(1+2e^{-m}) + \log|z| \leq c/4 + \log\max\{1,|z|\} + f_m(z)$$

On a ainsi montré (3.19).

De (3.19), on en déduit que

$$\frac{1}{[\mathbb{Q}(\gamma):\mathbb{Q}]} \sum_{\tau} \log|\tau(\gamma)-1|\} \leq \mathrm{h}(\alpha) + \mathrm{h}(\gamma) + \frac{1}{[\mathbb{Q}(\gamma):\mathbb{Q}]} \sum_{\tau} f_m(\tau(\gamma)). \tag{3.20}$$

Pour montrer (3.18), et ainsi terminer la preuve, nous allons utiliser le théorème de convergence dominée et le théorème d'équidistribution de Bilu [9] ci-dessous :

Théorème 3.1.11. *(Bilu) Soit $\gamma_1, \gamma_2, \ldots$ une suite de $\overline{\mathbb{Q}}\backslash\mu_\infty$ telle que $\lim_{i\to+\infty} \mathrm{h}(\gamma_i) = 0$. Si $f : \mathbb{C}^* \to \mathbb{R}$ est une fonction continue bornée, alors*

$$\lim_{i\to+\infty} \frac{1}{[\mathbb{Q}(\gamma_i) : \mathbb{Q}]} \sum_\tau f(\tau(\gamma_k)) = \int_0^1 f(e^{2i\pi t})dt$$

où τ parcourt tous les plongements de corps de $\mathbb{Q}(\gamma_i) \to \mathbb{C}$.

La suite de fonctions $g_m : t \mapsto f_m(e^{2i\pi t})$ converge point par point (lorsque m tend vers $+\infty$) vers la fonction $g : t \mapsto \log|e^{2i\pi t} - 1|$ sur $]0;1[$.

Clairement, $|g_m(t)| \leq |g(t)|$ et

$$\int_0^1 |g(t)|ds < +\infty.$$

Par le théorème de convergence dominée, il s'ensuit que

$$\lim_{m\to+\infty} \int_0^1 g_m(t) = \int_0^1 g(t)dt = 0$$

(où la dernière égalité vient du fait que $\int_0^1 |g(s)|ds = \log M(X-1) = 0$, en désignant par $M(\cdot)$ la mesure de Mahler). Ainsi, pour tout m assez grand, on a

$$\int_0^1 g_m(t)ds < c/8.$$

Rappelons que $\gamma \notin \mu_\infty$ d'après (3.17). En appliquant le théorème 3.1.11 à $f = f_m$ pour tout entier m assez grand,

$$\frac{1}{[\mathbb{Q}(\gamma) : \mathbb{Q}]} \sum_\tau f_m(\tau(\gamma)) \leq 2 \int_0^1 g_m(t)dt \leq c/4.$$

Or, de (3.17), $\mathrm{h}(\gamma) \leq p^3\mathrm{h}(\alpha)$. On déduit donc de (3.20) que

$$\frac{1}{[\mathbb{Q}(\gamma) : \mathbb{Q}]} \sum_\tau \log|\tau(\gamma) - 1|\} \leq (p^3+1)\mathrm{h}(\alpha) + c/2,$$

ce qui montre (3.18) et prouve ainsi le théorème. □

3.2 Généralisation de la conjecture de Rémond

Comme l'a déjà montré Rémond dans [36, section 5], la conjecture 3.0.1 ne peut s'énoncer dans le cas plus général où $\mathbb{G}$ est une variété semi-abélienne. Son contre-exemple repose sur le fait que $\mathbb{G}$ puisse posséder des points de Ribet (le lecteur souhaitant lire la définition d'un point de Ribet pourra voir [27]). Dans le cas où $\mathbb{G}$ est une variété semi-abélienne isotriviale, les points de Ribet sont des points de torsion. Par conséquent, il semble raisonnable de proposer la conjecture suivante :

Conjecture 3.2.1. *La conjecture 3.0.1 reste valable pour les variétés abéliennes isotriviales.*

À partir de maintenant, considérons des variétés abéliennes isotriviales de la forme $\mathbb{G} = \mathbb{G}_m \times A$ où A est une variété abélienne définie sur k. Notons $\hat{\mathrm{h}}(P,Q)$ la hauteur d'un point $(P,Q) \in \mathbb{G}$ comme étant la somme $\hat{\mathrm{h}}(P) + \hat{\mathrm{h}}(Q)$.

La conjecture 3.2.1 permet d'interpréter différents résultats déjà présents dans la littérature comme des cas particuliers de celle-ci. Le premier concerne le cas où $\Gamma = (\mathbb{G}_m)_{\mathrm{tors}} \times \{0\}$. On a alors $\Gamma_{\mathrm{sat}} = \mathbb{G}_{\mathrm{tors}}$ et $k(\Gamma) = k((\mathbb{G}_m)_{\mathrm{tors}}) \subset k^{ab}$. La conjecture 3.2.1 prédit donc l'existence d'un $c > 0$ tel que $\mathrm{h}(\alpha) + \hat{\mathrm{h}}(P) \geq c$ pour tout

$$(\alpha, P) \in \mathbb{G}(k((\mathbb{G}_m)_{\mathrm{tors}}))\backslash\mathbb{G}_{\mathrm{tors}}.$$

Amoroso et Zannier [5] ont montré qu'il existe $c > 0$ tel que pour tout $\alpha \in \mathbb{G}_m(k^{ab})\backslash(\mathbb{G}_m)_{\mathrm{tors}}$, on a $\mathrm{h}(\alpha) \geq c$. Par ailleurs, Baker et Silverman [6, Theorem 0.1] ont montré qu'il existe $c > 0$ tel que $\hat{\mathrm{h}}(P) \geq c$ pour tout $P \in A(k^{ab})\backslash A_{\mathrm{tors}}$. De ces deux résultats, on déduit que la conjecture 3.2.1 est satisfaite dans ce cas (en fait, elle est même équivalente à la concaténation de ces deux théorèmes).

Le second exemple concerne le cas où $\mathbb{G} = \mathbb{G}_m \times E$, avec E une courbe elliptique définie sur $\mathbb{Q}$, et $\Gamma = \{1\} \times E_{\mathrm{tors}}$. À nouveau, $\Gamma_{\mathrm{sat}} = \mathbb{G}_{\mathrm{tors}}$. De plus, $\mathbb{Q}(\Gamma) = \mathbb{Q}(E_{\mathrm{tors}})$. La conjecture 3.2.1 prédit donc l'existence d'un $c > 0$ tel que $\mathrm{h}(\alpha) + \hat{\mathrm{h}}(P) \geq c$ pour tout

$$(\alpha, P) \in \mathbb{G}(\mathbb{Q}(E_{\mathrm{tors}}))\backslash\mathbb{G}_{\mathrm{tors}}.$$

Cette prédiction correspond précisément à [26, Corollary 1].

Dans les deux exemples cités ci-dessus, on a $\Gamma_{\mathrm{sat}} = \mathbb{G}_{\mathrm{tors}}$. Dans cet article, on se propose de donner un exemple de la conjecture 3.2.1 dans le cas où $\Gamma_{\mathrm{sat}} \neq \mathbb{G}_{\mathrm{tors}}$. Pour un nombre algébrique $b \in \mathbb{G}_m(\overline{\mathbb{Q}})$ et un nombre premier p, notons

$$\langle b\rangle_{\mathrm{sat},p} = \{g \in \mathbb{G}_m(\overline{\mathbb{Q}}) \mid \exists n \geq 1,\ g^{p^n} \in \langle b\rangle\}.$$

Théorème 3.2.2. *Soient E une courbe elliptique et $p \geq 5$ un premier tel que E a une réduction supersingulière en p. Soit $b \geq 2$ un entier tel que $p \nmid b$ et $p^2 \nmid (b^{p-1} - 1)$. Alors, il existe $c_{\Gamma,E} > 0$ tel que $\hat{\mathrm{h}}(\alpha, P) \geq c_{\Gamma,E}$ pour tout $(\alpha, P) \in \mathbb{G}(\mathbb{Q}(\Gamma))\backslash\Gamma_{\mathrm{sat}}$ où $\Gamma = \langle b\rangle_{\mathrm{sat},p} \times \{0\}$ et où $\mathbb{G} = \mathbb{G}_m \times E$.*

Remarquons que $\Gamma_{\mathrm{sat}} = \langle b\rangle_{\mathrm{sat}} \times E_{\mathrm{tors}}$. Soit $(\alpha, P) \in \mathbb{G}(\mathbb{Q}(\Gamma))\backslash\Gamma_{\mathrm{sat}}$. Alors, $\alpha \in \mathbb{G}_m(\mathbb{Q}(\Gamma))\backslash\langle b\rangle_{\mathrm{sat}}$ ou $P \in E(\mathbb{Q}(\Gamma))\backslash E_{\mathrm{tors}}$. Dans [2], Amoroso a montré l'existence d'un $c > 0$ tel que $\mathrm{h}(\alpha) \geq c$ pour tout $\alpha \in \mathbb{G}_m(\mathbb{Q}(\Gamma))\backslash\langle b\rangle_{\mathrm{sat}}$. Par conséquent, le théorème 3.2.2 est une conséquence du théorème suivant :

Théorème 3.2.3. *Soient E une courbe elliptique et $p \geq 5$ un premier tel que E a une réduction supersingulière en p. Soit $b \geq 2$ un entier tel que $p \nmid b$ et $p^2 \nmid (b^{p-1} - 1)$. Alors, il existe $c > 0$ tel que $\hat{\mathrm{h}}(P) \geq c$ pour tout $P \in E(\mathbb{Q}(\langle b\rangle_{\mathrm{sat},p}))\backslash(E(\mathbb{Q}(\zeta_p)) \cap E_{\mathrm{tors}})$.*

Remarquons que le résultat que l'on obtient est apparemment légèrement plus précis car on retire seulement $E(\mathbb{Q}) \cap E_{\mathrm{tors}} \subset E(\mathbb{Q}(\langle b\rangle_{\mathrm{sat},p}) \cap E_{\mathrm{tors}}$. Cependant, on montrera dans le fait 3.2.13 que cette inclusion est en fait une égalité.

3.2.1 Un exemple

Fixons $E/\mathbb{Q}$ une courbe elliptique définie par une equation de Weierstrass courte et minimale à coefficients entiers. Il existe donc des entiers a et b tels que

$$E :\ Y^2 = X^3 + aX + b. \tag{3.21}$$

On dit que a et b sont les *coefficients de* E. Fixons également un nombre premier $p \geq 5$ tel que E a une réduction supersingulière en p.

Pour tous entiers $r, s \geq 0$, notons

$$\mathbb{Q}_{r,s} = \mathbb{Q}(\zeta_{p^r}, b^{1/p^s}) \text{ et } (\mathbb{Q}_p)_{r,s} = \mathbb{Q}_p(\zeta_{p^r}, b^{1/p^s}),$$

où b est choisi comme dans le théorème 3.2.3, et $\nu_{r,s}$ un idéal premier de $\mathcal{O}_{\mathbb{Q}_{r,s}}$ au-dessus de p. En appliquant le lemme 3.1.4 avec $K = \mathbb{Q}$, $\mathfrak{P} = \nu_{r,s}$ et avec $a = b$, on en déduit que $(\mathbb{Q}_{r,s})_{\nu_{r,s}} = (\mathbb{Q}_p)_{r,s}$.

Notons également $\mathbb{Q}_{\infty,\infty} = \mathbb{Q}(\zeta_{p^\infty}, b^{1/p^\infty}) = \mathbb{Q}(\langle b \rangle_{\mathrm{sat},p})$. Énonçons tout d'abord quelques propriétés concernant l'extension $\mathbb{Q}_{r,s}/\mathbb{Q}$.

Lemme 3.2.4. *Soient $r \geq s$ des entiers positifs avec $r \geq 1$. Alors*

i) l'extension $\mathbb{Q}_{r,s}/\mathbb{Q}$ est galoisienne ;

ii) p est totalement ramifié dans $\mathbb{Q}_{r,s}$. En particulier, $\nu_{r,s}$ est l'unique idéal premier de $\mathcal{O}_{\mathbb{Q}_{r,s}}$ au-dessus de p ;

iii) l'indice de ramification $e_{\nu_{r,s}}(\mathbb{Q}_{r,s}|\mathbb{Q})$ est égal à $(p-1)p^{r+s-1}$;

iv) notons $l_{r,s}$ le dernier saut de $(\mathbb{Q}_p)_{r,s}/\mathbb{Q}_p$. Alors $p^2(l_{r,s}+1) \geq e_{\nu_{r,s}}(\mathbb{Q}_{r,s}|\mathbb{Q})$;

v) le corps fixé par $\mathrm{Gal}(\mathbb{Q}_{r,s}/\mathbb{Q})_{l_{r,s}}(\nu_{r,s})$ est

$$\mathbb{Q}_{r,s}^{\mathrm{Gal}(\mathbb{Q}_{r,s}/\mathbb{Q})_{l_{r,s}}(\nu_{r,s})} = \begin{cases} \mathbb{Q}_{r-1,s} \text{ si } r > s \\ \mathbb{Q}_{r,s-1} \text{ si } r = s \end{cases} ;$$

vi) si $(r,s) \neq (1,0)$, l'extension $\mathbb{Q}_{r,s}/\mathbb{Q}_{r,s}^{\mathrm{Gal}(\mathbb{Q}_{r,s}/\mathbb{Q})_{l_{r,s}}(\nu_{r,s})}$ est cyclique de degré p.

Démonstration. Le *i)* est clair. Pour le *ii)*, *iii)* et *v)*, voir [2, Proposition 2.1] où on utilise, de façon essentielle, l'étude des groupes de ramification de [46]. Pour le *iv)*, voir [2, Lemma 2.2]. Le *vi)* découle de la remarque 1.1.3 appliquée à $r' = r-1$ et à $s' = s$ si $r > s$ ou à $r' = r$ et à $s' = s-1$ si $r = s$. □

Soient $r \geq s$ deux entiers tels que $r \geq 1$. Comme $\nu_{r,s}$ est l'unique idéal premier de $\mathcal{O}_{\mathbb{Q}_{r,s}}$ au-dessus de p, on confondra, à partir de maintenant, $\mathbb{Q}_{r,s}$ et son plongement dans son complété $(\mathbb{Q}_p)_{r,s}$.

Enfin, rappelons que quitte à plonger $\mathbb{Q}$ dans $\mathbb{Q}_p$, on peut voir E comme une courbe elliptique sur $\mathbb{Q}_p$.

D'après [40, Proposition 12], l'image de $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ dans $\mathrm{Aut}(E[p])$ (ici, $E[p]$ désigne l'ensemble des points de torsion d'ordre divisant p) est un Cartan non-déployé (en particulier cyclique d'ordre p^2-1). Cela implique le lemme suivant :

Lemme 3.2.5. *Soit $L/\mathbb{Q}_p$ une extension finie telle que $(p^2-1) \nmid [L:\mathbb{Q}_p]$. Alors $E(L) \cap E[p] = \{0\}$.*

Remarque 3.2.6. D'après le *ii)* et le *iii)* du lemme 3.2.4, on a

$$[\mathbb{Q}_{r,s} : \mathbb{Q}] = (p-1)p^{r+s-1}.$$

Ainsi, le lemme 3.2.5 appliqué à $L = (\mathbb{Q}_p)_{r,s}$ montre que 0 est le seul point de torsion d'ordre divisant p (et donc d'ordre divisant une puissance de p) de $E((\mathbb{Q}_p)_{r,s})$.

Reprenons maintenant quelques notations déjà introduites dans [26, section 8]. Pour un corps de nombres K et une place ν de K, notons K_ν le complété de K en ν. Soit $P = (x, y) \in E(\overline{\mathbb{Q}})$. Pour toute place q de $\mathbb{Q}$, notons

$$\hat{\mathrm{h}}_q(P) = \frac{1}{[\mathbb{Q}(P) : \mathbb{Q}]} \sum_{\mathfrak{q}|q} d_\mathfrak{q} \lambda_\mathfrak{q}(\iota_\mathfrak{q}(P)) \tag{3.22}$$

où $\mathfrak{q}$ parcourt l'ensemble des places de $\mathcal{O}_{\mathbb{Q}(P)}$ au-dessus de q, où $\iota_\mathfrak{q}$ désigne le plongement $\mathbb{Q}(P) \hookrightarrow \mathbb{Q}(P)_\mathfrak{q}$, où $\lambda_\mathfrak{q}$ est la hauteur locale (pour la définition complète de $\lambda_\mathfrak{q}$, voir [43, Chapter VI]) en $\mathfrak{q}$ et où $d_\mathfrak{q} = [\mathbb{Q}(P)_\mathfrak{q} : \mathbb{Q}_q]$ désigne le degré local. Remarquons que

$$\hat{\mathrm{h}}(P) = \hat{\mathrm{h}}_\infty(P) + \hat{\mathrm{h}}_2(P) + \hat{\mathrm{h}}_3(P) + \dots \ . \tag{3.23}$$

Précisons que l'on peut avoir $\hat{\mathrm{h}}_q(P) < 0$ pour un certain q. Cependant, le lemme suivant montre que si $\hat{\mathrm{h}}(P)$ est "assez petit", alors $\hat{\mathrm{h}}_q(P)$ ne peut pas être "trop petit négativement". Plus précisément,

Lemme 3.2.7 (Lemma 8.8, [26]). *Soit $(P_i)_i$ une suite de points de $E(\overline{\mathbb{Q}})\backslash E_{\mathrm{tors}}$ telle que $\lim_{i\to+\infty} \hat{\mathrm{h}}(P_i) = 0$. Si l est une place de $\mathbb{Q}$ (non nécessairement finie), alors*

$$\varliminf_{i\to+\infty} \hat{\mathrm{h}}_l(P_i) \geq 0.$$

De plus, si l est finie et si E a bonne réduction en l, alors $\hat{\mathrm{h}}_l(P_i) \geq 0$ pour tout i.

Comme E a bonne réduction pour presque toute place l de $\mathbb{Q}$ (i.e. pour toutes sauf un nombre fini), il s'ensuit que pour tout l, $\hat{\mathrm{h}}_l(P) \geq 0$ pour presque tout l et tout $P \in E(\overline{\mathbb{Q}})$. Par conséquent, le lemme 3.2.7 montre que si la hauteur $\hat{\mathrm{h}}(P_i)$ est "assez petite" pour un certain i avec $P_i \notin E_{\mathrm{tors}}$, alors $\hat{\mathrm{h}}_p(P_i) \geq 0$ (on rappelle que E a bonne réduction en p) est également "assez petit" d'après (3.23). Le résultat suivant est la contraposée de la phrase précédente, i.e. que si $\hat{\mathrm{h}}_p(P_i)$ est "assez grand" pour tout i, alors $\hat{\mathrm{h}}(P_i)$ l' est également pour tout i. Plus précisément,

Lemme 3.2.8. *Soit $(P_i)_i$ une suite de points de $E(\overline{\mathbb{Q}})\backslash E_{\mathrm{tors}}$ telle qu'il existe $c > 0$ vérifiant $\hat{\mathrm{h}}_p(P_i) \geq c$ pour tout i. Il existe alors $c' > 0$ tel que $\hat{\mathrm{h}}(P_i) \geq c'$ pour tout i.*

Démonstration. Supposons par l'absurde que $\varliminf_{i\to+\infty} \hat{\mathrm{h}}(P_i) = 0$. Quitte à en extraire une sous-suite, on peut supposer que $\lim_{i\to+\infty} \hat{\mathrm{h}}(P_i) = 0$. Comme E a bonne réduction en presque toute place l, cela signifie que pour presque tout l, on a que $\hat{\mathrm{h}}_l(P_i) \geq 0$ pour tout i. En utilisant la première affirmation du lemme 3.2.7, on en déduit l'existence d'un entier n_0 tel que $\sum_{l\neq p} \hat{\mathrm{h}}_l(P_i) \geq -c/2$ pour tout $i \geq n_0$. Par conséquent, on déduit de (3.23) que

$$\hat{\mathrm{h}}(P_i) = \hat{\mathrm{h}}_p(P_i) + \sum_{l\neq p} \hat{\mathrm{h}}_l(P_i) \geq c/2,$$

ce qui contredit le fait que $\lim_{i\to+\infty} \hat{\mathrm{h}}(P_i) = 0$. □

Soit $P = (x, y) \in E(\mathbb{Q}_{r,s})$ avec $r \geq s$. Comme E a bonne réduction en p et que $\nu_{r,s}$ est l'unique idéal premier de $\mathcal{O}_{\mathbb{Q}_{r,s}}$ au-dessus de p, on déduit alors de (3.22) que :

$$\hat{\mathrm{h}}_p(P) = \lambda_{\nu_{r,s}}(P) := \frac{1}{2}\log\max\{1, |x|_{\nu_{r,s}}\} \tag{3.24}$$

où la seconde égalité provient de la définition même de $\lambda_{\mathfrak{q}}$, dans le cas où E a bonne réduction en $\mathfrak{q}$ [43, Chapter VI].

Pour tous entiers $r \geq s$ positifs, avec $r \geq 1$, tels que $(r, s) \neq (1, 0)$, fixons à partir de maintenant un générateur $\sigma_{r,s}$ du dernier groupe de ramification non trivial de la suite $(\mathrm{Gal}(\mathbb{Q}_{r,s}/\mathbb{Q})_i(\nu_{r,s}))_i$, qui est cyclique d'ordre p d'après le v) du lemme 3.2.4. Pour tout $i \geq 0$, on a l'isomorphisme suivant :

$$\mathrm{Gal}(\mathbb{Q}_{r,s}/\mathbb{Q})_i(\nu_{r,s}) \simeq \mathrm{Gal}((\mathbb{Q}_{r,s})_{\nu_{r,s}}/\mathbb{Q}_p) = \mathrm{Gal}((\mathbb{Q}_p)_{r,s}/\mathbb{Q}_p).$$

On peut ainsi identifier $\sigma_{r,s}$ avec un élément de $\mathrm{Gal}((\mathbb{Q}_p)_{r,s}/\mathbb{Q}_p)$.

La proposition suivante est l'analogue de [26, Lemma 8.4], mais dont la preuve possède plus de détails.

Proposition 3.2.9. *Soient $r \geq s$ des entiers positifs tels que $r \geq 1$ et tels que $(r, s) \neq (1, 0)$. Soit $P \in E(\mathbb{Q}_{r,s})$ tel que $\sigma_{r,s}P \neq P$. Alors*

$$\lambda_{\nu_{r,s}}(\sigma_{r,s}P - P) \geq \frac{\log p}{p^2}.$$

Démonstration. Afin d'alléger les notations, notons $L = \mathbb{Q}_{r,s}$, $\sigma = \sigma_{r,s}$, $l = l_{r,s}$ (cf lemme 3.2.4, iv)) et $\nu = \nu_{r,s}$. Notons également l le dernier saut de l'extension $(\mathbb{Q}_{r,s})_{\nu_{r,s}}/\mathbb{Q}_p$. Notons $P = (x, y)$, $\sigma P = (x', y')$ et $Q = \sigma P - P = (x'', y'')$. Comme deux conjugués de L_ν ont la même valeur absolue, on en déduit que $|x|_\nu = |x'|_\nu$ et $|y|_\nu = |y'|_\nu$. Pour l'instant, supposons que $x \neq x'$, i.e. que $\sigma P \neq \pm P$.

Commençons par le cas où $|x|_\nu = |x'|_\nu \leq 1$. Comme $y^2 = x^3 + ax + b$ avec $a, b \in \mathbb{Z}_p$, on en déduit que $|y|_\nu = |y'|_\nu \leq 1$. Comme σ appartient (par définition) au dernier groupe de ramification de $\mathrm{Gal}(L_\nu/\mathbb{Q}_p)$, il s'ensuit que $|x' - x|_\nu \leq p^{-(l+1)/e}$. Or, $p^2(l + 1) \geq e$ d'après le iv) du lemme 3.2.4. Ainsi, $|x' - x|_\nu \leq p^{-1/p^2}$. De même, on a $|y' - y|_\nu \leq p^{-1/p^2}$.

La formule d'addition de deux points sur une courbe elliptique (cf [44, Chapter III, Algorithm 2.3]) donne la relation suivante :

$$x'' = \left(\frac{y' + y}{x' - x}\right)^2 - x' - x. \tag{3.25}$$

Ensuite, en soustrayant l'égalité $y^2 = x^3 + ax + b$ à l'égalité $y'^2 = x'^3 + ax' + b$ on obtient, après factorisation et division par $x' - x \neq 0$, que

$$\frac{y' + y}{x' - x} = \frac{x'^2 + x'x + x^2 + a}{y' - y}. \tag{3.26}$$

Supposons d'abord que $|y + y'|_\nu \geq 1$ (i.e. $|y + y'|_\nu = 1$ puisque $|y|_\nu = |y'|_\nu \leq 1$). Comme $|x|_\nu = |x'|_\nu \leq 1$ et que $|x' - x|_\nu^{-2} > 1$, il s'ensuit, en passant à la valeur absolue dans (3.25), que

$$|x''|_\nu = \max\left\{\left|\frac{y + y'}{x' - x}\right|_\nu^2, |x' + x|_\nu\right\} = |x' - x|_\nu^{-2} \geq p^{2/p^2}.$$

Du (3.24), on en déduit que $\lambda_\nu(Q) = \frac{1}{2}\log|x''|_\nu \geq (\log p)/p^2$.

Supposons maintenant que $|y'+y|_\nu < 1$. Comme $|y'-y|_\nu \leq p^{-1/p^2} < 1$, on en déduit que $|y|_\nu < 1$. Comme $p > 2$, il en résulte que

$$y^2 = x^3 + ax + b \equiv 0 \mod \nu. \tag{3.27}$$

De plus, $|y|_\nu^2 = |x|_\nu^3$ et $|y'|_\nu^2 = |x'|_\nu^3$. Ainsi, $|x|_\nu, |x'|_\nu < 1$ et on en déduit que $|x'^2 + x'x + x^2 + a|_\nu \leq 1$. Comme notre modèle E a bonne réduction en ν, cela implique que $(x, 0)$ est un point singulier sur la réduite de E modulo ν. De (3.27), il s'ensuit que $3x^2 + a \not\equiv 0 \mod \nu$. Comme $x' \equiv x \mod \nu$, on en conclut que $x'^2 + x'x + x^2 + a \not\equiv 0 \mod \nu$. Ceci prouve donc que $|x'^2 + x'x + x^2 + a|_\nu = 1$.

De (3.26), on en déduit alors que $|(y'+y)/(x'-x)|_\nu = 1/|y'-y|_\nu$. En injectant cette égalité dans (3.25), il s'ensuit que $|x''|_\nu = |y-y'|_\nu^{-2} > 1$. Comme dans le cas précédent, on en déduit que $\lambda_\nu(Q) \geq (\log p)/p^2$.

Supposons maintenant que $|x|_\nu > 1$ (et donc $|x|_\nu = |x'|_\nu > 1$ et $|y'|_\nu = |y|_\nu > 1$). Posons $t = -x/y$. Comme $|x|_\nu^2 = |y|_\nu^3$, on en déduit que $|t|_\nu = |x|_\nu^{-1/2} < 1$. De même, posons $t' = -x'/y'$. En plongeant $\mathbb{Q}$ dans $\mathbb{Q}_p$, on peut également voir E comme une courbe elliptique sur $\mathbb{Q}_p$. On note $F \in \mathbb{Z}_p[[X, Y]]$ la loi formelle associée à $E/\mathbb{Q}_p$ (pour plus de détails, le lecteur pourra consulter [44, Chapter IV]). Notons également $i \in \mathbb{Z}_p[[X]]$ l'unique série entière telle que $F(X, i(X)) = 0$ (cf [44, Chapter IV, Remark 2.1]). Comme $Q = \sigma P - P = (x'', y'')$, il s'ensuit que $t'' = -x''/y'' = F(t', i(t))$.

Comme $F(T, i(T)) = 0$, on en déduit l'existence d'une série entière $G \in \mathbb{Z}_p[[T_1, T_2]]$ telle que $F(T_1, T_2) = (i(T_1) - T_2)G(T_1, T_2)$. En prenant $T_1 = t'$ et $T_2 = i(t)$, on en déduit que $t'' = (i(t') - i(t))G(t', i(t))$. En passant à la valeur absolue ν-adique, il s'ensuit que

$$|t''|_\nu = |i(t'-t)|_\nu |G(t', i(t))|_\nu \leq |t'-t|_\nu. \tag{3.28}$$

Enfin, $t \in \mathcal{O}_{L_\nu}$ et $t' = \sigma t$. Il s'ensuit donc que $|t'-t|_\nu \leq p^{-(l+1)/e} \leq p^{-1/p^2}$. Comme $|x''|_\nu^{-1/2} = |t''|_\nu$, on déduit du (3.28) que $|x''|_\nu \geq p^{2/p^2}$. Comme précédemment, on en déduit que $\lambda_\nu(Q) \geq (\log p)/p^2$. On a ainsi montré la proposition dans le cas où $x' \neq x$.

Si $x' = x$ alors, $\sigma P = \pm P$. Or, $\sigma P \neq P$ par hypothèse. D'où, $\sigma P = -P$. Soit $(P_i)_i$ une suite de points de $E(L_\nu)$ qui converge (pour la topologie induite par la valeur absolue ν-adique) vers 0 telle que $\sigma P_i \neq \pm P_i$ pour tout i. Alors, $\sigma(P - P_i) - (P - P_i)$ converge vers $Q \neq 0$ par hypothèse. Ainsi, $\sigma(P - P_i) \neq (P - P_i)$ pour tout i assez grand. De plus, $\sigma(P - P_i) \neq -(P - P_i)$ puisque $\sigma P = -P$ et $\sigma P_i \neq -P_i$ par hypothèse. Par conséquent, l'abscisse du point $\sigma(P - P_i)$ est différente de l'abscisse de $P - P_i$. On s'est ainsi ramener au cas où $x \neq x'$. On en déduit donc que $\lambda_\nu(\sigma(P - P_i) - (P - P_i)) \geq (\log p)/p^2$ pour tout i assez grand. Enfin, comme λ_ν est continue sur $E(L_\nu)\backslash\{0\}$, on en déduit, en passant à la limite, que $\lambda_\nu(\sigma P - P) \geq (\log p)/p^2$, ce qui prouve la proposition. □

La proposition 3.2.9, couplée avec le lemme 3.2.8, permet d'en déduire le corollaire ci-dessous :

Corollaire 3.2.10. *Soit $(P_i)_i$ une suite de points de $E(\mathbb{Q}_{\infty,\infty})\backslash E_{\text{tors}}$. Pour tout i, choisissons un couple d'entiers $(r_i, s_i) \neq (1,0)$ tel que $r_i \geq s_i$, $r_i \geq 1$ et tel que $P_i \in E(\mathbb{Q}_{r_i,s_i})$. Supposons que $\lim_{i\to+\infty} \hat{\text{h}}(P_i) = 0$. Il existe alors un entier n_0 tel que $\sigma_{r_i,s_i}P_i - P_i \in E_{\text{tors}}$ pour tout $i \geq n_0$.*

Démonstration. Afin d'alléger les notations, notons $B_i = \sigma_{r_i,s_i}P_i - P_i$. Supposons par l'absurde qu'il existe une infinité d'entiers i telle que $B_i \notin E_{\text{tors}}$. Quitte à en extraire une sous-suite, on peut supposer que c'est vrai pour tout i. De la proposition 3.2.9 et du (3.24), on en déduit que $\hat{\text{h}}_p(B_i) \geq (\log p)/p^2$ pour tout i. Le lemme 3.2.8, appliqué à $c = (\log p)/p^2$, permet d'en déduire l'existence d'un $c' > 0$ tel que $\hat{\text{h}}(B_i) \geq c'$. Or, l'égalité du parallélogramme [44, Theorem 9.3] affirme que

$$\hat{\text{h}}(B_i) + \hat{\text{h}}(\sigma_{r_i,s_i}P_i + P_i) = 2(\hat{\text{h}}(\sigma_{r_i,s_i}(P_i)) + \hat{\text{h}}(P_i)).$$

Il s'ensuit donc que $\hat{\text{h}}(B_i) \leq 4\hat{\text{h}}(P_i)$. On obtient ainsi que $\hat{\text{h}}(P_i) \geq c'/4$, ce qui contredit le fait que $\lim_{i\to+\infty} \hat{\text{h}}(P_i) = 0$. □

De ce corollaire, il devient maintenant pertinent pour nous d'étudier les points $P \in E(\mathbb{Q}_{r,s})$ tels que $\sigma_{r,s}P - P \in E_{\text{tors}}$.

Proposition 3.2.11. *Soient $r \geq s$ des entiers tels que $r \geq 1$ et $(r,s) \neq (1,0)$. Soit $P \in E(\mathbb{Q}_{r,s})$ tel que $\sigma_{r,s}P - P \in E_{\text{tors}}$. Alors $P \in \mathbb{Q}_{r,s}^{\langle\sigma_{r,s}\rangle}$.*

Démonstration. Afin d'alléger les notations, notons $\sigma = \sigma_{r,s}$ et $B = \sigma_{r,s}P - P$. Notons également M l' ordre de $B \in E_{\text{tors}} \cap E(\mathbb{Q}_{r,s})$. Comme $\mathbb{Q}_{r,s} \subset (\mathbb{Q}_p)_{r,s}$, on déduit de la remarque 3.2.6 que M est premier à p. Dans ce cas, $\mathbb{Q}_p(E[M])/\mathbb{Q}_p$ est une extension non ramifiée d'après [44, Chapter VII, exercise 7.9]. Comme $(\mathbb{Q}_p)_{r,s}/\mathbb{Q}_p$ est totalement ramifié d'après le *ii)* du lemme 3.2.4, il s'ensuit donc que

$$B \in E((\mathbb{Q}_p)_{r,s} \cap \mathbb{Q}_p(E[M])) = E(\mathbb{Q}_p).$$

Ceci implique que $\sigma B = B$ ou encore que $\sigma^2 P = [2]\sigma P - P$. Par une simple récurrence, on en déduit que $\sigma^i P = [i]\sigma P - [i-1]P$ pour tout $i \geq 2$. En prenant $i = p$, il s'ensuit, car σ est d'ordre p, que $[p]\sigma P = [p]P$ et donc que $[p]B = 0$. Comme on a également que $[M]B = 0$ avec $p \nmid M$, on en déduit que $B = 0$. D'où $P \in \mathbb{Q}_{r,s}^{\langle\sigma\rangle}$. □

Remarque 3.2.12. En utilisant le *v)* du lemme 3.2.4, cette proposition montre que si $P \in E(\mathbb{Q}_{r,s})$ (avec $r \geq 1$ et $(r,s) \neq (1,0)$) est tel que $\sigma_{r,s}P - P \in E_{\text{tors}}$, alors

$$P \in \begin{cases} E(\mathbb{Q}_{r-1,s}) \text{ si } r > s \\ E(\mathbb{Q}_{r,s-1}) \text{ si } r = s \end{cases}.$$

Cela permet de montrer, comme énoncé dans le dernier paragraphe de l'introduction, que les points de torsion de $E(\mathbb{Q}_{\infty,\infty})$ sont tous dans $E(\mathbb{Q}(\zeta_p))$.

Fait 3.2.13. *On a $E_{\text{tors}} \cap E(\mathbb{Q}_{\infty,\infty}) = E_{\text{tors}} \cap E(\mathbb{Q}(\zeta_p))$.*

Démonstration. Soit $P \in E_{\text{tors}} \cap E(\mathbb{Q}_{\infty,\infty})$. Notons (r,s) le plus petit couple d'entiers (pour l'ordre lexicographique) tel que $r \geq s$ et $P \in E(\mathbb{Q}_{r,s})$ (c'est clair qu'un tel couple existe). Comme $P \in E_{\text{tors}}$, on a alors que $\sigma_{r,s}P - P \in E_{\text{tors}}$.

Ainsi, la proposition 3.2.11 et la remarque 3.2.12 contredisent la minimalité de (r,s), à condition que $r \geq 1$ et que $(r,s) \neq (1,0)$. On obtient ainsi que $r = 0$ ou que $(r,s) = (1,0)$. Il s'ensuit donc que $\mathbb{Q}_{r,s} \subset \mathbb{Q}(\zeta_p)$. D'où $\mathbb{Q}_{r,s} \subset \mathbb{Q}(\zeta_p)$, ce qui prouve le fait. □

Nous sommes maintenant en mesure de prouver le théorème 3.2.3, que l'on rappelle pour la commodité du lecteur :

Théorème. *Soit $b \in \mathbb{N}^*$ tel que $p \nmid b$ et $p^2 \nmid (b^{p-1}-1)$. Il existe alors $c > 0$ tel que $\hat{\mathrm{h}}(P) \geq c$ pour tout $P \in E(\mathbb{Q}(\langle b \rangle_{\mathrm{sat},p}))\backslash(E(\mathbb{Q}(\zeta_p)) \cap E_{\mathrm{tors}})$.*

Démonstration. Soit $(P_i)_i$ une suite de points de $E(\mathbb{Q}_{\infty,\infty})$ telle que $\lim_{i\to+\infty} \hat{\mathrm{h}}(P_i) = 0$. Pour tout i, il existe $t_i \geq 1$ tel que $P_i \in E(\mathbb{Q}_{t_i,t_i})$. Notons Λ_i l'ensemble des couples $(r,s) \in \mathbb{N}^2$ tel que $t_i \geq r \geq s$ et tel que $P_i \in E(\mathbb{Q}_{r,s})$. Remarquons que $\Lambda_i \neq \emptyset$ puisque $(t_i,t_i) \in \Lambda_i$. Ainsi, Λ_i admet un élément minimal pour l'ordre lexicographique que l'on nomme (r_i,s_i).

Supposons que $(r_i,s_i) \neq (1,0)$ et que $r_i \geq 1$ pour une infinité de i. Quitte à en extraire une sous-suite, on peut supposer que c'est vrai pour tout i. Par minimalité de (r_i,s_i), on déduit de la proposition 3.2.11 et de la remarque 3.2.12 que $B_i := \sigma_{r_i,s_i}P_i - P_i \notin E_{\mathrm{tors}}$. Ainsi, la proposition 3.2.9 et (3.22) montrent que $\hat{\mathrm{h}}_p(B_i) \geq (\log p)/p^2$ pour tout i. D'après le lemme 3.2.8, il existe alors une constante $c' > 0$ telle que $\hat{\mathrm{h}}(B_i) \geq c'$. Or, l'égalité du parallélogramme affirme que

$$\hat{\mathrm{h}}(B_i) + \hat{\mathrm{h}}(\sigma_{r_i,s_i}P_i + P_i) = 2(\hat{\mathrm{h}}(\sigma_{r_i,s_i}(P_i)) + \hat{\mathrm{h}}(P_i)).$$

Il s'ensuit donc que $\hat{\mathrm{h}}(B_i) \leq 4\hat{\mathrm{h}}(P_i)$. Par conséquent, $\hat{\mathrm{h}}(P_i) \geq c'/4$, ce qui contredit le fait que $\lim_{i\to+\infty} \hat{\mathrm{h}}(P_i) = 0$.

On a donc montré qu'il existe un rang n_0 à partir duquel $r_i = 0$ ou $(r_i,s_i) = (1,0)$ pour tout i. Ainsi, $P_i \in E(\mathbb{Q}(\zeta_p))$ pour tout $i \geq n_0$. Comme $\lim_{i\to+\infty} \hat{\mathrm{h}}(P_i) = 0$, un célèbre théorème de Northcott montre l'existence d'un entier $n_1 > 0$ tel que $P_i \in E_{\mathrm{tors}} \cap E(\mathbb{Q}(\zeta_p))$ pour tout $i \geq n_1$. Ceci prouve le théorème.

□

Bibliographie

[1] M. Acosta de Orozco and W.Y. Vélez. *The lattice of subfields of a radical extension.* J. Number Theory, no 15 : p. 388–405, 1982.

[2] F. Amoroso. *On a conjecture of G. rémond.* Ann. Sc. Norm. Super. Pisa Cl. Sci., no 15 : p. 599–608, 2016.

[3] F. Amoroso, S. David and U. Zannier. *On fields with the property (B)*, Proc. Amer. Math. Soc., vol. 142, no.6, p. 1893–1910, 2014.

[4] F. Amoroso and R. Dvornicich. *A lower bound for the height in abelian extensions*, J. Number Theory, vol. 80, no. 2, p.260–272, 2000.

[5] F. Amoroso and U. Zannier. *A uniform relative Dobrowolski's lower bound over abelian extensions.* Bull. Lond. Math. Soc., vol. 42, no. 3, p. 489–498, 2010.

[6] M. Baker and J.H. Silverman. *A lower bound for the canonical height on abelian varieties over abelian extensions*, Math. Res. Lett., vol.11, no.2-3, p. 377–396, 2004.

[7] M. Bhargava. *The density of discriminants of quartic rings and fields*, Ann. of Math. (2), vol. 162, no. 2, p. 1031–1063, 2005.

[8] M. Bhargava. *The density of discriminants of quintic rings and fields*, Ann. of Math. (2), vol. 172, no 3, p. 1559–1591, 2010.

[9] Y. Bilu *Limit distribution of small points on algebraic tori*, Duke Math. J., vol.89, no. 3, p. 465-476, 1997.

[10] E. Bombieri and W. Gubler. *Heights in Diophantine geometry*, Cambridge University Press, Cambridge, 2006.

[11] E. Bombieri and U. Zannier. *A note on heights in certain infinite extensions of* $\mathbb{Q}$, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl., vol. 12, p. 5–14 (2002), 2001.

[12] L. Capuano and I. Del Corso. *A note on upper ramification jumps in Abelian extensions of exponent p.* Riv. Math. Univ. Parma (N.S.), no 6 : p. 317–329, 2015.

[13] J.W.S. Cassels and A. Fröhlich. *Algebraic number theory*, Proceedings of an instructional conference organized by the London Mathematical Society, Academic press, London ; Thompson Book Co., Inc., Washington, D.C., 1967.

[14] S. Checcoli. *Fields of algebraic numbers with bounded local degrees and their properties*, Trans. Amer. Math. Soc., no. 4, vol. 365 : p. 2223–2240, 2013

[15] S. Checcoli and M. Widmer. *On the Northcott property and other properties related to polynomial mappings*, Math. Proc. Cambridge Philos. Soc., no. 1, vol. 155 : p. 1–12, 2013

[16] H. Cohen. *Advanced topics in computational number theory*, vol. 193. Springer-Verlag, N.Y., 2000.

[17] G. Cornell. *On the Construction of Relative Genus Fields*, Trans. Amer. Math. Soc., vol. 271, no. 2, p. 501–511, 1982.

[18] H. Davenport and H. Heilbronn. *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A, vol. 322, no. 1551, p. 405–420, 1971.

[19] I. Del Corso and Roberto Dvornicich. *Uniformity over primes of tamely ramified splittings*, Manuscripta Math., vol. 101, no. 2, p. 239–266, 2000.

[20] I. Del Corso and R. Dvornicich. *The compositum of wild extensions of local fields of prime degree*, Monatsh. Math., vol. 150, no. 4, p. 271–288, 2007

[21] E. Dobrowolski. *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith., vol.34, no.4, p. 391–401, 1979.

[22] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt. *Linear equations in variables which lie in a multiplicative group.* Ann. of Math. (2), vol.155, no.3, p. 807–836, 2002.

[23] G. Frei. *Heinrich Weber and the emergence of class field theory*, in *The history of modern mathematics, Vol. I (Poughkeepsie, NY, 1989)*, Academic Press, Boston, MA, p. 425–450, 1989.

[24] A. Fröhlich and M.J. Taylor. *Algebraic number theory*, Cambridge University Press, Cambridge, vol.27, 1993.

[25] A. Galateau. *Small height in fields generated by singular moduli*, Proc. Amer. Math. Soc., vol. 144, no.7, p. 2771–2786, 2016.

[26] P. Habegger. *Small height and infinite nonabelian extensions*, Duke Math. J., vol.162, no.11, p. 2027–2076, 2013.

[27] O. Jacquinot and K. Ribet. *Deficient points on extensions of abelian varieties by* $\mathbf{G}_m$, J. Number Theory, vol. 25, no. 2, p. 133–151, 1987.

[28] M. Krasner. *Nombre des extensions d'un degré donné d'un corps p-adique*, in *Les Tendances Géom. en Algèbre et Théorie des Nombres*, Editions du Centre National de la Recherche Scientifique, Paris, p. 143–169, 1966.

[29] S. Lang. *Algebra, third edition*, vol. 211. Springer-Verlag, N.Y., 2002.

[30] F. Laubie, *Suites de groupes de ramification supérieurs*, in *Séminaire Delange-Pisot-Poitou, 20e année : 1978/1979. Théorie des nombres, Fasc. 1 (French)*, Secrétariat Math., Paris, 1980.

[31] D.H. Lehmer. *Factorization of certain cyclotomic functions*, Ann. of Math. (2), vol.34, no.3, p. 461–479, 1933.

[32] J. Neukirch. *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, Berlin, vol. 322, 1999.

[33] A. Obus. *Conductors of wild extensions of local fields, especially in mixed characteristic* $(0, 2)$, Proc. Amer. Math. Soc., vol. 142, no. 5, p. 1485-1495, 2014.

[34] A. Plessis *Minoration de la hauteur dans un compositum de corps de rayon* à paraître dans : J. Number Theory, DOI : 10.1016/j.jnt.2019.05.008

[35] L. Pottmeyer. *Small totally p-adic algebraic numbers*, Int. Jour. of Number Theory, vol 14, no 10 : p. 2687–2697, 2018.

[36] G. Rémond. *Généralisations du problème de Lehmer et applications à la conjecture de Zilber-Pink*, *Panor. Synthèses*, vol.52, p. 243–284, 2017.

[37] A. Schinzel. *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith., vol.24, p.385–399, 1973.

[38] A. Schinzel. *Abelian binomials, power residues and exponential congruences* Acta Arith., no 32 : p. 245–274, 1977.

[39] J.P. Serre. *Corps locaux, Deuxième édition*, No. VIII. Hermann, Paris, 1968.

[40] J.P. Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., vol. 15, no. 4, p. 259–331, 1972.

[41] D. Shanks. *The simplest cubic fields*, Math. Comp., vol. 28, p. 1137–1152, 1974.

[42] R.T. Sharifi. *Ramification groups of nonabelian Kummer extensions* J. Number Theory, vol. 65, no. 1, p. 105–115, 1997.

[43] J. Silverman. *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, vol.151, 1994.

[44] J. H Silverman. *The arithmetic of elliptic curves*, Deuxième édition, Graduate Texts in Mathematics, vol. 106 Springer, Dordrecht, 2009

[45] C.J. Smyth. *On the measure of totally real algebraic integers*, J. Austral. Math. Soc. Ser. A, vol.30, no.2, p. 137–149, 1980/1981.

[46] F. Viviani. *Ramification groups and Artin conductors of radical extensions of* $\mathbb{Q}$. J. Théor. Nombres Bordeaux, no 16, p. 779–816, 2004.