Approche p-adique de la conjecture de Greenberg (cas totalement réel p-décomposé)

Georges Gras

APPROCHE p-ADIQUE DE LA CONJECTURE DE GREENBERG (CAS TOTALEMENT RÉEL p-DÉCOMPOSÉ)

GEORGES GRAS

Abstract. Let k be a totally real number field ant let k_∞ be its cyclotomic $\mathbb{Z}_p$-extension for a prime $p > 2$. We give (Theorem 3.4) a sufficient condition of nullity of the Iwasawa invariants λ, μ, when p totally splits in k, and we obtain important tables giving quadratic fields and various p for which we can conclude that $\lambda = \mu = 0$.

We show that the number of ambiguous p-classes of k_n (the nth stage in k_∞) becomes equal to the order of the torsion group $\mathcal{T}_k$, of the Galois group of the maximal Abelian p-ramified pro-p-extension of k (Theorem 4.7), for all $n \geq e$, where p^e is the exponent of $U_k^*/\overline{E}_k$ (local units of norm 1 modulo global units). Thus we recover some classical results of Fukuda, Greenberg, Inatomi, Komatsu, Sumida, Taya, ...

Then we establish analogs of Chevalley's formula for a family $(\Lambda_i)_{0\leq i\leq m_n}$ of subgroups of $k^\times$, prime to p, containing E_k, in which any x is norm of an ideal of k_n (Theorem 4.9, Corollary 4.12). This family is attached to the subgroups of the classical filtration of the p-class group of k_n giving the theoretical algorithm computing its order in m_n steps.

We show that $m_n \geq (\lambda \cdot n + \mu \cdot p^n + \nu)/v_p(\#\mathcal{T}_k)$ and that the condition $m_n = O(1)$ (i.e., $\lambda = \mu = 0$) depends essentially on the $\mathfrak{p}$-adic valuations, for $\mathfrak{p} \mid p$, of the $\frac{x_i^{p-1}-1}{p}$, $x_i \in \Lambda_i$, so that Greenberg's conjecture seems strongly related to the (tricky) properties of "Fermat quotients" of suitable elements of $k^\times$. A statistical analysis of these Fermat quotients (Section 7) shows that they follow natural probabilities, whatever the value of n, showing that, almost surely, $\lambda = \mu = 0$ (see the main Heuristic 7.3).

This would imply that for a proof of Greenberg's conjecture, some deep p-adic results are necessary before referring to the purely algebraic Iwasawa theory.

1. Introduction

Nous appelons *Conjecture de Greenberg pour les corps de nombres totalement réels* k, le fait que les invariants d'Iwasawa $\lambda_p(k)$ et $\mu_p(k)$ de leur p-tour cyclotomique k_∞ sont nuls (quel que soit p). Comme la nullité de $\lambda_p(k)$ et $\mu_p(k)$ implique celle relative aux sous-corps de k, on pourra toujours supposer $k/\mathbb{Q}$ Galoisienne réelle de degré d. Le corps k et le nombre premier p étant fixés, on désigne pour simplifier par λ, μ, ν les invariants d'Iwasawa pour k et p.

Dans l'approche classique, la décomposition de p dans $k/\mathbb{Q}$ joue un rôle important et nous nous limiterons ici au cas où p est totalement décomposé. La raison est la suivante : la nullité du p-groupe des classes $\mathcal{C}\ell_{k_n}$ du n-ième étage k_n de k_∞ est, en supposant implicitement que p est totalement ramifié dans k_∞/k, équivalente à celle de (formule des classes ambiges de Chevalley) :

$$\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{C}\ell_k \cdot \frac{p^{n\cdot(t-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))},$$

où $G_n = \mathrm{Gal}(k_n/k)$, $t \mid d$ est le nombre d'idéaux premiers au-dessus de p dans k, $\mathcal{C}\ell_k$ est le p-groupe des classes de k, et E_k son groupe des unités.

Date: 27 Novembre 2016.

1991 *Mathematics Subject Classification.* Primary 11R23, 11R29; 11R37.

Key words and phrases. Greenberg's conjecture, Iwasawa's theory, p-class groups, S-units, class field theory, p-adic regulators, Leopoldt's conjecture.

Le cas $t = 1$ implique $E_k \subset \mathrm{N}_{k_n/k}(k_n^\times)$ (formule du produit des symboles de restes normiques) et les invariants λ et μ dépendent essentiellement du comportement du p-groupe des classes de k par extension des idéaux dans la tour ([Gre, Theorem 1, § 4]).

Le cas $t = d$ montrera que, sous la conjecture de Leopoldt, le facteur $\dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ a même valuation p-adique que le régulateur p-adique normalisé R_k de k (Théorème 4.7).

Si $1 < t < d$, l'étude se ramène grosso modo aux cas précédents, ce que l'on peut justifier par exemple au moyen du cas Abélien réel de degré d étranger à p (en se reportant au principe de découpage selon les caractères p-adiques de $\mathrm{Gal}(k/\mathbb{Q})$ lorsque $p \nmid d$, e.g., [Gra5] et [Hi]) : si k' est le corps de décomposition de p dans k, alors $\dfrac{p^{n\cdot(t-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ est le produit de $\dfrac{p^{n\cdot(t-1)}}{(E_{k'} : E_{k'} \cap \mathrm{N}_{k'_n/k'}(k'^\times_n))}$ et de $\dfrac{1}{(E_k^* : E_k^* \cap \mathrm{N}_{k_n/k}(k_n^\times))} = 1$, où l'on a posé $E_k = E_{k'} \bigoplus E_k^*$ (à un indice près étranger à p), où E_k^* est le sous-groupe des unités de k de norme 1 sur k'. Autrement dit, on a toujours $E_k^* \subset \mathrm{N}_{k_n/k}(k_n^\times)$ pour tous les étages de la tour et on est ramené au cas totalement décomposé pour k'. Cependant, s'il existe un p-groupe de classes relatives dans k/k', la question est analogue, en relatif, au cas non décomposé $t = 1$.

2. Conjecture de Greenberg (cas totalement décomposé)

Soit k un corps de nombres Galoisien réel de degré d et soit $p > 2$ un nombre premier totalement décomposé dans k. Soit $\mathbb{Q}_\infty$ la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$ et $k_\infty := k\,\mathbb{Q}_\infty$ celle de k ; puisque p est non ramifié dans $k/\mathbb{Q}$, on a $k \cap \mathbb{Q}_\infty = \mathbb{Q}$. Il y a alors totale ramification de p dans k_∞/k.

On désigne par $k_n \subset k_\infty$ l'extension de degré p^n de k et par G_n son groupe de Galois. Soient $\mathcal{C}\ell_k$ et $\mathcal{C}\ell_{k_n}$ (resp. $\mathcal{C}\ell_k^{S_k}$ et $\mathcal{C}\ell_{k_n}^{S_{k_n}}$) les p-groupes des classes de k et k_n (resp. les S_k et S_{k_n}-groupes des classes de k et k_n) où S_k et S_{k_n} sont les ensembles des p-places de k et k_n respectivement. On a $\mathcal{C}\ell_k^{S_k} := \mathcal{C}\ell_k/\mathcal{C}\ell_k(S_k)$ où $\mathcal{C}\ell_k(S_k)$ est le sous-groupe de $\mathcal{C}\ell_k$ engendré par les p-classes des éléments de S_k (et de même pour $\mathcal{C}\ell_{k_n}^{S_{k_n}}$).

Théorème 2.1. [Gre, Theorem 2, (1976)]. *Sous les hypothèses et notations précédentes, et sous la conjecture de Leopoldt pour p dans k, les invariants $\lambda_p(k)$ et $\mu_p(k)$ d'Iwasawa sont nuls si et seulement si pour tout n assez grand, on a $\mathcal{C}\ell_{k_n}^{G_n} = \mathcal{C}\ell_{k_n}(S_{k_n})$ (i.e., le sous-groupe des p-classes ambiges de k_n est égal au sous-groupe engendré par les p-classes des éléments de S_{k_n}).*

On notera que dans cet énoncé interviennent le p-groupe des classes ambiges $\mathcal{C}\ell_{k_n}^{G_n}$ et le groupe $\mathcal{C}\ell_{k_n}(S_{k_n})$ qui est un sous-groupe du p-groupe des classes du groupe des idéaux invariants $I_{k_n}^{G_n}$; or on a l'isomorphisme classique $\mathcal{C}\ell_{k_n}^{G_n}/\mathcal{C}\ell_{k_n}(I_{k_n}^{G_n}) \simeq E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)/\mathrm{N}_{k_n/k}(E_{k_n})$, où E_k (resp. E_{k_n}) est le groupe des unités de k (resp. k_n). Or seul $E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)$, donné par le corps de classes local, est accessible en pratique, $\mathrm{N}_{k_n/k}(E_{k_n})$ étant un invariant arithmétique non trivial associé à l'extension k_n/k, ce qui explique la difficulté du calcul de λ et μ en termes d'unités globales (éventuellement comparées aux unités cyclotomiques du cadre Abélien comme dans [KS]). On a par ailleurs $\mathcal{C}\ell_{k_n}(I_{k_n}^{G_n}) = \mathcal{C}\ell_{k_n}(S_{k_n}) \cdot j_{k_n/k}(\mathcal{C}\ell_k)$, où $j_{k_n/k}$ est l'extension des classes de k à k_n ; la relation $\mathcal{C}\ell_{k_n}^{G_n} = \mathcal{C}\ell_{k_n}(S_{k_n})$ implique donc, de plus, la relation $j_{k_n/k}(\mathcal{C}\ell_k) \subseteq \mathcal{C}\ell_{k_n}(S_{k_n})$ pour tout n assez grand.

Remarque 2.2. Il est clair que si pour tout n assez grand on a $\mathcal{C}\ell_{k_n}^{G_n} = 1$, la conjecture de Greenberg est vraie ; or cette propriété a lieu si et seulement si (formule des classes ambiges de Chevalley qui s'écrit ici $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{C}\ell_k \cdot \dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}$, cf. Remarque 3.3) :

$$\mathcal{C}\ell_k = 1 \quad \& \quad (E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)},$$

puisque ici p est totalement ramifié dans k_n/k. On verra plus loin que la condition normique sur les unités équivaut au fait que le régulateur p-adique normalisé R_k de k (cf. [Gra6, Définition 2.3 (i)]) est une unité p-adique ; il en résultera que la condition $\mathcal{C}\ell_{k_n}^{G_n}=1$ pour tout n assez grand est équivalente à la nullité du groupe de torsion $\mathcal{T}_k$ de $\mathrm{Gal}(H_k^{\mathrm{pr}}/k)$ (i.e. p-rationalité de k), où H_k^{pr} est la pro-p-extension Abélienne p-ramifiée maximale de k (Théorème 4.7) (en effet, $\#\mathcal{T}_k=\#\mathcal{C}\ell_k\cdot R_k$). En outre on montrera que la condition $\mathcal{C}\ell_{k_n}^{G_n}=1$ pour tout n assez grand est équivalente à $\mathcal{C}\ell_{k_1}^{G_1}=1$ (Proposition 4.6).

3. Condition suffisante de nullité de λ et μ

Nous avons démontré dans [Gra3, (1973)], [Gra2, (1994)], et repris récemment dans [Gra4, Theorem 3.6, (2016)], le résultat suivant valable en toute généralité, ici énoncé dans le cas "$T=\emptyset$" qui correspond aux groupes de classes au sens classique (l'énoncé n'utilisant que la ramification des places finies et l'éventuelle complexification des places à l'infini on doit utiliser le sens restreint) ; on désigne par I_K et P_K le groupe des idéaux de K et son sous-groupe des idéaux principaux (au sens restreint) :

Théorème 3.1. *Soit K/k une extension cyclique quelconque de corps de nombres, de groupe de Galois G. Soient $\mathcal{C}\ell_K$ et $\mathcal{C}\ell_k$ les groupes des classes au sens restreint de K et k respectivement. Soit $e_{\mathfrak{q}}$ l'indice de ramification dans K/k d'un idéal premier $\mathfrak{q}$. Alors pour tout sous-G-module $\mathcal{H}$ de $\mathcal{C}\ell_K$ et tout sous-groupe $\mathcal{I}$ de I_K tel que $\mathcal{I}\cdot P_K/P_K=\mathcal{H}$, on a :*

$$\#\big(\mathcal{C}\ell_K/\mathcal{H}\big)^G=\frac{\#\mathcal{C}\ell_k\cdot\prod_{\mathfrak{q}}e_{\mathfrak{q}}}{[K:k]\cdot\#\mathrm{N}_{K/k}(\mathcal{H})\cdot(\Lambda:\Lambda\cap\mathrm{N}_{K/k}(K^\times))},\tag{1}$$

où $\mathrm{N}_{K/k}$ est la norme arithmétique et $\Lambda:=\{x\in k^\times\,(x\gg 0),\ \ (x)\in\mathrm{N}_{K/k}(\mathcal{I})\}$.

Corollaire 3.2. *Si $\mathcal{H}=cl_K(S_K)$, où S_K est un ensemble fini quelconque d'idéaux premiers de K, on obtient :*

$$\#\mathcal{C}\ell_K^{S_KG}=\frac{\#\mathcal{C}\ell_k\cdot\prod_{\mathfrak{q}}e_{\mathfrak{q}}}{[K:k]\cdot\#cl_k(\mathrm{N}S_K)\cdot(E_k^{\mathrm{N}S_K}:E_k^{\mathrm{N}S_K}\cap\mathrm{N}_{K/k}(K^\times))},\tag{2}$$

où $\mathrm{N}=\mathrm{N}_{K/k}$ et donc, $E_k^{\mathrm{N}S_K}=\{x\in E_k^{S_k}(x\gg 0),\ \ v_{\mathfrak{q}}(x)\equiv 0\pmod{f_{\mathfrak{q}}}\ \forall\mathfrak{q}\in S_k\}$, où S_k est l'ensemble des idéaux premiers de k au-dessous de S_K et $f_{\mathfrak{q}}$ le degré résiduel de $\mathfrak{q}$ dans K/k.

Jaulent a obtenu dans [Ja1, p. 177, (1986)] une autre écriture de cette même formule (2) :

$$\#\mathcal{C}\ell_K^{S_KG}=\frac{\#\mathcal{C}\ell_k^{S_k}\cdot\prod_{\mathfrak{q}\notin S_k}e_{\mathfrak{q}}\cdot\prod_{\mathfrak{q}\in S_k}e_{\mathfrak{q}}\,f_{\mathfrak{q}}}{[K:k]\cdot(E_k^{S_k}:E_k^{S_k}\cap\mathrm{N}_{K/k}(K^\times))}.$$

On peut utiliser la relation $E_k^{S_k}\cap\mathrm{N}_{K/k}(K^\times)=E_k^{\mathrm{N}S_K}\cap\mathrm{N}_{K/k}(K^\times)$ et la suite exacte :

$$1\longrightarrow E_k^{S_k}/E_k^{\mathrm{N}S_K}\longrightarrow\langle S_k\rangle_{\mathbb{Z}}/\langle\mathrm{N}_{K/k}S_K\rangle_{\mathbb{Z}}\longrightarrow cl_k(S_k)/cl_k(\mathrm{N}_{K/k}S_K)\longrightarrow 1$$

pour comparer les deux expressions. Dans l'application que nous en ferons (totale ramification de S_k dans K/k) on aura $\mathrm{N}_{K/k}S_K=S_k$ quel que soit $K\subset k_\infty$.

Remarques 3.3. (i) Il est important de noter que la relation (1) (et ses analogues) peut se mettre sous la forme du produit de deux entiers :

$$\#\big(\mathcal{C}\ell_K/\mathcal{H}\big)^G=\frac{[H_k:K\cap H_k]}{\#\mathrm{N}_{K/k}(\mathcal{H})}\times\frac{\prod_{\mathfrak{q}}e_{\mathfrak{q}}}{[K:K\cap H_k]\cdot(\Lambda:\Lambda\cap\mathrm{N}_{K/k}(K^\times))},\tag{3}$$

où H_k est le corps de classes de Hilbert de k ; si $K\cap H_k=k$, alors le premier facteur est égal à $\dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{K/k}(\mathcal{H})}$.

La norme $\mathrm{N}_{K/k}:\mathcal{C}\ell_K\to\mathcal{C}\ell_k$ a pour image le sous-groupe de $\mathcal{C}\ell_k$ isomorphe à $\mathrm{Gal}(H_k/K\cap H_k)$.

(ii) Pour $K = k_n \subset k_\infty$, $G = G_n = \mathrm{Gal}(k_n/k)$, et pour les ensembles de p-places S_k et S_{k_n} (p totalement décomposé dans $k/\mathbb{Q}$), la formule devient :

$$\#\mathcal{C}\ell_{k_n}^{S_{k_n}G_n} = \#\mathcal{C}\ell_k^{S_k} \times \frac{p^{n\cdot(d-1)}}{(E_k^{S_k} : E_k^{S_k} \cap \mathrm{N}_{k_n/k}(k_n{}^\times))}. \tag{4}$$

On peut alors énoncer, en désignant maintenant par $\mathcal{C}\ell$ les *p-groupes de classes*, et en prenant un corps de la forme k_n, de degré p^n, de groupe de Galois G_n :

Théorème 3.4. *Soit k un corps de nombres Galoisien réel de degré d et soit $p > 2$ un nombre premier totalement décomposé dans k vérifiant la conjecture de Leopoldt pour p dans k. Soit k_1, de degré p sur k, le premier étage de la $\mathbb{Z}_p$-extension cyclotomique de k. Alors une condition suffisante pour que $\lambda = \mu = 0$ est que les deux conditions suivantes soient réalisées, où S_k est l'ensemble des p-places de k :*
(i) $\mathcal{C}\ell_k^{S_k} = 1$ (i.e., S_k engendre le p-groupe des classes de k),
(ii) $(E_k^{S_k} : E_k^{S_k} \cap \mathrm{N}_{k_1/k}(k_1^\times)) = p^{d-1}$.

Démonstration. Soit $n \geq 1$ et considérons k_n. On a la suite exacte de G_n-modules :

$$1 \longrightarrow \mathcal{A}\ell_{k_n}(S_{k_n}) \longrightarrow \mathcal{C}\ell_{k_n} \longrightarrow \mathcal{C}\ell_{k_n}^{S_{k_n}} \longrightarrow 1,$$

qui conduit à :

$$1 \longrightarrow \mathcal{A}\ell_{k_n}(S_{k_n})^{G_n} \longrightarrow \mathcal{C}\ell_{k_n}^{G_n} \longrightarrow \mathcal{C}\ell_{k_n}^{S_{k_n}G_n} \longrightarrow \mathrm{H}^1(G_n, \mathcal{A}\ell_{k_n}(S_{k_n})).$$

Ici, comme p est totalement ramifié dans k_∞/k, on a $\mathcal{A}\ell_{k_n}(S_{k_n})^{G_n} = \mathcal{A}\ell_{k_n}(S_{k_n})$ et finalement :

$$1 \longrightarrow \mathcal{C}\ell_{k_n}^{G_n}/\mathcal{A}\ell_{k_n}(S_{k_n}) \longrightarrow \mathcal{C}\ell_{k_n}^{S_{k_n}G_n} = (\mathcal{C}\ell_{k_n}/\mathcal{A}\ell_{k_n}(S_{k_n}))^{G_n} \longrightarrow \mathrm{H}^1(G_n, \mathcal{A}\ell_{k_n}(S_{k_n})),$$

qui fait que la condition $\mathcal{C}\ell_{k_n}^{S_{k_n}G_n} = 1$ pour tout n assez grand implique la conjecture de Greenberg (cf. Théorème 2.1) ; cette condition équivaut à la réunion de la condition (i) et de la condition $(E_k^{S_k} : E_k^{S_k} \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)}$ d'après (4). Or d'après la Proposition 4.6, il suffit que cette dernière condition soit satisfaite pour $n = 1$ pour qu'elle le soit pour tout n. □

Remarques 3.5. (i) Pour le cas des corps quadratiques réels, il est facile de faire un programme qui teste cette condition suffisante quel que soit $p > 2$. La condition de nullité du S_k-groupe des classes de k doit être examinée en relation avec la détermination des S_k-unités puisque celles-ci dépendent de l'ordre de la classe des $\mathfrak{p} \in S_k$.
(ii) On a $\mathrm{H}^1(G_n, \mathcal{A}\ell_{k_n}(S_{k_n})) = {}_{\nu_n}\mathcal{A}\ell_{k_n}(S_{k_n})$ où ν_n est la norme algébrique pour G_n ; par conséquent, si $\mathrm{N}_{k_n/k}$ est la norme arithmétique et $j_{k_n/k}$ l'extension des classes, on a $\nu_n = j_{k_n/k} \circ \mathrm{N}_{k_n/k}$ avec surjectivité de la norme arithmétique. Fixons $n \geq 1$. On a $\mathrm{H}^1(G_n, \mathcal{A}\ell_{k_n}(S_{k_n})) = 0$ si et seulement si ν_n est injective, donc si et seulement si (l'image de ν_n étant $j_{k_n/k}(\mathcal{A}\ell_k(S_k))$ puisque $\mathrm{N}_{k_n/k}(S_{k_n}) = S_k$) on a l'isomorphisme :

$$\nu_n : \mathcal{A}\ell_{k_n}(S_{k_n}) \xrightarrow{\simeq} j_{k_n/k}(\mathcal{A}\ell_k(S_k)) \subseteq \mathcal{A}\ell_{k_n}(S_{k_n})$$

qui indique que $\mathcal{A}\ell_{k_n}(S_{k_n}) = j_{k_n/k}(\mathcal{A}\ell_k(S_k))$; or $j_{k_n/k}(\mathcal{A}\ell_k(S_k)) = \mathcal{A}\ell_{k_n}(S_{k_n})^{p^n}$ puisque si $\mathfrak{p} \in S_k$, on a $j_{k_n/k}(\mathfrak{p}) = \mathfrak{P}^{p^n}$, $\mathfrak{P} \mid \mathfrak{p}$ dans k_n, d'où $\mathcal{A}\ell_{k_n}(S_{k_n}) = \mathcal{A}\ell_{k_n}(S_{k_n})^{p^n}$ et $\mathcal{A}\ell_{k_n}(S_{k_n}) = 1$. On a donc $\mathrm{H}^1(G_n, \mathcal{A}\ell_{k_n}(S_{k_n})) = 0$ si et seulement si $\mathcal{A}\ell_{k_n}(S_{k_n}) = 1$.

4. Symboles de restes normiques

Par commodité, rappelons (d'après [Gra1, II.4.4.3]) une méthode de calcul (global) des symboles de restes normiques de Hasse $\left(\dfrac{x\,,\,k_n/k}{\mathfrak{p}}\right) \in G_n := \mathrm{Gal}(k_n/k)$, dans le cas particulier d'un corps de nombres Galoisien réel k avec $k_n \subset k_\infty$ de degré p^n sur k, et relativement à un idéal premier $\mathfrak{p} \mid p$ de k.

Dans notre cas ($p > 2$ totalement décomposé), le conducteur de k_n/k divise (p^{n+1}) puisque localement, $1 + p^{n+1}\,\alpha_0 = (1 + p\,\alpha_0')^{p^n} = \mathrm{N}_{k_n/k}(1 + p\,\alpha_0')$, où α_0, α_0' sont des p-entiers du produit des complétés $\prod_{\mathfrak{p}|p} k_{\mathfrak{p}}$ de k. Le conducteur de $\mathbb{Q}_n$ est p^{n+1} pour tout $n \geq 1$.

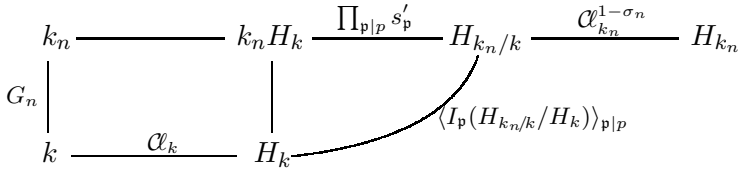
Les calculs en question sont liés à la théorie des genres dont nous rappelons l'essentiel ci-après. On désigne par H_k (resp. H_{k_n}) le p-corps de classes de Hilbert de k (resp. k_n).

4.1. **Suite exacte des genres pour les sous-corps de k_∞/k.** Dans le cas p totalement décomposé dans k, les groupes d'inertie $I_{\mathfrak{p}}(k_n/k)$ des $\mathfrak{p} \mid p$ dans k_n/k sont égaux à G_n.

On considère l'application ω_n qui associe à $x \in E_k$ la famille des symboles de Hasse $\left(\frac{x\,,\,k_n/k}{\mathfrak{p}}\right)$, $\mathfrak{p} \mid p$. On obtient alors la suite exacte des genres interprètant la formule du produit des symboles de Hasse d'une unité (voir, e.g., [Gra1, Proposition IV.4.5.1] pour $T = S = \emptyset$) :

$$(5) \qquad 1 \longrightarrow E_k/E_k \cap \mathrm{N}_{k_n/k}(k_n^\times) \xrightarrow{\omega_n} \bigoplus_{\mathfrak{p}|p} I_{\mathfrak{p}}(k_n/k) \xrightarrow{\pi_n} \mathrm{Gal}(H_{k_n/k}/k_n H_k) \longrightarrow 1,$$

où $H_{k_n/k}$ *est le p-corps des genres de* k_n défini comme la sous-extension maximale de H_{k_n}, Abélienne sur k, selon le schéma suivant où l'on sait que $H_{k_n/k}$ est fixe par l'image de $\mathcal{C}\ell_{k_n}^{1-\sigma_n}$, où σ_n est un générateur de G_n (en effet, le groupe des commutateurs $[\Gamma, \Gamma]$ de $\Gamma = \mathrm{Gal}(H_{k_n}/k)$ est $\mathrm{Gal}(H_{k_n}/k_n)^{1-\sigma_n}$ puisque $\Gamma/\mathrm{Gal}(H_{k_n}/k_n)$ est cyclique) :



L'image de ω_n est contenue dans $\Omega(k_n/k) := \left\{(s_{\mathfrak{p}})_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p}|p} I_{\mathfrak{p}}(k_n/k), \prod_{\mathfrak{p}|p} s_{\mathfrak{p}} = 1\right\} \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d-1}$ et l'application π_n est ainsi définie : à $(s_{\mathfrak{p}})_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p}|p} I_{\mathfrak{p}}(k_n/k)$, π_n associe le produit des relèvements $s_{\mathfrak{p}}'$ des $s_{\mathfrak{p}}$ dans les groupes d'inertie $I_{\mathfrak{p}}(H_{k_n/k}/H_k)$ qui engendrent $\mathrm{Gal}(H_{k_n/k}/H_k)$; il résulte de la formule du produit que si $(s_{\mathfrak{p}})_{\mathfrak{p}}$ est dans $\Omega(k_n/k)$, $\prod_{\mathfrak{p}|p} s_{\mathfrak{p}}'$ fixe à la fois H_k et k_n, donc $k_n H_k$. La suite exacte des genres montre que le noyau de π_n est $\omega_n(E_k)$.

On a comme attendu, puisque $\#\Omega(k_n/k) = p^{n\cdot(d-1)}$ et $H_k \cap k_\infty = k$,

$$[H_{k_n/k} : k_n] = \#\mathcal{C}\ell_k \cdot \frac{p^{n\cdot(d-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} = \#\mathcal{C}\ell_{k_n}^{G_n}.$$

On montrera que le degré $[H_{k_n/k} : k_n]$ (et donc $\#\mathcal{C}\ell_{k_n}^{G_n}$) est constant à partir du rang $n = e$ donné par l'exposant p^e du groupe de torsion de $\mathrm{Gal}(H_k^{\mathrm{pr}}/H_k)$, où H_k^{pr} est la pro-p-extension Abélienne p-ramifiée maximale de k et que ce degré est égal à $\#\mathcal{T}_k$, où $\mathcal{T}_k$ est le groupe de torsion de $\mathrm{Gal}(H_k^{\mathrm{pr}}/k)$ (cf. Théorèmes 4.7 et 4.9).

4.2. **Calcul effectif des symboles $\left(\frac{x\,,\,k_n/k}{\mathfrak{p}}\right)$.** Soit $x \in k^\times$ et soit $\mathfrak{p} \mid p$ un idéal premier de k au-dessus de p (x n'est pas supposé étranger à $\mathfrak{p}$). Soit $x_{\mathfrak{p}}' \in k^\times$ (appelé un $\mathfrak{p}$-associé de x relativement à k_n/k) tel que (théorème des restes chinois) :

(i) $x_{\mathfrak{p}}' x^{-1} \equiv 1 \pmod{\mathfrak{p}^{n+1}}$,

(ii) $x_{\mathfrak{p}}' \equiv 1 \pmod{\mathfrak{p}'^{n+1}}$, pour tout $\mathfrak{p}' \mid p,\ \mathfrak{p}' \neq \mathfrak{p}$.

Par la formule du produit, $\left(\frac{x_{\mathfrak{p}}'\,,\,k_n/k}{\mathfrak{p}}\right) = \prod_{\mathfrak{q}\,,\,\mathfrak{q}\neq\mathfrak{p}} \left(\frac{x_{\mathfrak{p}}'\,,\,k_n/k}{\mathfrak{q}}\right)^{-1}$, et comme $\left(\frac{x\,,\,k_n/k}{\mathfrak{p}}\right) = \left(\frac{x_{\mathfrak{p}}'\,,\,k_n/k}{\mathfrak{p}}\right)$ d'après (i) et par définition du $\mathfrak{p}$-conducteur local de k_n/k, $\left(\frac{x\,,\,k_n/k}{\mathfrak{p}}\right) = \prod_{\mathfrak{q}\,,\,\mathfrak{q}\neq\mathfrak{p}} \left(\frac{x_{\mathfrak{p}}'\,,\,k_n/k}{\mathfrak{q}}\right)^{-1}$.

Déterminons les symboles du membre de droite :

- si $\mathfrak{q} = \mathfrak{p}' \mid p$, $\mathfrak{p}' \neq \mathfrak{p}$, $x'_\mathfrak{p} \equiv 1 \pmod{\mathfrak{p}'^{n+1}}$ (d'après (ii)) et on a $\left(\frac{x'_\mathfrak{p}\,,\,k_n/k}{\mathfrak{p}'}\right) = 1$,
- si $\mathfrak{q} \nmid p$, $\mathfrak{q}$ est non ramifié et dans ce cas, $\left(\frac{x'_\mathfrak{p}\,,\,k_n/k}{\mathfrak{q}}\right) = \left(\frac{k_n/k}{\mathfrak{q}}\right)^{v_\mathfrak{q}(x'_\mathfrak{p})}$ (où $\left(\frac{k_n/k}{\mathfrak{q}}\right)$ est le symbole de Frobenius de $\mathfrak{q}$ et $v_\mathfrak{q}$ la valuation $\mathfrak{q}$-adique).

Finalement, $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right) = \prod_{\mathfrak{q}\nmid p} \left(\frac{k_n/k}{\mathfrak{q}}\right)^{-v_\mathfrak{q}(x'_\mathfrak{p})}$. Posons $\mathfrak{a}_\mathfrak{p}(x) = \prod_{\mathfrak{q}\nmid p} \mathfrak{q}^{v_\mathfrak{q}(x'_\mathfrak{p})}$ ($\mathfrak{a}_\mathfrak{p}(x)$ est étranger à p), alors on a :

$$(x'_\mathfrak{p}) =: \mathfrak{p}^{v_\mathfrak{p}(x'_\mathfrak{p})}\mathfrak{a}_\mathfrak{p}(x) = \mathfrak{p}^{v_\mathfrak{p}(x)}\mathfrak{a}_\mathfrak{p}(x), \tag{6}$$

et on a obtenu (pour $\mathfrak{p} \mid p$) $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right) = \left(\frac{k_n/k}{\mathfrak{a}_\mathfrak{p}(x)}\right)^{-1}$ (inverse du symbole d'Artin de $\mathfrak{a}_\mathfrak{p}(x)$). On vérifie que $\left(\frac{k_n/k}{\mathfrak{a}_\mathfrak{p}(x)}\right)$ ne dépend pas du choix de $x'_\mathfrak{p}$. Si $v_\mathfrak{p}(x) = 0$, alors $\mathfrak{a}_\mathfrak{p}(x) = (x'_\mathfrak{p})$.
En dépit des notations, $(x'_\mathfrak{p})$ et $\mathfrak{a}_\mathfrak{p}(x)$ dépendent de n.

D'après le théorème de relèvement normique dans $k/\mathbb{Q}$, l'image canonique de $\left(\frac{k_n/k}{\mathfrak{a}_\mathfrak{p}(x)}\right) \in G_n$ dans $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \{a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times,\ a \equiv 1 \pmod p\} \simeq \mathbb{Z}/p^n\mathbb{Z}$, est le symbole d'Artin $\left(\frac{\mathbb{Q}_n/\mathbb{Q}}{\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x))}\right)$ qui caractérise $\left(\frac{k_n/k}{\mathfrak{a}_\mathfrak{p}(x)}\right)$ et où $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x)) > 0$ (norme absolue). [1]

Définitions 4.1. *(i) Soit $x \in k^\times$ étranger à p. On suppose p totalement décomposé dans k. Alors on définit les coefficients $\delta_\mathfrak{p}(x) \geq 0$, pour tout $\mathfrak{p} \mid p$, par la relation :*

$$(x^{p-1} - 1) = p \cdot \prod_{\mathfrak{p}\mid p} \mathfrak{p}^{\delta_\mathfrak{p}(x)} \cdot \mathfrak{b}_p, \quad \mathfrak{b}_p \text{ étranger à } p.$$

(ii) Si x n'est pas étranger à p, on définit les coefficients $\delta_\mathfrak{p}(x) \geq 0$ par les relations :

$$\left((x \cdot p^{-v_\mathfrak{p}(x)})^{p-1} - 1\right) = \mathfrak{p} \cdot \mathfrak{p}^{\delta_\mathfrak{p}(x)} \cdot \mathfrak{b}_\mathfrak{p}, \quad \mathfrak{b}_\mathfrak{p} \text{ étranger à } \mathfrak{p}.$$

Ces définitions ont un rapport avec les groupes de classes logarithmiques et les valuations logarithmiques introduites par Jaulent (cf. [Ja4], [Ja6] et leurs bibliographies ainsi que [BJ] pour les aspects numériques ; voir aussi [Gra1, III.5]).
Dans le cas où x est étranger à p, on a $\delta_\mathfrak{p}(\tau x) = \delta_{\tau^{-1}\mathfrak{p}}(x)$ pour tout $\mathfrak{p} \mid p$ et $\tau \in \mathrm{Gal}(k/\mathbb{Q})$.

Lemme 4.2. *Soit $x \in k^\times$, x étranger à p, et soit $\mathfrak{p} \mid p$ fixé. Soit $\mathfrak{a}_\mathfrak{p}(x) = (x'_\mathfrak{p})$, où $x'_\mathfrak{p}$ est un $\mathfrak{p}$-associé de x relativement à k_n/k. Alors on a $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x)) \equiv x \pmod{\mathfrak{p}^{n+1}}$ et on a, pour tout $n \geq \delta_\mathfrak{p}(x)$, $\frac{1}{p} \cdot \log(\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x))) \equiv \alpha_\mathfrak{p}(x) \cdot p^{\delta_\mathfrak{p}(x)} \pmod{p^n}$, $\alpha_\mathfrak{p}(x) \in \mathbb{Z}_p^\times$.*

Démonstration. On peut écrire (i) et (ii) définissant $x'_\mathfrak{p}$, sous la forme :

(i′) $x'_\mathfrak{p}\, x^{-1} \equiv 1 \pmod{\mathfrak{p}^{n+1}}$,

(ii′) $x'_\mathfrak{p} \equiv 1 \pmod{\tau^{-1}\mathfrak{p}^{n+1}}$, pour tout $\tau \in \mathrm{Gal}(k/\mathbb{Q})$, $\tau \neq 1$.

On a $\mathrm{N}_{k/\mathbb{Q}}(x'_\mathfrak{p}) = \prod_{\tau\in\mathrm{Gal}(k/\mathbb{Q})} (\tau x'_\mathfrak{p}) = x'_\mathfrak{p} \cdot \prod_{\tau\neq 1} (\tau x'_\mathfrak{p})$ qui conduit à :

$$\mathrm{N}_{k/\mathbb{Q}}(x'_\mathfrak{p}) \equiv x \pmod{\mathfrak{p}^{n+1}}.$$

Donc, pour $n \geq \delta_\mathfrak{p}(x)$, il vient en élevant la congruence ci-dessus à la puissance $p-1$:

$$v_\mathfrak{p}(\mathrm{N}_{k/\mathbb{Q}}(x'_\mathfrak{p})^{p-1} - 1) = v_\mathfrak{p}(x^{p-1} - 1) = \delta_\mathfrak{p}(x) + 1;$$

mais comme $\mathrm{N}_{k/\mathbb{Q}}(x'_\mathfrak{p})$ est rationnel, on a $v_p(\mathrm{N}_{k/\mathbb{Q}}(x'_\mathfrak{p})^{p-1} - 1) = \delta_\mathfrak{p}(x) + 1$, d'où le lemme en prenant le "logarithme normalisé" $\frac{1}{p} \cdot \log$. □

Lemme 4.3. *Soient $\mathfrak{p} \mid p$ fixé et $x'_\mathfrak{p}$ un $\mathfrak{p}$-associé de x relativement à k_n/k, et soit $\mathfrak{a}_\mathfrak{p}(x) = (x'_\mathfrak{p}) \cdot \mathfrak{p}^{-v_\mathfrak{p}(x)}$. Alors on a $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x)) \equiv x \cdot p^{-v_\mathfrak{p}(x)} \pmod{\mathfrak{p}^{n+1}}$, et on a, pour tout $n \geq \delta_\mathfrak{p}(x)$, $\frac{1}{p} \cdot \log(\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x))) \equiv \alpha_\mathfrak{p}(x) \cdot p^{\delta_\mathfrak{p}(x)} \pmod{p^n}$, $\alpha_\mathfrak{p}(x) \in \mathbb{Z}_p^\times$.*

[1] Pour $p \neq 2$, $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ est l'ensemble des restrictions à $\mathbb{Q}_n$ des automorphismes définis sur les racines p^{n+1}-ièmes de l'unité ζ par $\zeta \longrightarrow \zeta^a$, pour $a > 0$, $a \equiv 1 \pmod p$. On a alors $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = 1 + p \cdot \mathbb{Z}_p$.

Démonstration. On a alors $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x)) = \mathrm{N}_{k/\mathbb{Q}}(x'_\mathfrak{p}) \cdot p^{-v_\mathfrak{p}(x)}$; on est ramené au calcul précédent via les congruences (i′), (ii′), où l'on aura $\mathrm{N}_{k/\mathbb{Q}}(x'_\mathfrak{p})\, x^{-1} \equiv 1 \pmod{\mathfrak{p}^{n+1}}$. Finalement, $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x)) \equiv x \cdot p^{-v_\mathfrak{p}(x)} \pmod{\mathfrak{p}^{n+1}}$ qui conduit à :

$$v_p(\mathrm{N}_{k/\mathbb{Q}}\big(\mathfrak{a}_\mathfrak{p}(x)\big)^{p-1} - 1\big) = v_\mathfrak{p}\big((x \cdot p^{-v_\mathfrak{p}(x)})^{p-1} - 1\big) = \delta_\mathfrak{p}(x) + 1,$$

et à une conclusion analogue pour l'expression du logarithme. □

Vu comme élément de $\{a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times,\ a \equiv 1 \pmod p\}$, le symbole d'Artin $\left(\frac{\mathbb{Q}_n/\mathbb{Q}}{\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x))}\right)$ est représenté sous forme additive par le logarithme normalisé $\frac{1}{p} \cdot \log$ (avec $\log(p) = 0$) de $a_\mathfrak{p}(x) := \mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x)) > 0$. On identifie par abus cet automorphisme d'Artin à :

$$\tfrac{1}{p} \cdot \log(a_\mathfrak{p}(x)) =: \alpha_\mathfrak{p}(x) \cdot p^{\delta_\mathfrak{p}(x)} \pmod{p^n}, \quad \alpha_\mathfrak{p}(x) \in \mathbb{Z}_p^\times.$$

L'ordre de $\left(\frac{k_n/k}{\mathfrak{a}_\mathfrak{p}(x)}\right)$ dans G_n est l'ordre de $\left(\frac{\mathbb{Q}_n/\mathbb{Q}}{a_\mathfrak{p}(x)}\right)$ dans $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. On peut alors énoncer :

Théorème 4.4. *Soit k un corps de nombres Galoisien réel et soit $p > 2$ un nombre premier totalement décomposé dans k. Soit k_∞ la $\mathbb{Z}_p$-extension cyclotomique de k et, pour tout $n \geq 0$, soit k_n le sous-corps de k_∞ de degré p^n sur k. Soit $x \in k^\times$ et soient $\delta_\mathfrak{p}(x) \geq 0$, pour $\mathfrak{p} \mid p$, les entiers définis par $\delta_\mathfrak{p}(x) + 1 := v_\mathfrak{p}((x\, p^{-v_\mathfrak{p}(x)})^{p-1} - 1)$ pour tout $\mathfrak{p} \mid p$ (Définition 4.1) :*
(i) L'élément x est norme locale en $\mathfrak{p} \mid p$ dans k_n/k si et seulement si $\delta_\mathfrak{p}(x) \geq n$.
(ii) Pour $\mathfrak{p} \mid p$ fixé, soit $x'_\mathfrak{p}$ un $\mathfrak{p}$-associé de x relativement au calcul du symbole $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right)$ et soit $a_\mathfrak{p}(x) := \mathrm{N}_{k/\mathbb{Q}}((x'_\mathfrak{p}) \cdot p^{-v_\mathfrak{p}(x)})$. Alors, si $\delta_\mathfrak{p}(x) \leq n$, l'ordre et l'image de $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right)$ dans $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$ sont $p^{n-\delta_\mathfrak{p}(x)}$ et $\frac{1}{p} \cdot \log(a_\mathfrak{p}(x)) =: \alpha_\mathfrak{p}(x) \cdot p^{\delta_\mathfrak{p}(x)} \pmod{p^n}$, $\alpha_\mathfrak{p}(x) \in \mathbb{Z}_p^\times$.

Corollaire 4.5. *Si $x \in k^\times$, étranger à p, est partout norme locale en dehors de p dans k_n/k (i.e., (x) norme d'un idéal de k_n), il est alors partout norme locale (donc norme globale dans k_n/k) si et seulement si $\delta_\mathfrak{p}(x) \geq n$ pour tout $\mathfrak{p} \mid p$ (sauf un).*

D'un point de vue heuristique on a, a priori, $\delta_\mathfrak{p}(x) \geq 1$ avec la probabilité $\frac{1}{p}$, de sorte qu'en general $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right) = \left(\frac{k_n/k}{\mathfrak{a}_\mathfrak{p}(x)}\right)^{-1}$ est un générateur de G_n, ce qui est très favorable pour la conjecture de Greenberg. Cependant, le cas de $x \in k^\times$ partout norme locale en dehors de p dans k_n/k montre que, pour $\mathfrak{p} \mid p$, les $\delta_\mathfrak{p}(x)$ ne sont pas indépendants en raison de la formule du produit (considérée comme unique) ; on verra que ceci provient aussi du fait que $\mathrm{N}_{k/\mathbb{Q}}(x)^{p-1} \equiv 1 \pmod{p^{n+1}}$ (voir Section 7 pour une analyse détaillée).

Proposition 4.6. *Soit Λ un sous-groupe de $k^\times$ tel que tout $x \in \Lambda$ soit partout norme locale en dehors de p dans k_n/k, $n \geq 1$ donné (i.e., (x) est norme d'un idéal de k_n). On suppose que $(\Lambda : \Lambda \cap \mathrm{N}_{k_1/k}(k_1^\times)) = p^{d-1}$; alors on a $(\Lambda : \Lambda \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)}$.*
Si Λ est le groupe $E_k^{S_k}$ des S_k-unités, on a $(E_k^{S_k} : E_k^{S_k} \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)}$ pour tout $n \geq 1$ dès que ceci est vrai pour $n = 1$. De même pour $\Lambda = E_k$.

Démonstration. L'hypothèse signifie que $\omega_1(\Lambda) = \Omega(k_1/k)$ (cf. § 4.1). Il existe donc des éléments $x_i \in \Lambda$, $1 \leq i \leq d-1$, tels que $\Omega(k_1/k) = \bigoplus_{i=1}^{d-1} \langle \omega_1(x_i) \rangle$, où chaque $\omega_1(x_i) = \big(\big(\frac{x_i\,,k_1/k}{\mathfrak{p}}\big)\big)_{\mathfrak{p}|p}$ est d'ordre p ; les $\omega_1(x_i)$ sont les images canoniques (par restriction des symboles de Hasse) des $\omega_\infty(x_i) := \big(\big(\frac{x_i\,,k_\infty/k}{\mathfrak{p}}\big)\big)_{\mathfrak{p}|p}$ qui constituent une $\mathbb{Z}_p$-base topologique de $\Omega(k_\infty/k) \simeq \mathbb{Z}_p^{d-1}$ car toute relation $\prod_{i=1}^{d-1} \omega_\infty(x_i)^{a_i} = 1$, $a_i \in \mathbb{Z}_p$ non tous divisibles par p, conduit à une relation non triviale au niveau $n = 1$. Par restriction au niveau n, on obtient $\omega_n(\Lambda) = \bigoplus_{i=1}^{d-1} \langle \omega_n(x_i) \rangle$, d'ordre $p^{n\cdot(d-1)}$. Pour les S_k-unités, la condition de normes locales en dehors de p dans k_n/k est satisfaite pour tout n (totale ramification de p dans k_n/k). □

En pratique, ayant un système de générateurs de Λ dont on connait les $\delta_{\mathfrak{p}}$, on obtient facilement l'ordre de $\omega_n(\Lambda) \subseteq \Omega(k_n/k) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d-1}$.

4.3. **Groupe de torsion de la p-ramification Abélienne.** Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale $H_k^{\rm pr}$ de k. En appliquant la formule classique donnant $\#\mathcal{T}_k$ dans le cas réel sous la conjecture de Leopoldt (cf. [Co, Appendix, (1975)], [Gra1, Remark III.2.6.5 (i)]), en tenant compte du fait que $H_k \cap k_\infty = k$, que p est totalement décomposé dans k, que $\frac{\prod_{\mathfrak{p}\mid p} {\rm N}_{k/\mathbb{Q}}(\mathfrak{p})}{p} = p^{d-1}$, et que le régulateur p-adique normalisé R_k (cf. [Gra6, Définition 2.3 (i)]) est le régulateur p-adique classique précisément divisé par p^{d-1}, on a :

$$\#\mathcal{T}_k = \#\mathcal{C}\ell_k \cdot \#{\rm tor}_p(U_k/\overline{E}_k) \quad \& \quad \#{\rm tor}_p(U_k/\overline{E}_k) \sim R_k,$$

en désignant par $U_k := \prod_{\mathfrak{p}\mid p}(1+\mathfrak{p})$ le groupe des unités locales principales de k, et par $\overline{E}_k$ l'adhérence de E_k dans U_k. Par abus, nous écrirons que ce régulateur R_k est égal à $p^{v_p(R_k)}$ bien qu'il soit un élément non nul de $\mathbb{Z}_p$ défini à une unité p-adique près.

Posons $U_k^* := \{u \in U_k,\ {\rm N}_{k/\mathbb{Q}}(u) = 1\}$. De fait, on a ${\rm tor}_p(U_k/\overline{E}_k) = U_k^*/\overline{E}_k$, car U_k^* est un $\mathbb{Z}_p$-module libre de rang $d-1$ dans lequel $\overline{E}_k$ est d'indice fini (conjecture de Leopoldt).

Théorème 4.7. *Soit k un corps de nombres Galoisien réel de degré d dans lequel p est totalement décomposé. On suppose que la conjecture de Leopoldt est vraie pour p dans k. Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale $H_k^{\rm pr}$ de k et soit p^e l'exposant de $U_k^*/\overline{E}_k$. Alors :*

(i) Pour tout n, il existe une injection canonique ψ_n de $E_k \cap {\rm N}_{k_n/k}(k_n^\times)/E_k^{p^n}$ dans $U_k^*/\overline{E}_k$, et par conséquent $\dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap {\rm N}_{k_n/k}(k_n^\times))}$ divise R_k et $\#\mathcal{C}\ell_{k_n}^{G_n}$ divise $\#\mathcal{T}_k$ pour tout n.

(ii) Pour tout $n \geq e$, l'application ψ_n est de plus surjective et dans ce cas les divisibilités précédentes sont des égalités. En particulier $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{T}_k$ pour tout $n \geq e$.

Démonstration. Nous supposerons dans la suite que tout nombre étranger à p est de fait congru à 1 modulo p (quitte à l'élever à la puissance $p-1$).

Soit $\varepsilon \in E_k \cap {\rm N}_{k_n/k}(k_n^\times)$; vue dans U_k, on a $\varepsilon = {\rm N}_{k_n/k}(u_n)$, où $u_n \in U_{k_n} := \prod_{\mathfrak{P}\in S_{k_n}}(1+\mathfrak{P})$ et par conséquent on a $\delta_{\mathfrak{p}}(\varepsilon) \geq n$ pour tout $\mathfrak{p} \mid p$ (cf. Corollaire 4.5). Donc $\varepsilon = u_0^{p^n}$, $u_0 \in U_k$. Comme ${\rm N}_{k/\mathbb{Q}}(\varepsilon) = 1$, on a $u_0 \in U_k^*$.

(i) (définition de ψ_n). Soit ψ_n l'application qui à $\varepsilon \in E_k \cap {\rm N}_{k_n/k}(k_n^\times)$ associe la classe de u_0 dans $U_k^*/\overline{E}_k$. L'application ψ_n est définie car il n'y a pas de p-torsion dans U_k^*.

(ii) (calcul de ${\rm Ker}(\psi_n)$). Si $u_0 \in \overline{E}_k$, alors $\varepsilon \in (\overline{E}_k)^{p^n}$ est arbitrairement proche d'un élément de $E_k^{p^n}$; en effet, $\varepsilon = \varepsilon_N'^{p^n} \cdot u_N$, $\varepsilon_N' \in E_k$, $u_N \to 1$ dans E_k pour $N \to \infty$, d'où $u_N \in E_k^{p^n}$ (conjecture de Leopoldt [Gra1, Théorème III.3.6.2 (iv)]) ; d'où $\varepsilon \in E_k^{p^n}$ et ${\rm Ker}(\psi_n) = E_k^{p^n}$. A ce stade, puisque $(E_k : E_k^{p^n}) = p^{n\cdot(d-1)}$, on obtient pour tout n les divisibilités du (i) de l'énoncé.

(iii) (surjectivité pour $n \geq e$). Soit $u \in U_k^*$ et écrivons que $u^{p^e} \in \overline{E}_k$; pour $N \to \infty$, il existe $\varepsilon_N' \in E_k$ tel que $u^{p^e} = \varepsilon_N' \cdot u_N$, $u_N \to 1$ dans U_k^*. Il en résulte que $u_N = u_1^{p^N} = (u_1^{p^e})^{p^{N-e}}$, $u_1 \in U_k^*$ et $u_1^{p^e} =: \overline{\varepsilon} \in \overline{E}_k$ par définition de e. Donc $u_N = \overline{\varepsilon}'^{p^e}$ pour N assez grand, auquel cas on obtient $u^{p^e} = \varepsilon_N' \cdot \overline{\varepsilon}'^{p^e}$; par conséquent il existe $u' = u \cdot \overline{\varepsilon}'^{-1}$ dans la classe de u modulo $\overline{E}_k$ tel que $u'^{p^e} = \varepsilon_N'$. Posons $\varepsilon := \varepsilon_N'^{p^{n-e}} = u'^{p^n}$ (car $n \geq e$) ; il est clair que $\varepsilon \in {\rm N}_{k_n/k}(k_n^\times)$ et que $\psi_n(\varepsilon)$ est la classe de u modulo $\overline{E}_k$, d'où la surjectivité de ψ_n et le fait que $\dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap {\rm N}_{k_n/k}(k_n^\times))} = \#(U_k^*/\overline{E}_k)$ et $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{T}_k$.

(iv) (calcul direct de l'ordre pour $n \geq e$). On peut calculer $\#\mathcal{C}\ell_{k_n}^{G_n}$ de la façon suivante : puisque p^e annule $U_k^*/\overline{E}_k$, on a pour $n \geq e$, $U_k^*/\overline{E}_k = U_k^*/(U_k^*)^{p^n}\overline{E}_k$ et la suite exacte :

$$1 \longrightarrow \overline{E}_k/\overline{E}_k \cap (U_k^*)^{p^n} \longrightarrow U_k^*/(U_k^*)^{p^n} \longrightarrow U_k^*/(U_k^*)^{p^n}\overline{E}_k \longrightarrow 1.$$

On a $\overline{E}_k/\overline{E}_k \cap (U_k^*)^{p^n} = E_k/E_k \cap (U_k^*)^{p^n}$; or $E_k \cap (U_k^*)^{p^n} = E_k/E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)$; d'où le résultat puisque $\#(U_k^*/(U_k^*)^{p^n}) = p^{n\cdot(d-1)}$. □

Corollaire 4.8. *On a la suite exacte* $1 \longrightarrow E_k^{p^n} \longrightarrow E_k \cap \mathrm{N}_{k_n/k}(k_n^\times) \xrightarrow{\psi_n} U_k^*/\overline{E}_k \longrightarrow 1$, *pour tout* $n \geq e$.

Théorème 4.9. *Soit k un corps de nombres Galoisien réel de degré d dans lequel p est totalement décomposé. On suppose que la conjecture de Leopoldt est vraie pour p dans k. Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale H_k^{pr} de k et soit p^e l'exposant du groupe $U_k^*/\overline{E}_k$. On a les résultats suivants :*

(i) Le corps des genres $H_{k_n/k}$ de k_n est, sur k_n, de degré $\#\mathcal{T}_k$ pour tout $n \geq e$.

(ii) On a $k_\infty H_{k_e/k} = H_k^{\mathrm{pr}}$. Par conséquent l'extension $H_k^{\mathrm{pr}}/k_\infty$ est non ramifiée.[2]

(iii) Soit Λ un sous-groupe de $k^\times$, contenant E_k, tel que tout $x \in \Lambda$ soit norme locale dans k_n/k en dehors de p, pour un entier $n \geq 0$ donné (i.e., (x) est norme d'un idéal de k_n). Alors $\dfrac{p^{n\cdot(d-1)}}{(\Lambda : \Lambda \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ divise R_k. Pour $\Lambda \subseteq E_k^{S_k}$, cette divisibilité a lieu pour tout n.

(iv) Supposons que $p \nmid d$. Si Λ contenant E_k est étranger à p et constitué de normes locales dans k_n/k en dehors de p pour $n \geq e$, alors il existe une injection de $\Lambda/\Lambda \cap \overline{E}_k$ dans $U_k^*/\overline{E}_k$. On a la suite exacte $1 \to \Lambda \cap \overline{E}_k^{p^n} \longrightarrow \Lambda \cap \mathrm{N}_{k_n/k}(k_n^\times) \xrightarrow{\psi_n} U_k^*/\overline{E}_k \to 1$.

Démonstration. (i) Considérons les corps des genres $H_{k_e/k}$ et $H_{k_n/k}$ (cf. § 4.1) ; on a $H_{k_e/k}k_n \subseteq H_{k_n/k}$ en raison des hypothèses de ramification dans k_∞/k et de l'Abélianité au-dessus de k. D'où la valeur stationnaire du degré $[H_{k_n/k} : k_n]$ puisque $[H_{k_n/k} : k_n] = \#\mathcal{C}\ell_{k_n}^{G_n}$ et que $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{T}_k$ pour tout $n \geq e$ d'après le Théorème 4.7.

(ii) Conséquence immédiate de (i).

(iii) On a les injections canoniques $E_k/E_k \cap \mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \Lambda/\Lambda \cap \mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \Omega(k_n/k)$ car les symboles de Hasse en p des $x \in \Lambda$ vérifient la formule du produit par hypothèse ; donc $\dfrac{p^{n\cdot(d-1)}}{(\Lambda : \Lambda \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ divise $\dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ qui divise R_k (Théorème 4.7 (i)). Dans le cas de $E_k^{S_k}$, toute S_k-unité est norme locale en dehors de p dans k_n/k pour tout n.

(iv) Le premier point vient de la relation $\mathrm{N}_{k/\mathbb{Q}}(x)^{p-1} \equiv 1 \pmod{p^{n+1}}$ (cf. Corollaire 4.5) et du fait que $\mathrm{N}_{k/\mathbb{Q}}(U_k) = U_\mathbb{Q}$. L'application ψ_n du Théorème 4.7 est définie sur $\Lambda \cap \mathrm{N}_{k_n/k}(k_n^\times)$, car il existe une injection de $\Lambda/\Lambda \cap \overline{E}_k$ dans U_k^*, et ψ_n est a fortiori surjective. □

Remarque 4.10. La théorie des genres du § 4.1 dit que l'image par π_n de $\Omega(k_n/k)$ est $\mathrm{Gal}(H_{k_n/k}/k_nH_k)$ et que $\mathrm{Ker}(\pi_n) = \omega_n(E_k) \subseteq \Omega(k_n/k)$, où $\omega_n(\varepsilon) = \left(\left(\frac{\varepsilon\,,\,k_n/k}{\mathfrak{p}}\right)\right)_{\mathfrak{p}|p}$ pour tout $\varepsilon \in E_k$ et où $\#\omega_n(E_k) = (E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))$.

Autrement dit, pour tout n fixé, l'application $\theta_n := \pi_n \circ \omega_n$ définit un isomorphisme de $\Omega(k_n/k)/\omega_n(E_k)$ sur $\mathrm{Gal}(H_{k_n/k}/k_nH_k)$ et l'image d'un sous-groupe Λ (contenant E_k et constitué de normes locales en dehors de p dans k_n/k) par θ_n est un sous-groupe de $\mathrm{Gal}(H_{k_n/k}/k_nH_k)$ isomorphe à $\omega_n(\Lambda)/\omega_n(E_k)$, où $\#\omega_n(\Lambda) = (\Lambda : \Lambda \cap \mathrm{N}_{k_n/k}(k_n^\times))$.

[2]Ce résultat et une partie du Théorème 4.7 sont aussi démontrés dans [Ta2, Theorem 1.1, Lemma 2.3] par introduction du corps des genres. Il est aussi une conséquence du corps de classes ℓ-adique de Jaulent [Ja6, Corollaire 6].

Comme $H_{k_e/k}$ est contenu dans $H_{k_n/k}$ pour $n \geq e$, les symboles $\left(\frac{x\,,H_{k_e/k}/H_k}{\mathfrak{p}}\right)$ sont les restrictions des symboles $\left(\frac{x\,,H_{k_n/k}/H_k}{\mathfrak{p}}\right)$, et l'image de $\theta_n(\Lambda)$ dans la surjection canonique $\mathrm{Gal}(H_{k_n/k}/k_nH_k) \longrightarrow \mathrm{Gal}(H_{k_e/k}/k_eH_k)$ est égale à $\theta_e(\Lambda)$. Calculons son noyau :
Supposons que $x \in \Lambda$ est tel que $\pi_e \circ \omega_e(x) = 1$; on a donc $\omega_e(x) = \omega_e(\varepsilon)$, $\varepsilon \in E_k$, et on voit que cela implique $x \cdot \varepsilon^{-1}$ norme globale dans k_e/k ; donc $x \cdot \varepsilon^{-1} \in U_k^{*p^e} \subseteq \overline{E}_k$, soit $x \in \overline{E}_k$. Ceci implique facilement $x \in E_k \cdot \overline{E}_k^{p^n}$ et $\omega_n(x) \in \omega_n(E_k)$, d'où $\theta_n(x) = 1$ (injectivité de $\theta_n(\Lambda) \longrightarrow \theta_e(\Lambda)$) ; par conséquent on a $\theta_n(\Lambda) \simeq \theta_e(\Lambda) \subseteq \mathrm{Gal}(H_{k_n/k}/k_nH_k)$.
Tout ce qui précède relativement à l'entier $n \geq e$ est valable pour n' tel que $e \leq n' \leq n$.

Définition 4.11. *Soit p^e l'exposant de $U_k^*/\overline{E}_k$. Pour $n \geq e$, soit $\mathcal{N}_n$ le sous-groupe des $x \in k^\times$, x étranger à p, x partout norme locale en dehors de p.*
Soit θ_∞ l'application définie par $\theta_\infty(x) = \prod_{\mathfrak{p}|p} \left(\frac{x\,,H_k^{\mathrm{pr}}/H_k}{\mathfrak{p}}\right) \in \mathrm{Gal}(H_k^{\mathrm{pr}}/k_\infty H_k) \simeq U_k^*/\overline{E}_k$, pour tout $x \in \mathcal{N}_n$, où $\left(\frac{x\,,H_k^{\mathrm{pr}}/H_k}{\mathfrak{p}}\right)$ relève $\left(\frac{x\,,H_{k_n/k}/H_k}{\mathfrak{p}}\right)$ (cf. Théorème 4.9).

On peut énoncer avec ces définitions et la Remarque 4.10 (interprétation de Λ/E_k dans $\mathcal{T}_k$) :

Corollaire 4.12. *On a $\theta_\infty(E_k) = 1$ et pour tout sous-groupe Λ de $\mathcal{N}_n$, $n \geq e$, $\theta_\infty(\Lambda)$ est isomorphe à un sous-groupe de $U_k^*/\overline{E}_k$; en particulier $\#\theta_\infty(\Lambda)$ divise R_k. Comme $E_k^{S_k} \subset \mathcal{N}_n$ pour tout n, $\#\theta_\infty(E_k^{S_k})$ divise R_k.*

Remarques 4.13. (i) Certains résultats de théorie d'Iwasawa donnent des isomorphismes au niveau infini mettant en jeu le groupe $\mathcal{T}_k$ (cf. [LMN, Lemma 4.7], [Ta1], [Ta2], [OT], [BaN, Lemme 3.1]), mais en réalité, il y a régularisation à un niveau fini explicite. On peut également rappeler le comportement (lorsque $\mu = 0$) de λ dans les p-extensions (relations de Riemann–Hurwitz–Kida (e.g., [Iw], [Sin]), et analyse du phénomène à un niveau fini [Gra7]).
(ii) On a $\dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} = 1$ pour tout n assez grand si et seulement si ceci est vrai pour $n = 1$ (Proposition 4.6). Dans ce cas, $R_k = 1$, $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{T}_k = \#\mathcal{C}\ell_k$ pour tout n.
(iii) Si $\mathcal{T}_k = 1$ (i.e., k est p-rationnel), on a évidemment $\lambda = \mu = 0$; ceci s'applique dans de nombreux cas numériques, comme par exemple le corps cubique étudié dans [Ta3] pour $p = 5$. Plus généralement on trouvera de nombreux exemples concrets dans ce cadre et une étude détaillée des régulateurs p-adiques dans [Gra6]. Dans [Ja6, Théorèmes 11 et 15], les résultats sont exprimés en termes de groupes de classes logarithmiques, sous la conjecture de Gross-Kuzmin.
(iv) On a $\mathcal{T}_k = 1$ si et seulement si $\mathcal{C}\ell_k = R_k = 1$, et alors la formule de points fixes donnant $\#\mathcal{T}_{k_n}^{G_n}$ (cf. [Gra1, Théorème IV.3.3], § IV (b)) conduit à $\mathcal{T}_{k_n} = 1$ car k_n/k est "p-primitivement ramifiée". D'où $\mathcal{C}\ell_{k_n} = 1$ et $R_{k_n} = 1$ pour tout $n \geq 0$.

Théorème 4.14. *Soit k un corps de nombres Galoisien réel de degré d dans lequel p est totalement décomposé. On suppose que la conjecture de Leopoldt est vraie pour p dans k. Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale H_k^{pr} de k et soit p^e l'exposant de $U_k^*/\overline{E}_k$. Soit I_k le groupe des idéaux de k étrangers à p et, pour $n \geq 0$, soit $\widetilde{E}_k^n := \{x \in k^\times,\ (x) \in I_k^{p^n}\}$. Alors, $\widetilde{E}_k^n$ contient E_k et pour tout $n \geq e$, on a une suite exacte de la forme $1 \longrightarrow k^{\times p^n} \longrightarrow \widetilde{E}_k^n \cap \mathrm{N}_{k_n/k}(k_n^\times) \xrightarrow{\widetilde{\psi}_n} \mathcal{T}_k \longrightarrow 1$.*

Démonstration. Dans toute la suite, les nombres et idéaux considérés sont étrangers à p.
(i) (définition de $\widetilde{\psi}_n$). Soit $x \in \widetilde{E}_k^n \cap \mathrm{N}_{k_n/k}(k_n^\times)$; on a $(x) = \mathfrak{a}^{p^n}$ et x norme locale en p, d'où $x = u_0^{p^n}$ dans U_k ; par conséquent, pour $N \to \infty$, il existe $y_N \in k^\times$, $u_N \in k^\times$, $u_N \to 1$ dans U_k, tels que $x = y_N^{p^n} \cdot u_N$ et $(x) = \mathfrak{a}^{p^n}$, auquel cas :

$$(\mathfrak{a} \cdot (y_N)^{-1})^{p^n} = (u_N).$$

Alors, à x on associe la limite, lorsque $N \to \infty$, du symbole d'Artin $\left(\frac{H_k^{\rm pr}/k}{\mathfrak{a}\cdot(y_N)^{-1}}\right)$ qui est un élément de $\mathcal{T}_k$ (pour $\mathcal{T}_k$ vu comme sous-groupe de torsion de $\mathrm{Gal}(H_k^{\rm pr}/k) \simeq \mathcal{I}_k/\mathcal{P}_{k,\infty}$ en termes d'infinitésimaux, cf. [Gra1, III, § (b)], [Ja1], [Ja2], [Ja3], [Ja4]).

(ii) (noyau de $\widetilde{\psi}_n$). Si $\left(\frac{H_k^{\rm pr}/k}{\mathfrak{a}\cdot(y_N)^{-1}}\right)$ tend vers 1 lorsque $N \to \infty$, c'est que $\mathfrak{a}\cdot(y_N)^{-1}$ peut s'écrire $(u'_{N'})$, $u'_{N'} \to 1$, d'où $(u_N) = (u'_{N'})^{p^n}$, soit $u_N = u'^{p^n}_{N'} \cdot \varepsilon_N$, $\varepsilon_N \in E_k$; comme ε_N est arbitrairement proche de 1, on a $\varepsilon_N = \varepsilon'^{p^n}_{N'}$ (conjecture de Leopoldt) et finalement $x = y_N^{p^n} \cdot u'^{p^n}_{N'} \cdot \varepsilon'^{p^n}_{N'} \in k^{\times p^n}$, ce qui montre que le noyau est $k^{\times p^n}$.

(iii) (surjectivité de $\widetilde{\psi}_n$ pour $n \geq e$). On a la suite exacte immédiate :

$$1 \longrightarrow E_k/E_k^{p^n} \longrightarrow \widetilde{E}_k^n/k^{\times p^n} \longrightarrow \mathcal{C}\ell_k \longrightarrow 1.$$

En tenant compte de la suite exacte du Corollaire 4.8 (qui suppose $n \geq e$) et du fait que $\widetilde{E}_k^n \cap \mathrm{N}_{k_n/k}(k_n^\times)/k^{\times p^n}$ est isomorphe à un sous-groupe de $\mathcal{T}_k$, la surjectivité a lieu si et seulement si on montre que l'injection canonique $E_k/E_k \cap \mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \widetilde{E}_k^n/\widetilde{E}_k^n \cap \mathrm{N}_{k_n/k}(k_n^\times)$ est surjective, auquel cas il vient :

$$\begin{aligned}(\widetilde{E}_k : \widetilde{E}_k \cap \mathrm{N}_{k_n/k}(k_n^\times)) \cdot (\widetilde{E}_k \cap \mathrm{N}_{k_n/k}(k_n^\times) : k^{\times p^n}) \\ = \#\mathcal{C}\ell_k \cdot (E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)) \cdot (E_k \cap \mathrm{N}_{k_n/k}(k_n^\times) : E_k^{p^n}),\end{aligned}$$

d'où $(\widetilde{E}_k \cap \mathrm{N}_{k_n/k}(k_n^\times) : k^{\times p^n}) = \#\mathcal{C}\ell_k \cdot R_k = \#\mathcal{T}_k$.

Soit $x \in \widetilde{E}_k^n$; on a $(x) = \mathfrak{a}^{p^n}$ et on relève le symbole d'Artin $\left(\frac{H_k/k}{\mathfrak{a}}\right) \in \mathrm{Gal}(H_k/k)$ dans $\mathcal{T}_k$ en le symbole $\lim\limits_{N\to\infty}\left(\frac{H_k^{\rm pr}/k}{\mathfrak{a}'_N\cdot(y_N)^{-1}}\right)$ (cf. (i)), où $y_N \in k^\times$, et où $\mathfrak{a}'_N$ est dans la classe de $\mathfrak{a}$ et vérifie $(\mathfrak{a}'_N \cdot (y_N)^{-1})^{p^n} = (u'_{N'})$, avec $u'_{N'} \in k^\times$ tendant vers 1 (ceci est possible car la projection canonique $\mathcal{T}_k \longrightarrow \mathcal{C}\ell_k$ est surjective). On a alors, $\mathfrak{a} = \mathfrak{a}'_N \cdot (y_N)^{-1} \cdot (u_N)$, avec $u_N \in k^\times$ tendant vers 1. Donc $(x) = \mathfrak{a}^{p^n} = \left(\mathfrak{a}'_N \cdot (y_N)^{-1}\right)^{p^n} \cdot (u_N)^{p^n}$, et x est de la forme $x = u''_{N''} \cdot \varepsilon$, $\varepsilon \in E_k$, $u''_{N''} \in \widetilde{E}_k^n$, $u''_{N''} \to 1$. On considère alors ε dont l'image dans $\widetilde{E}_k^n/\widetilde{E}_k^n \cap \mathrm{N}_{k_n/k}(k_n^\times)$ est dans la classe de x. □

Corollaire 4.15. *On a l'isomorphisme $\widetilde{E}_k^e \cap \mathrm{N}_{k_e/k}(k_e^\times)/k^{\times p^e} \simeq \mathcal{T}_k$, où p^e est l'exposant de $U_k^*/\overline{E}_k$ et où $\widetilde{E}_k^e := \{x \in k^\times,\ (x) \in I_k^{p^e}\}$, où I_k est le groupe des idéaux de k étrangers à p.*

Remarques 4.16. (i) Une S_k-unité est norme locale en dehors de p dans k_n/k pour tout $n \geq 0$, tandis que pour $x \notin E_k^{S_k}$ ceci n'a lieu dans k_n/k que si (x) est norme d'un idéal de k_n : en effet, supposons x norme locale en dehors de p dans k_n/k, pour tout n, et posons $(x) = \mathfrak{a}\cdot\prod_{\mathfrak{p}|p}\mathfrak{p}^{c_\mathfrak{p}}$, $\mathfrak{a}$ étranger à p ; si $\mathfrak{l}^{c_\mathfrak{l}}$ est la composante $\mathfrak{l}$-primaire de $\mathfrak{a}$ pour l'idéal premier $\mathfrak{l}$, pour un idéal $\mathfrak{L}_n \mid \mathfrak{l}$ de k_n, il doit exister $\omega_n \in \mathbb{Z}[G_n]$ tel que $\mathfrak{l}^{c_\mathfrak{l}} = \mathrm{N}_{k_n/k}(\mathfrak{L}_n^{\omega_n}) = \mathfrak{l}^{f_\mathfrak{l}^n\cdot\omega_n(1)}$, où $f_\mathfrak{l}^n$ est le degré résiduel de $\mathfrak{l}$ dans k_n/k et $\omega_n(1) \in \mathbb{Z}$ est l'image de ω_n par l'application canonique $\mathbb{Z}[G_n] \longrightarrow \mathbb{Z}$. Comme les $f_\mathfrak{l}^n$ sont strictement croissants pour n assez grand, ceci est impossible pour tout n sauf si $c_\mathfrak{l} = \omega_n(1) = 0$, auquel cas x est une S_k-unité.

Par conséquent, dès que Λ est quelconque, pour chaque $x \in \Lambda$ il existe $n(x)$ tel que pour tout $n > n(x)$, x n'est pas partout norme locale en dehors de p dans k_n/k ; $n(x)$ dépend simplement de la décomposition de (x) en produit d'idéaux premiers et de leurs degrés résiduels dans k_∞/k. Pour $n > n(x)$ on ne peut donc pas appliquer de formule du produit sur les p-places.

(ii) Le cadre de la conjecture de Greenberg et l'introduction de la filtration des groupes de classes $\mathcal{C}\ell_{k_n}$ mettra en jeu des groupes $\Lambda^n = \{x \in k^\times,\ \ (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}^n)\}$ et le calcul de $(\Lambda^n : \Lambda^n \cap \mathrm{N}_{k_n/k}(k_n^\times))$, où $\mathrm{N}_{k_n/k}(\mathcal{I}^n) = \langle \mathrm{N}_{k_n/k}(\mathfrak{A}^1), \ldots, \mathrm{N}_{k_n/k}(\mathfrak{A}^r)\rangle_\mathbb{Z}$, où les idéaux $\mathfrak{A}^j$ sont étrangers à p et représentent des classes de k_n annulées par une certaine puissance de $1-\sigma_n$.

Donc Λ^n ne contiendra pas de S_k-unités autres que les unités. Ainsi l'aspect heuristique se ramènera à l'étude des $x \in \Lambda^n$ et de leurs quotients de Fermat, ce qui constitue une approche différente de la conjecture de Greenberg (cf. Sections 6 et 7).

(iii) On a $\mathrm{N}_{k/\mathbb{Q}}\big(\mathrm{N}_{k_n/k}(\mathfrak{A}^j)\big) = \mathrm{N}_{\mathbb{Q}_n/\mathbb{Q}}\big(\mathrm{N}_{k_n/\mathbb{Q}_n}(\mathfrak{A}^j)\big) = (a)$, où $a > 0$ vérifie $a^{p-1} \equiv 1 \pmod{p^{n+1}}$ (cf. Corollaire 4.5), et par conséquent $(\mathrm{N}_{k/\mathbb{Q}}(x))^{p-1} \equiv 1 \pmod{p^{n+1}}$ pour tout $x \in \Lambda^n$.

5. Aspects numériques – Cas des corps quadratiques réels

Soient $\mathfrak{p}_1$ et $\mathfrak{p}_2$ les deux idéaux premiers de $k = \mathbb{Q}(\sqrt{m})$ au-dessus de p et S_k leur ensemble. Les S_k-unités génératrices modulo les unités sont données par π_1 et sa $\mathbb{Q}$-conjuguée π_2, et sont telles que $(\pi_j) = \mathfrak{p}_j^{h_0}$ où h_0 est un entier divisant le nombre de classes h de k.

Lemme 5.1. *Soit $\alpha \in k^\times$, de conjugués α_1 et α_2, α étranger à p, tel que $(\mathrm{N}_{k/\mathbb{Q}}(\alpha))^{p-1} \equiv 1 \pmod{p^{n+1}}$, $n \geq 1$; alors on a (cf. Définition 4.1) $\delta_{\mathfrak{p}_1}(\alpha) = \delta_{\mathfrak{p}_2}(\alpha)$ ou bien $\delta_{\mathfrak{p}_1}(\alpha) \geq n$ & $\delta_{\mathfrak{p}_2}(\alpha) \geq n$. Alors, si $\alpha^{p-1} \not\equiv 1 \pmod{p^{n+1}}$, on a $\alpha^{p-1} = 1 + p \cdot p^{\delta_p(\alpha)} \cdot \beta$, avec $\delta_p(\alpha) < n$ et β étranger à p.*

Démonstration. On a $\mathrm{N}_{k/\mathbb{Q}}(\alpha)^{p-1} = (\alpha_1 \cdot \alpha_2)^{p-1} \equiv 1 \pmod{p^{n+1}}$; donc :

$$\pi_1^{\delta_{\mathfrak{p}_1}(\alpha)} \cdot \pi_2^{\delta_{\mathfrak{p}_2}(\alpha)} \cdot \beta_1 + \pi_2^{\delta_{\mathfrak{p}_1}(\alpha)} \cdot \pi_1^{\delta_{\mathfrak{p}_2}(\alpha)} \cdot \beta_2 + p^{1+\delta_{\mathfrak{p}_1}(\alpha)+\delta_{\mathfrak{p}_2}(\alpha)} \cdot \beta_1\,\beta_2 \equiv 0 \pmod{p^n};$$

si $\delta_{\mathfrak{p}_1}(\alpha) < n$ ou $\delta_{\mathfrak{p}_2}(\alpha) < n$, il vient nécessairement $\delta_{\mathfrak{p}_1}(\alpha) = \delta_{\mathfrak{p}_2}(\alpha) < n$. □

Remarque 5.2. Dans cette situation pour les corps quadratiques, les $\delta_{\mathfrak{p}}(\alpha)$ seront notés $\delta_p(\alpha)$. Ceci vaut pour un $\alpha \in k^\times$ étranger à p et partout norme locale en dehors de p (i.e., norme d'un idéal de k_n) ; en effet, le conducteur de $\mathbb{Q}_n/\mathbb{Q}$ étant p^{n+1}, on a $\mathrm{N}_{k/\mathbb{Q}}(\alpha)^{p-1} \equiv 1 \pmod{p^{n+1}}$. Pour une unité $\alpha = \varepsilon$ de k, on a (indépendamment de n) $\varepsilon^{p-1} = 1 + p \cdot p^{\delta_p(\varepsilon)} \cdot \beta$, $\delta_p(\varepsilon) \geq 0$, avec β étranger à p.

5.1. **Calcul pratique des symboles normiques des S_k-unités.** Pour le calcul des $\left(\frac{\pi_j\,,k_n/k}{\mathfrak{p}_1}\right)$ et $\left(\frac{\pi_j\,,k_n/k}{\mathfrak{p}_2}\right)$, $j = 1, 2$, on remarque que les π_j sont normes locales en dehors de p et que la formule du produit permet de ne calculer que les $\left(\frac{\pi_j\,,k_n/k}{\mathfrak{p}_1}\right)$ par exemple ; mais l'action de $\mathrm{Gal}(k/\mathbb{Q}) =: \{1, \tau\}$ montre que :

$$\left(\frac{\tau(\pi_j)\,,k_n/k}{\tau(\mathfrak{p}_1)}\right) = \tau\left(\frac{\pi_j\,,k_n/k}{\mathfrak{p}_1}\right)\tau^{-1} = \left(\frac{\pi_j\,,k_n/k}{\mathfrak{p}_1}\right).$$

On est donc ramené au seul calcul de $\left(\frac{\pi_2\,,k_n/k}{\mathfrak{p}_1}\right)$ avec π_2 étranger à $\mathfrak{p}_1$. On a à résoudre le système de congruences définissant un $\mathfrak{p}_1$-associé de $x = \pi_2$ (pour n majorant $\delta_{\mathfrak{p}_1}(\pi_2)$) :

$$\begin{aligned} x' &\equiv \pi_2 \pmod{\mathfrak{p}_1^{n+1}}, \\ x' &\equiv 1 \pmod{\mathfrak{p}_2^{n+1}}, \end{aligned} \tag{7}$$

que l'on peut remplacer, a fortiori, par les congruences :

$$\begin{aligned} x' &\equiv \pi_2 \pmod{\pi_1^{n+1}}, \\ x' &\equiv 1 \pmod{\pi_2^{n+1}}, \end{aligned} \tag{8}$$

On détermine alors une "relation de Bézout" $U_1 \cdot \pi_1^{n+1} + U_2 \cdot \pi_2^{n+1} = 1$, $U_1, U_2 \in Z_{k,(p)}$ (anneau des p-entiers de k), qui conduit à la solution $x' = U_1 \cdot \pi_1^{n+1} + U_2 \cdot \pi_2^{n+1} \cdot \pi_2 \pmod{p^{n+1}}$ pour laquelle on a bien les congruences ci-dessus. L'idéal $\mathfrak{a}_{\mathfrak{p}_1}(x)$ est alors (x') dont on prend la norme dans $k/\mathbb{Q}$ pour trouver $a_{\mathfrak{p}_1}$ définissant le symbole d'Artin pour k_n/k dont on calcule l'ordre dans $(\mathbb{Z}/p^{n+1}\,\mathbb{Z})^\times$ qui est, pour n assez grand, de la forme $p^{n-\delta_{\mathfrak{p}_1}(\pi_2)}$.

Le cas de ε est identique à partir du $\mathfrak{p}_1$-associé $x'' = U_1 \cdot \pi_1^{n+1} + U_2 \cdot \pi_2^{n+1} \cdot \varepsilon \pmod{p^{n+1}}$.

5.2. **Programmes PARI.** Le programme suivant (d'après [P]) fournit les informations : m, h = nombre de classes de k, $\varepsilon = u + v \cdot \sqrt{m}$ = unité fondamentale de k, $u, v \in \mathbb{Z}$ ou $\frac{1}{2}\mathbb{Z}$, $\{\pi_1, \pi_2\}$, $z_1 = p^{-\delta_{\mathfrak{p}_1}(\pi_2)}$ et $z_e = p^{-\delta_p(\varepsilon)}$, et aussi n_1 et n_e qui figurent les symboles de Hasse de π_2 et ε dans $\Omega(k_n/k)$.

La conjecture de Greenberg est vérifiée (cf. Théorème 3.4) dès que $\mathscr{C}\ell_k(S_k) = \mathcal{C}\ell_k$ et que l'un au moins des nombres z_1 ou z_e est égal à 1 (i.e., $\delta_{\mathfrak{p}_1}(\pi_2) = 0$ ou $\delta_p(\varepsilon) = 0$) car alors l'automorphisme correspondant engendre G_n et ceci a lieu pour tout $n > \max(\delta_{\mathfrak{p}_1}(\pi_2), \delta_p(\varepsilon))$ (si ceci a lieu pour z_e, c'est que le régulateur normalisé $R_k \sim \frac{1}{p}\log(\varepsilon)$, est égal à 1). En pratique le programme utilise un n_0 de l'ordre de 8 qui suffit largement dans tous les résultats numériques obtenus pour avoir les valeurs exactes de z_1 et z_e, mais d'après la Proposition 4.6, il suffit de prendre $n_0 = 1$ (donc des calculs modulo p^2 seulement) pour obtenir tous les cas où le test est positif.

Les mentions "PROBLÈME-NORMIQUE" (resp. "PROBLÈME-CLASSES") indiquent que $z_1 \geq 1$ et $z_e \geq 1$ (resp. que S_k n'engendre pas le p-groupe des classes de k).

```
{m = 10^4; p = 11; n0 = 8; n = n0 + 1;
while(m < 10^4 + 10^3, m = m + 1; if(core(m) == m&kronecker(m, p) == 1,
y = x; Q = x^2 - m; K = bnfinit(Q, 1); M = m; q = Mod(m, 4); if(q! = 1, M = 4 * m);
E = quadunit(M); h = qfbclassno(M); e1 = component(E, 2); e2 = component(E, 3);
if(q == 1, e2 = e2/2; e1 = e1 + e2); E = e1 + e2 * x;
D = divisors(h); nh = numdiv(h); for(k = 1, nh, d = component(D, k);
Sm = bnfisintnorm(K, -p^d); Sp = bnfisintnorm(K, p^d);
if(component(matsize(Sm), 2) > 1, pi1 = component(Sm, 1); k = nh);
if(component(matsize(Sp), 2) > 1, pi1 = component(Sp, 1); k = nh); h0 = d);
delta = valuation(h, p) - valuation(h0, p); pi2 = -component(pi1, 1) + component(pi1, 2) * x;
print(""); print("m = ", m, "h = ", h, "E = ", E); print("p = ", p, "S = ", pi1, "", pi2);
Pi1 = pi1^n; Pi2 = pi2^n; Z = bezout(Pi1, Pi2); U1 = component(Z, 1); U2 = component(Z, 2);
P = y^2 - Mod(m, p^n); Y = Mod(y, P); x = Y; A1 = eval(U1); A2 = eval(U2);
B1 = eval(Pi1); B2 = eval(Pi2); b1 = eval(pi1); b2 = eval(pi2); e = eval(E);
XP1 = Mod(A1 * B1 + A2 * B2 * b2, P); XPe = Mod(A1 * B1 + A2 * B2 * e, P);
n1 = norm(XP1)^(p-1); ne = norm(XPe)^(p-1); z1 = znorder(n1)/p^n0; ze = znorder(ne)/p^n0;
if(z1 + ze < 1, print("PROBLEME - NORMIQUE"));
if(delta! = 0, print("PROBLEME - CLASSES")); print(z1, "", ze); x = y))}
```

On pourrait en déduire un programme plus court ne calculant que $\delta_{\mathfrak{p}_1}(\pi_2)$ et $\delta_p(\varepsilon)$.

Donnons l'extrait suivant pour $30007 \leq m \leq 30097$, $m \equiv 1 \pmod 3$, et $p = 3$ (la dernière colonne donne la structure du 3-groupe des classes du premier étage k_1) :

m	h	z_1	z_e	structure	m	h	z_1	z_e	structure
30001	1	1	1	1	30055	2	1/27	1/27	$\mathbb{Z}/3\mathbb{Z}$
30007	2	1/9	1/3	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	30058	4	1	1	1
30010	8	1	1	1	30061	1	1	1	1
30013	1	1/3	1	1	30067	2	1	1	1
30019	4	1	1/3	$\mathbb{Z}/3\mathbb{Z}$	30070	4	1	1/3	$\mathbb{Z}/3\mathbb{Z}$
30022	4	1/3	1	1	30073	4	1	1/27	$\mathbb{Z}/3\mathbb{Z}$
30031	2	1/3	1/3	$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	30079	2	1	1	1
30034	2	1	1	1	30085	2	1/3	1	1
30043	18	1	1	$\mathbb{Z}/9\mathbb{Z}$	30091	1	1	1	1
30046	2	1	1	1	30094	8	1	1/3	$\mathbb{Z}/3\mathbb{Z}$
30049	1	1	1/3	$\mathbb{Z}/3\mathbb{Z}$	30097	1	1	1	1

Si le nombre de classes est divisible par p, il faut vérifier si le p-groupe des classes de k est engendré par les idéaux premiers au-dessus de p, sinon la conclusion n'est pas valable. Pour cela le programme retient l'ordre h_0 de la classe de $\mathfrak{p}_1$ pour lequel $\mathfrak{p}_1^{h_0} = (\pi_1)$; si les valuations p-adiques de h_0 et de $h = \#\mathcal{C}\ell_k$ sont égales, ceci veut dire que $\mathcal{C}\ell_k$ est cyclique et engendré par la p-classe de $\mathfrak{p}_1$.

Par exemple, dans le cas de $m = 30043$ où $h = 18$, la S_k-unité génératrice est $317 + 2 \cdot \sqrt{m}$, de norme 3^9, et par conséquent la classe de $\mathfrak{p}_1$, d'ordre 9, est génératrice de $\mathcal{C}\ell_k$.

La méthode est extrêmement simple et le programme très rapide pour n'importe quel p ; pour les 22794 valeurs de m inférieures à 10^5, on a 19993 valeurs pour lesquelles on peut conclure que $\lambda_3 = \mu_3 = 0$. Mais dès que p est un peu grand le test est presque toujours positif et montre que $\lambda_p = \mu_p = 0$.

Pour chaque p, $3 \le p \le 541$, on obtient le tableau suivant selon le programme de comptage ci-après indiquant successivement le nombre C_1 de $m \le 10^4$ (tels que p soit décomposé dans $k = \mathbb{Q}(\sqrt{m})$), le nombre C_2 de cas donnant $\lambda_p = \mu_p = 0$, et $C_1 - C_2$ (cas non résolus) :

p	C_1	C_2	$C_1 - C_2$	p	C_1	C_2	$C_1 - C_2$
3	2279	2042	237	67	2993	2993	0
5	2534	2459	75	71	2994	2994	0
7	2660	2599	61	73	3001	3001	0
11	2781	2759	22	79	3001	3000	1
13	2822	2808	14	83	3002	3002	0
17	2873	2860	13	89	3008	3007	1
19	2886	2877	9	97	3011	3011	0
23	2908	2904	4	101	3010	3009	1
29	2936	2931	5	103	3005	3004	1
31	2944	2939	5	...	...	...	...
37	2960	2958	2	149	3020	3019	1
41	2968	2967	1	...	...	...	...
43	2971	2971	0	193	3023	3022	1
47	2971	2971	0	197	3029	3028	1
53	2983	2982	1	...	...	...	...
59	2986	2984	2	211	3027	3026	1
61	2988	2988	0	...	...	...	...

Les nombres premiers p, $223 \le p \le 541$, absents du tableau, donnent $\lambda_p = \mu_p = 0$ pour tous les $m \le 10^4$ tels que p soit décomposé dans $\mathbb{Q}(\sqrt{m})$.

```
{for(j=2,100,C1=0;C2=0;m=1;p=prime(j);n0=1;n=n0+1;
while(m<10^4,m=m+1;if(core(m)==m&kronecker(m,p)==1,C1=C1+1;
y=x;Q=x^2-m;K=bnfinit(Q,1);
M=m;q=Mod(m,4);if(q!=1,M=4*m);E=quadunit(M);h=qfbclassno(M);
e1=component(E,2);e2=component(E,3);if(q==1,e2=e2/2;e1=e1+e2);E=e1+e2*x;
D=divisors(h);nh=numdiv(h);for(k=1,nh,d=component(D,k);
Sm=bnfisintnorm(K,-p^d);Sp=bnfisintnorm(K,p^d);
if(component(matsize(Sm),2)>1,pi1=component(Sm,1);k=nh);
if(component(matsize(Sp),2)>1,pi1=component(Sp,1);k=nh);h0=d);
delta=valuation(h,p)-valuation(h0,p);pi2=-component(pi1,1)+component(pi1,2)*x;
Pi1=pi1^n;Pi2=pi2^n;Z=bezout(Pi1,Pi2);U1=component(Z,1);U2=component(Z,2);
P=y^2-Mod(m,p^n);Y=Mod(y,P);x=Y;A1=eval(U1);A2=eval(U2);
B1=eval(Pi1);B2=eval(Pi2);b1=eval(pi1);b2=eval(pi2);e=eval(E);
XP1=Mod(A1*B1+A2*B2*b2,P);XPe=Mod(A1*B1+A2*B2*e,P);
n1=norm(XP1)^(p-1);ne=norm(XPe)^(p-1);z1=znorder(n1)/p^n0;ze=znorder(ne)/p^n0;
if(z1+ze>1&delta==0,C2=C2+1);x=y));print(C1,"",C2))}
```

Dans [Su] il y a deux exemples plus délicats (pour $p = 3$) :

(i) $m = 2659$, $h = 3$, $\varepsilon = 63190881 \cdot \sqrt{m} + 3258468890$, $\pi_1 = -2\sqrt{m} + 103$ qui dans notre table est indiqué avec $z_1 = \frac{1}{3}$ et $z_e = \frac{1}{3^2}$ (mais $\mathcal{C}\ell_k$ est engendré par S_k). Il faut alors d'autres calculs explicites dans la tour pour démontrer que $\lambda_3 = \mu_3 = 0$ (cf. [FuTa1], [FuKo], [KS], [IS1], [IS2] utilisant les unités cyclotomiques).

(ii) $m = 12007$, $h = 3$, $\varepsilon = 65199591367431507 \cdot \sqrt{m} + 7144340241111277688$, $p = 3$, $\pi_1 = 429331 \cdot \sqrt{m} + 47044570$, avec $z_1 = \frac{1}{3^6}$ et $z_e = \frac{1}{3^2}$ ($\mathcal{C}\ell_k$ est engendré par S_k). Dans ce cas, la vérification utilise les fonctions L p-adiques, de nombreux arguments et aussi [IS1], [IS2].

Voir d'autres calculs dans [BJ], [CN], [Fu1], [FuKo], [FuTa1], [FuTa2], [I], [KS], [LMN], [Ni] (cas $p = 2$), [Ta1], [Ta2] (pour des corps cubiques totalement réels et $p = 3$), et bien d'autres. Pour une table plus complète ($p = 3, 5, 7, 11, 13, 17, 19$), prière de se connecter à :

https://www.dropbox.com/s/8wgjdkbm1m04xu4/R%C3%A9sultat%20de%20Terminal-GC.txt?dl=0

Il y a identité des valeurs de $\delta_{\mathfrak{p}_1}(\pi_2)$ et $\delta_p(\varepsilon)$, pour $p=3$, avec celles de la table de [FuTa1].

Pour une table plus importante (mais avec $n_0=1$), utiliser :

https://www.dropbox.com/s/tcqfp41plzl3u60/R%C3%A9sultat%20de%20Terminal-GC-II.txt?dl=0

Le programme suivant calcule la structure des groupes des classes de k (dans h_m) et de k_1 pour $p=3$; les bornes b et B de l'intervalle $[b,B]$ des m testés peut être choisie quelconque car le programme n'utilise que les $m\equiv 1 \pmod 3$ de cet intervalle :

$\{b=10^6; B=10^3; b=b-component(Mod(b,3),2)+1; m=b;$
$while(m<b+B, m=m+3; if(core(m)==m, K=bnfinit(x^2-m,1); hm=bnrinit(K,1);$
$hm=component(hm,5); R=component(polcompositum(x^3-3*x+1,x^2-m),1);$
$H=bnrinit(bnfinit(R,1),1); F=component(H,5); G=component(F,1);$
$print("m=",m,"hm=",hm,"structure=",F)))\}$

Ce qui donne les quelques exemples suivants (sous la forme $[\#\mathcal{C}\ell_k, [\text{structure}]]$) :

m	$\mathcal{C}\ell_k$	$\mathcal{C}\ell_{k_1}$	m	$\mathcal{C}\ell_k$	$\mathcal{C}\ell_{k_1}$
1000003	[3, [3]]	[27, [3, 3, 3]]	1000126	[2, [2]]	[24, [6, 2, 2]]
1000018	[4, [4]]	[12, [12]]	1000135	[4, [2, 2]]	[12, [6, 2]]
1000042	[36, [18, 2]]	[36, [18, 2]]	1000147	[30, [30]]	[90, [30, 3]]
1000051	[4, [2, 2]]	[12, [6, 2]]	1000159	[1]	[3, [3]]
1000093	[12, [6, 2]]	[48, [6, 2, 2, 2]]	1000177	[1]	[12, [6, 2]]
1000099	[1]	[3, [3]]	1000189	[1]	[9, [3, 3]]
1000102	[2, [2]]	[18, [6, 3]]	1000198	[12, [12]]	[36, [36]]

6. Filtration des $\mathcal{C}\ell_{k_n}$ – Etude quantitative

On revient au cas général d'un corps de nombres Galoisien réel k de degré d et où $p>2$ est un nombre premier totalement décomposé dans k. On suppose que la conjecture de Leopoldt est vérifiée pour p dans k.

Dans cette section nous reprenons l'analyse de la conjecture de Greenberg sous la forme directe du "calcul" du p-groupe des classes de k_n selon l'algorithme défini dans [Gra4, (2016)], et en utilisant des idéaux étrangers à p pour représenter les classes.

6.1. **Introduction de la filtration de $\mathcal{C}\ell_{k_n}$.** On rappelle que si l'on pose pour simplifier $M^n:=\mathcal{C}\ell_{k_n}$, $k_n\subset k_\infty$ de degré p^n sur k et de groupe de Galois $G_n=:\langle\sigma_n\rangle$, il existe une filtration ainsi définie :

Définition 6.1. *Pour n fixé, soit $(M_i^n)_{i\geq 0}$ la i-suite croissante de sous-G_n-modules de M^n définie (avec $M_0^n:=1$) par $M_{i+1}^n/M_i^n:=(M^n/M_i^n)^{G_n}$, pour $0\leq i\leq m_n-1$, où m_n est le plus petit entier i tel que $M_i^n=M^n$ (i.e., $M^n=M_{m_n}^n$).*

Remarques 6.2. (i) Pour $i=0$, on obtient $M_1^n=(M^n)^{G_n}$.

(ii) On a $M_{i+1}^n=\{h\in M^n,\ h^{1-\sigma_n}\in M_i^n\}$. Ainsi $M_i^n=\{h\in M^n,\ h^{(1-\sigma_n)^i}=1\}$, et $(1-\sigma_n)^{m_n}\in\mathbb{Z}_p[G_n]$ est contenu dans l'annulateur de M^n.

(iii) Pour n fixé, la i-suite des $\#(M_{i+1}^n/M_i^n)$, $0\leq i\leq m_n-1$, est majorée par $\#M_1^n$ et décroissante vers 1 en raison des injections

$$M_{i+1}^n/M_i^n\hookrightarrow M_i^n/M_{i-1}^n\hookrightarrow\cdots\hookrightarrow M_2^n/M_1^n\hookrightarrow M_1^n$$

définies par l'opération de $1-\sigma_n$.

Ensuite, pour les sous-G_n-modules $M_i^n=:\mathcal{A}_{k_n}(\mathcal{I}_i^n)$ de M^n, on a la formule générale (Théorème 3.1) qui devient dans notre cas particulier :

$$\#\big(M_{i+1}^n/M_i^n\big)=\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)}\cdot\frac{p^{n\cdot(d-1)}}{(\Lambda_i^n:\Lambda_i^n\cap\mathrm{N}_{k_n/k}(k_n^\times))},\tag{9}$$

où $\Lambda_i^n := \{x \in k^\times,\ (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)\}$ qui contient E_k, et tout $x_i \in \Lambda_i^n$ est norme locale en dehors de p dans k_n/k. On a alors :

$$\#M^n = \prod_{i=0}^{m_n-1} \#\big(M_{i+1}^n/M_i^n\big). \tag{10}$$

Ainsi, dans cette filtration (n fixé), les M_i^n et $\mathrm{N}_{k_n/k}(M_i^n)$ définissent des i-suites *croissantes* de sous-groupes de $\mathcal{C}\ell_{k_n}$ et $\mathcal{C}\ell_k$ respectivement ; donc $M_{m_n}^n = \mathcal{C}\ell_{k_n}$ et $\mathrm{N}_{k_n/k}(M_{m_n}^n) = \mathcal{C}\ell_k$.

On obtient alors que, pour n fixé, les entiers $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))}$, $i \geq 0$, forment une i-suite *décroissante* de diviseurs du régulateur R_k pour $n \geq e$ (Théorème 4.9 (iii)), en raison des injections :

$$E_k/E_k \cap \mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \cdots \hookrightarrow \Lambda_i^n/\Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \Lambda_{i+1}^n/\Lambda_{i+1}^n \cap \mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \cdots$$

Par conséquent, on a au rang final $i = m_n$, en utilisant ce qui précède pour $M_{m_n}^n = \mathcal{C}\ell_{k_n}$:

$$(\Lambda_{m_n}^n : \Lambda_{m_n}^n \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)} \quad \& \quad \mathrm{N}_{k_n/k}\big(M_{m_n}^n\big) = \mathcal{C}\ell_k,$$

ce qui explique que $\#\mathcal{C}\ell_{k_n}$ dépend essentiellement du nombre de pas m_n, car dès qu'un $x \in \Lambda_{i+1}^n$ se rajoute aux éléments de Λ_i^n, ses $\delta_{\mathfrak{p}}(x)$, $\mathfrak{p} \mid p$, ont une grande probabilité d'être nuls ou au moins inférieurs aux précédents, ce qui donne la i-suite croissante des indices $(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))$ (cf. Section 7 pour une approche heuristique).

Remarque 6.3. D'après le Théorème 2.1 de Greenberg, on a $\lambda = \mu = 0$ si et seulement si $\mathcal{C}\ell_{k_n}^{G_n} = c\ell_{k_n}(S_{k_n})$ pour tout n assez grand. Si cette condition est vérifiée, alors nécessairement $(M^n/M_1^n)^{G_n} = (M^n/c\ell_{k_n}(S_{k_n}))^{G_n}$, ce qui s'écrit $M_2^n/M_1^n = \mathcal{C}\ell_{k_n}^{S_{k_n}G_n}$. En particulier, M_1^n est d'ordre égal à $\#\mathcal{T}_k$ (Théorème 4.7), ce qui conduit à $\#\mathcal{C}\ell_{k_n} \geq M_2^n = \#\mathcal{T}_k \cdot \#\mathcal{C}\ell_{k_n}^{S_{k_n}G_n}$. On a $\omega_n(E_k^{S_k}) = (E_k^{S_k} : E_k^{S_k} \cap \mathrm{N}_{k_n/k}(k_n^\times))$ et $\omega_n(E_k) = (E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))$, où ω_n est l'application qui à $x \in k^\times$ associe la famille des symboles de Hasse dans k_n/k, et on obtient :

$$\#\mathcal{C}\ell_{k_n} \geq \#\mathcal{T}_k \times \frac{\#\mathcal{T}_k}{\#c\ell_k(S_k) \cdot (\omega_n(E_k^{S_k}) : \omega_n(E_k))}.$$

Le second facteur est entier et se calcule explicitement à partir de $\#\mathcal{C}\ell_k$, du régulateur normalisé R_k, $\#\mathcal{T}_k = \#\mathcal{C}\ell_k \cdot R_k$, et $\big(\omega_n(E_k^{S_k}) : \omega_n(E_k)\big)$ se calcule en fonction des entiers $\delta_{\mathfrak{p}}(\eta)$ des S_k-unités η de k.

Théorème 6.4. *Soit k un corps de nombres Galoisien réel de degré d dans lequel p est totalement décomposé. On suppose que la conjecture de Leopoldt est vraie pour p dans k. Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale H_k^{pr} de k (cf. §4.3).*
On a, en termes d'invariants d'Iwasawa $\lambda \geq 0$, $\mu \geq 0$, $\nu \in \mathbb{Z}$, les propriétés suivantes :
(i) On a les inégalités $m_n \leq \lambda \cdot n + \mu \cdot p^n + \nu \leq v_p(\#\mathcal{T}_k) \cdot m_n$, pour tout $n \geq n_0$, où n_0 est un rang à partir duquel la formule d'Iwasawa est valable.
(ii) Si $\mathcal{T}_k = 1$, alors $\lambda = \mu = \nu = 0$, sinon les inégalités du (i) se traduisent par :

$$m_n = c(n) \cdot (\lambda \cdot n + \mu \cdot p^n + \nu), \quad \tfrac{1}{v_p(\#\mathcal{T}_k)} \leq c(n) \leq 1,$$

avec en particulier l'inégalité essentielle $m_n \geq \frac{1}{v_p(\#\mathcal{T}_k)}\,(\lambda \cdot n + \mu \cdot p^n + \nu)$.

Démonstration. On a $\#\mathcal{C}\ell_{k_n} = p^{\lambda\cdot n+\mu\cdot p^n+\nu}$. Comme $\#\big(M_{i+1}^n/M_i^n\big) \geq p$ pour $0 \leq i \leq m_n - 1$, soit $\#\mathcal{C}\ell_{k_n} \geq p^{m_n}$ en utilisant (10), on en déduit l'inégalité $m_n \leq \lambda \cdot n + \mu \cdot p^n + \nu$; ensuite, d'après (9) et le Théorème 4.9, on a pour $0 \leq i \leq m_n - 1$, $\#\big(M_{i+1}^n/M_i^n\big) \leq \#\mathcal{T}_k$; d'où $\#\mathcal{C}\ell_{k_n} \leq (\#\mathcal{T}_k)^{m_n}$, ce qui achève la démonstration. □

Une heuristique raisonnable est que m_n reste, pour tout n, d'une valeur moyenne fonction de $\mathrm{Gal}(k/\mathbb{Q})$ et du groupe de torsion $\mathcal{T}_k$ et non de n. Si cela pouvait être prouvé, on en déduirait $\lambda = \mu = 0$. Or, pour tout n assez grand, les $\#\big(M_{i+1}^n/M_i^n\big)$ forment, à partir de $\#M_1^n$, une i-suite *décroissante* d'entiers divisant $\#\mathcal{T}_k$; une telle suite ne peut avoir, pour λ ou μ non nuls, au moins $\frac{1}{v_p(\#\mathcal{T}_k)}\,(\lambda\cdot n+\mu\cdot p^n+\nu)$ termes non triviaux sauf à établir un lien de type particulier avec les normes d'idéaux $\mathfrak{A}_i \in \mathcal{I}_i^n$ utilisés dans la tour, ce qui philosophiquement semble exclu, à notre avis, car ceci implique l'existence d'au moins un diviseur t^n de $\#\mathcal{T}_k$ tel que $\#\big(M_{i+1}^n/M_i^n\big) = t^n$ pour $O(1)\cdot(\lambda\cdot n+\mu\cdot p^n+\nu)$ valeurs *consécutives* de $i \in [0, m_n]$. Nous examinerons cet aspect dans les §§ 6.3, 6.5, et dans la Section 7.

A cet effet, rappelons l'algorithme qui permet de passer de Λ_i^n à Λ_{i+1}^n, et qui détermine le nombre de pas m_n, pour analyser les phénomènes en jeu.

6.2. **Algorithme de calcul des Λ_i.** On omet l'indice n qui est fixé et on se place dans l'extension $K \subset k_\infty$ de degré p^n et de groupe de Galois $G =: \langle\sigma\rangle$ d'ordre p^n.

On désigne pour simplifier par N la norme arithmétique $\mathrm{N}_{K/k}$ et on pose $M := \mathcal{C}\ell_K$.

(i) Pour le calcul de $M_1 = M^G$ à partir de $M_0 = 1$ et $\mathcal{I}_0 = 1$, on a la formule des classes ambiges $\#M_1 = \#\mathcal{C}\ell_k \cdot \dfrac{p^{n\cdot(d-1)}}{(\Lambda_0 : \Lambda_0 \cap \mathrm{N}(K^\times))}$ avec $\Lambda_0 = \{x_0 \in k^\times,\ (x_0) \in \mathrm{N}(1)\} = E_k$.

On considère les $x_0 \in \Lambda_0$ qui sont normes d'un élément $y_1 \in K^\times$. Donc $(x_0) = \mathrm{N}(y_1) = (1)$, ce qui conduit à l'existence de $\mathfrak{A}_1 \in I_K$ tel que $\mathfrak{A}_1^{1-\sigma} = (y_1)$, où $\mathfrak{A}_1$ est défini à un idéal invariant près ; donc ici, puisque les idéaux premiers au-dessus de p sont invariants, on peut prendre $\mathfrak{A}_1$ étranger à p. On a $\mathcal{C}\ell_K(\mathfrak{A}_1) \in M_1$.

Réciproquement, si $\mathcal{C}\ell_K(\mathfrak{A}_1') \in M_1$, $\mathfrak{A}_1'$ choisi étranger à p dans sa classe, il existe $y_1' \in K^\times$ tel que ${\mathfrak{A}_1'}^{1-\sigma} = (y_1')$, donnant $\mathrm{N}(y_1') = x_0' \in \Lambda_0 \cap \mathrm{N}(K^\times)$. Ainsi y_1' est étranger à p.

Les classes de ces idéaux $\mathfrak{A}_1$ engendrent M_1 et on pose :

$$\mathcal{I}_1 = \langle \mathfrak{A}_1^1, \ldots, \mathfrak{A}_1^{r_1}\rangle.$$

Ceci suppose que l'on a résolu suffisamment d'équations normes. Par exemple, le cas $x_0 = y_1 = 1$ conduit normalement à inclure dans $\mathcal{I}_1$ des idéaux ambiges représentant les classes de k et les idéaux $\mathfrak{P}$ de K au-dessus de p ; en effet, $\mathfrak{A}_1$ est défini à un idéal invariant près, ce qui peut changer la classe car $\mathfrak{A}_1$ peut être principal et non $\mathfrak{A}_1 \cdot \mathfrak{P}$; mais on peut toujours représenter la classe de $\mathfrak{P}$ par un idéal $\mathfrak{B}$ de K étranger à p.

On obtient $\mathrm{N}(M_1)$ comme sous-groupe de $\mathcal{C}\ell_k$, à partir de $\mathrm{N}(\mathcal{I}_1) = \langle \mathrm{N}(\mathfrak{A}_1^1), \ldots, \mathrm{N}(\mathfrak{A}_1^{r_1})\rangle$; alors il vient $\Lambda_1 = \{x_1 \in k^\times,\ (x_1) \in \mathrm{N}(\mathcal{I}_1)\}$ et, toujours au niveau n fixé :

$$\#(M_2/M_1) = \frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}(M_1)} \times \frac{p^{n\cdot(d-1)}}{(\Lambda_1 : \Lambda_1 \cap \mathrm{N}(K^\times))}.$$

On vérifie qu'en dépit de la non unicité de $\mathcal{I}_1$, le groupe Λ_1 est unique modulo $\mathrm{N}(K^\times)$.

(ii) Pour le calcul de $\mathcal{I}_2$, on considère les éléments x_1 de Λ_1 qui sont normes d'un $y_2 \in K^\times$; alors $(x_1) = \mathrm{N}(y_2) = \mathrm{N}(\mathfrak{B}_1)$, $\mathfrak{B}_1 \in \mathcal{I}_1$, donc il existe $\mathfrak{A}_2 \in I_K$ tel que $\mathfrak{A}_2^{1-\sigma} \cdot \mathfrak{B}_1 = (y_2)$, avec $\mathfrak{A}_2$ choisi étranger à p. On a $\mathcal{C}\ell_K(\mathfrak{A}_2)^{1-\sigma} \in M_1$.

Inversement, si $\mathcal{C}\ell_K(\mathfrak{A}_2') \in M_2$, $\mathfrak{A}_2'$ étranger à p, il existe $y_2' \in K^\times$ tel que ${\mathfrak{A}'}_2^{1-\sigma} \cdot \mathfrak{B}_1' = (y_2')$, avec $\mathfrak{B}_1' \in \mathcal{I}_1$, d'où $\mathrm{N}(\mathfrak{B}_1') = \mathrm{N}(y_2') =: (x_1')$, $x_1' \in \Lambda_1 \cap \mathrm{N}(K^\times)$.

Ces idéaux de la forme $\mathfrak{A}_2^1, \ldots, \mathfrak{A}_2^{r_2}$, sont ajoutés à $\mathcal{I}_1$ (puisque $M_2 \supseteq M_1$) pour former :

$$\mathcal{I}_2 = \langle \mathfrak{A}_1^1, \ldots, \mathfrak{A}_1^{r_1}\ ;\ \mathfrak{A}_2^1, \ldots, \mathfrak{A}_2^{r_2}\rangle,$$

d'où $\mathrm{N}(M_2)$ et $\Lambda_2 = \{x_2 \in k^\times,\ (x_2) \in \mathrm{N}(\mathcal{I}_2)\}$, etc.

On obtient donc des groupes Λ_i, étrangers à p, uniques modulo $\mathrm{N}(K^\times)$, tels que :

$$E_k \subseteq \Lambda_1 \subseteq \cdots \subseteq \Lambda_i \subseteq \ldots.$$

On suppose implicitement que chaque $\mathcal{I}_i$ est constitué d'idéaux étrangers à p.

Cette description n'a pas lieu d'être effective dans la tour k_∞, mais elle montre comment se déterminent les éléments x_i des Λ_i dont on rappelle que tout repose sur leurs "$\mathfrak{p}$-quotients de Fermat", $\mathfrak{p} \mid p$, à partir de l'écriture $x_i^{p-1} = 1 + p \cdot \beta(x_i)$, conduisant à $\delta_\mathfrak{p}(x_i) = v_\mathfrak{p}(\beta(x_i)) \geq 0$. Compte tenu du fait que $E_k \subseteq \Lambda_i$, les $\delta_\mathfrak{p}(x_i)$ sont définis modulo $\delta_\mathfrak{p}(E_k)$.

Une heuristique classique est que, pour $\mathfrak{p}$ fixé, les $\delta_\mathfrak{p}(x)$, $x \in k^\times$, sont aléatoires, indépendants, donnant ainsi une heuristique, de type Borel–Cantelli lorsque $n \to \infty$, "justifiant" très facilement la conjecture de Greenberg. Cependant, il est nécessaire de préciser la nature et l'indépendance des idéaux $\mathfrak{A}_i$ de k_n constituant les groupes $\mathcal{I}_i^n$ pour lesquels $\mathrm{N}_{k_n/k}(\mathcal{I}_i)$ conduit aux nombres x_i. Nous montrerons dans la Section 7 qu'il en est bien ainsi d'un point de vue heuristique en utilisant des programmes établissant des statistiques très convaincantes.

En effet, si, comme nous l'avons observé dans [Gra6], les $\delta_\mathfrak{p}(x_i)$ sont nuls avec une probabilité de l'ordre de $\frac{1}{p}$, ceci rend le facteur $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ égal à 1 très rapidement, c'est-à-dire m_n borné, mais ici, contrairement au cas général, les x_i sont soumis à certaines conditions (normes locales en dehors de p) et dépendant fortement de n. Pour cela examinons le cas non trivial le plus simple possible ci-après en supposant la conjecture fausse.

6.3. **Analyse de la i-suite des groupes Λ_i^n sous l'hypothèse $\mathcal{C}\ell_k = 1$ & $\lambda \geq 1$.** Pour fixer les idées, supposons que k est un corps quadratique réel, que $p > 2$ est décomposé, que $\#\mathcal{C}\ell_k = 1$, que $\delta_p(\varepsilon) \geq 1$, et que (en posant pour simplifier $\mathfrak{p}_1 =: \mathfrak{p}$ et $\pi_2 =: \pi$) on a $\delta_\mathfrak{p}(\pi) = 1$ (cf. § 5.1).

Par exemple, $m = 103$, $\varepsilon = 22419 \cdot \sqrt{103} + 227528$, $\pi = \sqrt{103} + 10$, pour lesquels k est principal, $\delta_p(\varepsilon) = 1$ et $\delta_\mathfrak{p}(\pi) = 1$; ainsi la condition suffisante du Théorème 3.4 n'est pas vérifiée. On a donc $R_k = p$ et la formule du Théorème 4.7.

Soit n fixé pour lequel la formule d'Iwasawa est applicable, posons à nouveau $K := k_n$, $M := \mathcal{C}\ell_K$, et supposons par exemple $\lambda = 1$ (on a $\mu = 0$ et $\nu \in \mathbb{Z}$) ; on a donc au niveau n, $\#M = p^{n+\nu}$ et puisque $\delta_p(\varepsilon) = 1$:

$$\#M_1 = \frac{p^n}{(\Lambda_0 : \Lambda_0 \cap \mathrm{N}_{K/k}(K^\times))} = p,$$

où $\Lambda_0 = E_k$. On a $\mathcal{I}_1 = \langle \mathfrak{A}_1 \rangle$ obtenu de la façon suivante : pour une puissance convenable ε' de l'unité fondamentale ε (de fait, sous l'hypothèse faite, nécessairement $\varepsilon' = \varepsilon^{p^{n-1}}$), on a $\varepsilon' = \mathrm{N}(y_1)$, $y_1 \in K^\times$, d'où $(y_1) = \mathfrak{A}_1^{1-\sigma}$ avec $\mathfrak{A}_1$ convenable étranger à p. La classe de $\mathfrak{A}_1$ est d'ordre p puisque M_1 est d'ordre p.

Posons $\mathfrak{A}_1^p = (z_1)$, $z_1 \in K^\times$, et $\mathrm{N}_{K/k}(\mathfrak{A}_1) = (\alpha_1)$, $\alpha_1 \in k^\times$; on obtient $\alpha_1^p = \mathrm{N}_{K/k}(z_1) \cdot \eta_1$ où η_1 est une unité de k.

Soit alors $\omega = \omega_n$ l'application qui à $x \in k^\times$ associe dans $\Omega(K/k) \simeq \mathbb{Z}/p^n\mathbb{Z}$ la famille des symboles de restes normiques dans K/k. On obtient $\omega(\eta_1) = \omega(\alpha_1^p) = \omega(\alpha_1)^p \in \Omega(K/k)^p$; or, en raison de l'hypothèse $\delta_p(\varepsilon) = 1$, on a $\omega(\eta_1) \in \Omega(K/k)^p$, et par conséquent $\omega(\alpha_1)$, donc $\delta_p(\alpha_1)$, peut a priori prendre toute valeur de façon équiprobable dans $\Omega(K/k)$ (sans la condition $\omega(\eta_1) \in \Omega(K/k)^p$, l'algorithme se serait arrêté avant, la relation $\omega(\eta_1) = \omega(\alpha_1^p)$ étant alors absurde). On a donc obtenu $\mathrm{N}_{K/k}(\mathcal{I}_1) = \langle \mathrm{N}_{K/k}(\mathfrak{A}_1) \rangle = \langle (\alpha_1) \rangle$, d'où :

$$\#(M_2/M_1) = \frac{p^n}{(\Lambda_1 : \Lambda_1 \cap \mathrm{N}_{K/k}(K^\times))}, \quad \text{avec } \Lambda_1 = \langle \varepsilon,\, \alpha_1 \rangle.$$

Puisque $\delta_p(\varepsilon) = 1$, l'algoritme ne peut se terminer en donnant $M = M_1$ que si $\delta_p(\alpha_1)$ est nul ; sinon l'algorithme se poursuit, et en supposant $\delta_p(\alpha_1) \geq 1$, il faut prendre un élément convenable de Λ_1, de la forme $\alpha_1^u \cdot \varepsilon^v$, $u, v \in \mathbb{Z}$, comme norme dans K/k et on obtient, puisque $\mathrm{N}_{K/k}(\mathfrak{A}_1) = (\alpha_1)$, une relation de la forme $\mathfrak{A}_2^{1-\sigma} = \mathfrak{A}_1^u\,(y_2)$ dans K pour définir $\mathcal{I}_2$. Mais M_2/M_1 est annulé par p, et en supposant $M_2 \neq M_1$, on aura $\mathfrak{A}_2^p = \mathfrak{A}_1^w \cdot (z_2)$, $w \in \mathbb{Z}$, $z_2 \in K^\times$, d'où $\mathrm{N}_{K/k}(\mathfrak{A}_2^p) = (\alpha_1^w)\,\mathrm{N}_{K/k}(z_2)$ qui conduit, en posant $(\alpha_2) = \mathrm{N}_{K/k}(\mathfrak{A}_2)$, à $\omega(\alpha_2^p) = \omega(\alpha_2)^p = \omega(\alpha_1^w \cdot \eta_2)$ pour une unité η_2 de k (or $\omega(\alpha_1)$ et $\omega(\eta_2)$ sont dans $\Omega(K/k)^p$).

Comme précédemment, $\omega(\alpha_2)$ n'est soumis a priori à aucune obstruction pour conduire éventuellement à $\delta_p(\alpha_2)=0$.

L'algorithme pour k_n se poursuit avec des calculs analogues, pour lesquels on a :

$$(11)\quad \omega(\alpha_1^p)\in\omega(\Lambda_0),\ \omega(\alpha_2^p)\in\omega(\Lambda_1),\dots,\omega(\alpha_{i+1}^p)\in\omega(\Lambda_i),\dots\ \text{ où } \Lambda_i=\langle\varepsilon,\alpha_1,\dots,\alpha_i\rangle.$$

et où l'on sait que les $\#\omega(\Lambda_i)$ forment une suite croissante, ici majorée par p^{n-1} puisque $\#(M_{i+1}/M_i)=\dfrac{p^n}{\#\omega(\Lambda_i)}=p$ pour $0\le i\le m_n-1$, donc stationnaire à la valeur p^{n-1} dès l'indice 0 ; chaque fois la relation $\omega(\alpha_{i+1}^p)\in\omega(\Lambda_i)$ permet, statistiquement, une "décroissance" des $\delta_p(\alpha_i)$, ce qui semble contradictoire avec un nombre de pas m_n tel que $m_n\ge n+\nu$ découlant de l'hypothèse $\lambda=1$, $\mu=0$, $v_p(\#\mathcal{T}_k)=1$ (cf. Théorème 6.4).

Une autre façon d'aborder ces questions heuristiques est la suivante (sous les mêmes hypothèses de travail que ci-dessus) : représentons la classe de $\mathfrak{A}$ dans K par un idéal premier $\mathfrak{L}$ de K ; on a $\mathrm{N}_{K/k}(\mathfrak{L})=\mathfrak{l}^{f^n}=:(\beta)^{f^n}=:(\alpha)$ où $\mathfrak{l}=(\beta)$ est l'idéal premier de k en-dessous de $\mathfrak{L}$ et f^n son degré résiduel dans K/k (autrement dit, $\alpha=\beta^{f^n}\cdot\eta$, $\eta\in E_k$). Or la condition normique $\delta_{\mathfrak{p}}(\alpha)=0$ ne peut avoir lieu que si $f^n=1$ (i.e., $\mathfrak{l}$ totalement décomposé dans K/k), puisque $\delta_{\mathfrak{p}}(\eta)\ge 1$ par hypothèse sur $\delta_{\mathfrak{p}}(\varepsilon)$; ainsi $\delta_{\mathfrak{p}}(\alpha)=0$ implique, pour ℓ en-dessous de $\mathfrak{l}$, $l^{p-1}\equiv 1\pmod{p^{n+1}}$, condition nécessaire très forte pour $n\to\infty$ (mais c'est toujours possible au moyen du théorème de Tchebotarev, cf. Section 7).

Or ceci n'a pas lieu pour $\mathfrak{P}\in S_K$, de degré résiduel 1. Ceci explique en partie la condition nécessaire et suffisante de Greenberg (Théorème 2.1) qui semble la seule "possibilité raisonnable" pour avoir $\mathcal{C}\ell_{k_n}^{G_n}=c\ell_{k_n}(S_{k_n})$ pour tout n assez grand.

On a donc, sous l'hypothèse $\mathcal{C}\ell_k=1$, $R_k=p$, $\lambda=1$, $\#(M_{i+1}/M_i)=p$ pour environ n pas, ce qui est considérable, et on peut même conjecturer que pour n assez grand on a $M=M_{O(1)}$ qui est essentiellement le critère de Greenberg dans notre cas particulier.

Le programme du § 5.2, donne pour $m=103$, $\mathcal{C}\ell_{k_1}\simeq\mathbb{Z}/3\,\mathbb{Z}\oplus\mathbb{Z}/3\,\mathbb{Z}$, ce qui prouve que au premier étage on a un M_2 distinct de M_1, de probabilité $1/3$. Ensuite on obtient $\mathcal{C}\ell_{k_2}\simeq\mathcal{C}\ell_{k_3}\simeq\mathbb{Z}/3\,\mathbb{Z}\oplus\mathbb{Z}/3\,\mathbb{Z}$, qui suppose également $M=M_2\ne M_1$ au second et troisième étage ; il serait utile de savoir si ceci se prolonge indéfiniment et donne l'invariant ν. On peut par des méthodes numériques de type "spiegelungssatz" montrer que $\lambda=0$ (cf. [FuTa1]). Le paragraphe suivant peut permettre d'analyser ce fait.

6.4. **Conséquences locales de la conjecture de Greenberg sur les unités.** Soit n fixé assez grand tel que la formule d'Iwasawa soit applicable, et soit $h\to\infty$. On a, d'après la formule de Chevalley pour $G_{n+h,n}:=\mathrm{Gal}(k_{n+h}/k_n)$, la relation :

$$\#\mathcal{C}\ell_{k_{n+h}}^{G_{n+h,n}}=\#\mathcal{C}\ell_{k_n}\cdot\frac{p^{h\cdot(d-1)}}{(E_{k_n}:E_{k_n}\cap\mathrm{N}_{k_{n+h}/k_n}(k_{n+h}^\times))}\le\#\mathcal{C}\ell_{k_{n+h}}.$$

Si $\lambda=\mu=0$, on a donc $\#\mathcal{C}\ell_{k_{n+h}}=\#\mathcal{C}\ell_{k_n}=p^\nu$, d'où $\dfrac{p^{h\cdot(d-1)}}{(E_{k_n}:E_{k_n}\cap\mathrm{N}_{k_{n+h}/k_n}(k_{n+h}^\times))}=1$, pour tout $h\ge 0$. Soit $\omega_{n+h,n}$ l'application qui à une unité $\varepsilon^n\in E_{k_n}$ associe la famille $\Big(\Big(\dfrac{\varepsilon^n\,,\,k_{n+h}/k_n}{\mathfrak{p}_n}\Big)\Big)_{\mathfrak{p}_n|p}$ dans $\Omega(k_{n+h}/k_n)\simeq\mathbb{Z}/p^{h\cdot(d-1)}\mathbb{Z}$ (cf. § 4.1), alors $\omega_{n+h,n}(E_{k_n})=\Omega(k_{n+h}/k_n)$. Il existe donc des unités $\varepsilon_j^n\in E_{k_n}$, $1\le j\le d-1$, telles que les $d-1$ familles $\Big(\Big(\frac{\varepsilon_j^n\,,k_\infty/k_n}{\mathfrak{p}_n}\Big)\Big)_{\mathfrak{p}_n|p}$ constituent une base topologique, de sorte que :

$$(12)\qquad \Omega(k_\infty/k_n)=\bigoplus_{j=1}^{d-1}\Big\langle\Big(\Big(\frac{\varepsilon_j^n\,,\,k_\infty/k_n}{\mathfrak{p}_n}\Big)\Big)_{\mathfrak{p}_n|p}\Big\rangle\simeq\mathbb{Z}_p^{d-1}.$$

Soit n_0 fixé pour lequel les $\varepsilon_j^{n_0}$ vérifient la relation ci-dessus. Alors on peut prendre $\varepsilon_j^n=\varepsilon_j^{n_0}$ pour tout j et tout $n\ge n_0$; en effet, posons $\varepsilon_j:=\varepsilon_j^{n_0}$ et $F_0:=\bigoplus_{j=1}^{d-1}\langle\varepsilon_j\rangle$. Au niveau n_0,

si $\varepsilon \in F_0$ est norme dans k_{n_0+h}/k_{n_0}, alors $\varepsilon \in F_0^{p^h}$; supposons ε vue dans k_n et norme dans k_{n+h}/k_n, alors en prenant la norme dans k_n/k_{n_0}, on obtient que $\varepsilon^{p^{n-n_0}}$ est norme dans k_{n+h}/k_{n_0} (degré p^{n-n_0+h}), donc $\varepsilon^{p^{n-n_0}} \in F_0^{p^{n-n_0+h}}$, d'où la propriété.
On notera aussi que pour tout $\mathfrak{p}_n \mid p$, $\delta_{\mathfrak{p}}^n(\varepsilon_j) = p^{n-n_0} \cdot \delta_{\mathfrak{p}}^{n_0}(\varepsilon_j) + p^{n-n_0} - 1$, ce qui fait que ces unités sont rapidement des puissances p^N-ièmes locales en p, où N tend vers l'infini avec n.
On a alors, pour tout $n \geq n_0$ et tout $h \geq 0$:

$$E_{k_n}/E_{k_n} \cap \mathrm{N}_{k_{n+h}/k_n}(k_{n+h}^\times) \simeq F_0/F_0^{p^h}, \ \text{ où } \ F_0 = \bigoplus_{j=1}^{d-1} \langle \varepsilon_j \rangle \subseteq E_{k_{n_0}}. \tag{13}$$

Si l'on prend n_0 minimum, on aura $n_0 = 0$ si et seulement si pour les $\mathfrak{p} \mid p$ on a $\delta_{\mathfrak{p}}(\varepsilon_j) = 0$ pour un système fondamental d'unités définissant E_k, soit $R_k = 1$.
Inversement, sous l'existence de F_0 pour un n_0 convenable, on obtient la condition nécessaire à la conjecture de Greenberg, $\dfrac{p^{h\cdot(d-1)}}{(E_{k_n} : E_{k_n} \cap \mathrm{N}_{k_{n+h}/k_n}(k_{n+h}^\times))} = 1$, d'où $\#\mathcal{C}\ell_{k_{n+h}}^{G_{n+h,n}} = \#\mathcal{C}\ell_{k_n}$ pour tout n assez grand.

6.5. **Heuristiques sur les propriétés de la filtration dans k_∞/k.** Ici, contrairement aux études précédentes, on fixe $i \geq 1$ et on considère la n-suite des groupes M_i^n des filtrations des groupes $M^n := \mathcal{C}\ell_{k_n}$ pour $n \longrightarrow \infty$.

6.5.1. *Approche générale.* On considère les quotients $\#\big(M_{i+1}^n/M_i^n\big)$ pour i fixé et $n \to \infty$ et leurs deux facteurs donnés par la formule 9.

Lemme 6.5. *Pour tout $i \geq 0$ fixé, les $\#\big(M_{i+1}^n/M_i^n\big)$ forment une n-suite croissante stationnaire de diviseurs de $\#\mathcal{T}_k$, et les $\#M_i^n$ définissent une n-suite croissante d'entiers, stationnaire à partir d'un rang $e_i \geq e$, où p^e est l'exposant de $U_k^*/\overline{E}_k$.*

Démonstration. On a $\#M_1^n = \#\mathcal{C}\ell_k \cdot \dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}$. Le cas de $\#(M_1^n/M_0^n) = \#M_1^n = \#\mathcal{T}_k$ $(n \geq e)$ est donc clair (Théorème 4.7) et on a $e_1 = e$. Considérons pour $i \geq 0$ fixé la n-suite définie par :

$$\#\big(M_{i+1}^n/M_i^n\big) = \frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} \cdot \frac{p^{n\cdot(d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))},$$

où $\Lambda_i^n = \{x \in k^\times,\ (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)\}$.
Puisque $M_i^n = \{h \in M^n,\ \ h^{(1-\sigma_n)^i} = 1\}$, on a $\mathrm{N}_{k_{n+h}/k_n}(M_i^{n+h}) \subseteq \mathrm{N}_{k_n/k}(M_i^n)$, pour tout $h \geq 0$, et la n-suite d'entiers $\dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} =: p^{h_i^n}$ est *croissante*, donc stationnaire à une valeur notée $p^{h_i^\infty} \mid \#\mathcal{C}\ell_k$, à partir d'un certain rang.
Le second facteur $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))} =: p^{\rho_i^n}$ définit une n-suite *croissante* stationnaire à une valeur notée $p^{\rho_i^\infty} \mid R_k$ (cf. Théorème 4.9 et Remarque 4.10), à partir d'un certain rang, et le premier point du lemme en résulte pour la n-suite $\#\big(M_{i+1}^n/M_i^n\big)$; on a $\lim\limits_{n\to\infty} \#\big(M_{i+1}^n/M_i^n\big) = p^{h_i^\infty} \cdot p^{\rho_i^\infty} \mid \#\mathcal{T}_k$. Enfin si on suppose par récurrence que la n-suite $\#M_i^n$ stationnaire à partir d'un certain rang, la propriété en résulte pour la n-suite M_{i+1}^n. □

On a $e_1 = e \leq e_2 \leq \cdots \leq e_i \leq \cdots$ et la i-suite des $p^{h_i^\infty} \cdot p^{\rho_i^\infty}$ est *décroissante* (cf. Remarque 6.2 (iii)) donc stationnaire, mais non nécessairement de limite 1 ; en effet, on a seulement que $p^{h_i^\infty} \cdot p^{\rho_i^\infty}$ divise $\#\mathcal{T}_k$ et il convient d'examiner chacun des deux facteurs.
On dira que le processus sur i est fini (ce qui équivaut à $\lambda = \mu = 0$) s'il existe $i_0 \in \mathbb{N}$ tel que $p^{h_{i_0}^\infty} \cdot p^{\rho_{i_0}^\infty} = 1$; dans ce cas, pour tout n assez grand, $\#M^n$ est une constante p^ν indépendante de n, et est obtenu au moyen de la filtration au niveau n.

6.5.2. *Comportement heuristique de $\omega_n(\Lambda_i^n) \subseteq \Omega(k_n/k)$, $n \to \infty$.* Dans le cas où par exemple $\mathcal{C}\ell_k = 1$, le processus sur i est infini si et seulement si pour tout i il existe n assez grand tel que $\omega_n(\Lambda_i^n) := \Lambda_i^n/\Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times) \subsetneqq \Omega(k_n/k) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d-1}$ (i.e., $p^{\rho_i^\infty} \neq 1$).
Par conséquent la finitude du processus dans ce cas ne peut provenir que de l'heuristique suivante, en raison des propriétés des quotients de Fermat (voir le § 7.1 qui montre l'indépendance probable de ces propriétés par rapport à n) :

Heuristique 6.6. *On considère les Λ_i^n associés à l'ensemble des algorithmes de détermination des sous-groupes M_i^n, $0 \leq i \leq m_n$, des filtrations des groupes $M^n := \mathcal{C}\ell_{k_n}$, $n \geq 0$.*
Alors il existe i_1 assez grand, indépendant de n, tel que $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_{i_1}^n : \Lambda_{i_1}^n \cap \mathrm{N}_{k_n/k}(k_n^\times))} = 1$ pour $n \to \infty$. On peut remplacer i_1 par une fonction $i_1(n)$ telle que $\frac{i_1(n)}{n} \to 0$ si $n \to \infty$.

Par exemple, dans le cas quadratique p-principal, la finitude du processus est assurée dès que le $\delta_p(x)$ d'un $x \in \Lambda_i^n$ est nul puisqu'alors $\omega_n(x)$ engendre $\Omega(k_n/k)$ (cf. § 6.3).

6.5.3. *Comportement heuristique de $\mathrm{N}_{k_n/k}(M_i^n) \subseteq \mathcal{C}\ell_k$, $n \to \infty$.* Supposons $\mathcal{C}\ell_k \neq 1$; la non finitude du processus sur i (à l'infini) peut provenir du fait que pour tout i il existe n assez grand tel que $\mathrm{N}_{k_n/k}(M_i^n) \subsetneqq \mathcal{C}\ell_k$ (i.e., $p^{h_i^\infty} \neq 1$) où l'on rappelle que $\mathrm{N}_{k_n/k}(\mathcal{I}_i^n)$ permet la poursuite de l'algorithme à partir des $x_i = \mathrm{N}_{k_n/k}(y_i) \in \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times)$ par définition tels que $(x_i) = \mathrm{N}_{k_n/k}(\mathfrak{B}_i)$, $\mathfrak{B}_i \in \mathcal{I}_i^n$, et conduisant à $\mathfrak{A}_{i+1}^{1-\sigma_n} \cdot \mathfrak{B}_i = (y_i)$ pour obtenir la p-classe (a priori aléatoire) de $\mathrm{N}_{k_n/k}(\mathfrak{A}_{i+1}) \in \mathrm{N}_{k_n/k}(\mathcal{I}_{i+1}^n)$ dans k.

On a, pour tout n et tout $h \geq 0$ (i fixé), le diagramme suivant où les normes N_{k_{n+h}/k_n} définies sur M^{n+h} et $(M^{n+h})^{(1-\sigma_{n+h})^i}$ sont surjectives, mais non celle définie sur M_i^{n+h} (qui peut être ni injective ni surjective) :

$$\begin{array}{ccccccccc}
1 & \longrightarrow & M_i^{n+h} & \longrightarrow & M^{n+h} & \xrightarrow{(1-\sigma_{n+h})^i} & (M^{n+h})^{(1-\sigma_{n+h})^i} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{N}_{k_{n+h}/k_n}} & & \downarrow{\scriptstyle \mathrm{N}_{k_{n+h}/k_n}} & & \\
1 & \longrightarrow & M_i^{n} & \longrightarrow & M^{n} & \xrightarrow{(1-\sigma_{n})^i} & (M^{n})^{(1-\sigma_{n})^i} & \longrightarrow & 1\,.
\end{array}$$

On a $\mathrm{N}_{k_{n+h}/k_n}(M_i^{n+h}) \subseteq M_i^n$ et on peut supposer, en modifiant $\mathcal{I}_i^n$ modulo les idéaux principaux, que l'on a $\mathrm{N}_{k_{n+1}/k_n}(\mathcal{I}_i^{n+1}) \subseteq \mathcal{I}_i^n$ et par conséquent que, *pour tout h fixé* :

$$E_k \subseteq \Lambda_i^{n+h} \subseteq \ldots \subseteq \Lambda_i^{n+h-j} \subseteq \ldots \subseteq \Lambda_i^n,$$

mais on ne peut pas définir une n-suite de Λ_i^n (i fixé) décroissante infinie contenant E_k.
On peut appliquer l'Heuristique 6.6 en affirmant qu'il existe i_1 assez grand indépendant de $n \to \infty$ tel que $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_{i_1}^n : \Lambda_{i_1}^n \cap \mathrm{N}_{k_n/k}(k_n^\times))} = 1$, pour tout n assez grand. On considère alors n assez grand tel que la n-suite des $\dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_{i_1}^n)}$ soit constante égale à $p^{h_{i_1}^\infty} \neq 1$; il vient $\#(M_{i+1}^n/M_i^n) = \#(M_{i_1+1}^n/M_{i_1}^n) = p^{h_{i_1}^\infty}$, pour $i_1 \leq i \leq m_n - 1$ (Remarque 6.2 (iii)). Ceci signifie que sous l'hypothèse $\lambda \geq 1$, l'algorithme habituel au niveau n devrait comporter $O(\lambda \cdot n)$ étapes en fonction de la différence $m_n - i_1$ (cf. Théorème 6.4). Or on peut se baser sur l'heuristique naturelle suivante stipulant que les classes des idéaux de k de la forme $\mathrm{N}_{k_n/k}(\mathfrak{A}_i)$ (ou $\mathrm{N}_{k_n/k}(\mathcal{L}_i)$ avec un représentant premier $\mathcal{L}_i$ totalement décomposé dans k_n/k, cf. Section 7.1) sont aléatoires, indépendantes, et se répartissent dans le groupe fini $\mathcal{C}\ell_k$ selon les probabilités standard dans la mesure où $\mathrm{N}_{k_n/k}(\mathcal{C}\ell_{k_n}) = \mathcal{C}\ell_k$:

Heuristique 6.7. *On considère les Λ_i^n associés à l'ensemble des algorithmes de détermination des sous-groupes M_i^n, $0 \leq i \leq m_n$, des filtrations des groupes $M^n := \mathcal{C}\ell_{k_n}$, $n \geq 0$.*
Alors il existe $i_2 \geq i_1$, assez grand, indépendant de n, tel que $\mathrm{N}_{k_n/k}(M_{i_2}^n) = \mathcal{C}\ell_k$ pour $n \to \infty$.
On peut remplacer i_2 par une fonction $i_2(n) \geq i_1(n)$ telle que $\frac{i_2(n)}{n} \to 0$ si $n \to \infty$.

Dans le cas quadratique où l'on suppose par exemple $\#\mathcal{C}\ell_k = p$, la finitude du processus est assurée dès que la classe d'un $\mathfrak{A}_i$ de l'algorithme est non p-principale, ce qui est raisonnable.

On peut proposer le programme suivant, pour $p = 3$ et $n = 1$, lorsque $\#\mathcal{C}\ell_k = p$ et lorsque l'unité fondamentale ε de k est telle que $\delta_p(\varepsilon) = 0$, auquel cas $\omega_n(\Lambda_i^n) = 1$ pour tout i et tout n, et $\#\big(M_{i+1}^n/M_i^n\big) = \dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)}$. On suppose également que $\mathcal{C}\ell_k$ n'est pas engendré par la classe de $\mathfrak{p} \mid p$ (sinon le critère du Théorème 3.4 s'applique trivialement puisqu'alors $\mathcal{C}\ell_k^{S_k} = 1$ et $\omega_1(E_k^{S_k}) = \omega_1(E_k) = p$). On a évidemment $\#\mathcal{C}\ell_{k_1} = p^w$, $w \geq 1$.

$\{p = 3; n = 1; b = 10^3; B = 10^6; Cyclo = polsubcyclo(p^{(n+1)}, p^n);$
$C2 = 0; C3 = 0; C4 = 0; C5 = 0; CM = 0; m = b; while(m < B, m = m + 1;$
$if(core(m) == m\&kronecker(m,p) == 1, Q = x^2 - m; K = bnfinit(Q,1);$
$M = m; t = Mod(m,4); if(t! = 1, M = 4 * m);$
$h = qfbclassno(M); v = valuation(h,p); if(v == 1, T = 0; hh = h/p^v;$
$D = divisors(hh); nh = numdiv(hh); for(k = 1, nh, d = component(D,k);$
$Sm = bnfisintnorm(K, -p^d); Sp = bnfisintnorm(K, p^d);$
$if(component(matsize(Sm),2) > 1, Am = Mod(component(Sm,1), Q);$
$vm = valuation(component(Sm,1),p); if(vm == 0, k = nh; T = 1));$
$if(component(matsize(Sp),2) > 1, Ap = Mod(component(Sp,1), Q);$
$vp = valuation(component(Sp,1),p); if(vp == 0, k = nh; T = 1)));$
$E = quadunit(M); e1 = component(E,2); e2 = component(E,3);$
$if(t == 1, e2 = e2/2; e1 = e1 + e2); E = Mod(e1 + e2 * x, Q;);$
$EE = component(E^{(p-1)} - 1, 2); vale = valuation(EE,p) - 1;$
$if(vale == 0\&T == 1, CM = CM + 1; P = polcompositum(Cyclo, Q);$
$R = component(P,1); KK = bnfinit(R,1); HH = bnrinit(KK,1);$
$H = component(component(HH,5),1); w = valuation(H,p);$
$if(w == 2, C2 = C2 + 1); if(w == 3, C3 = C3 + 1);$
$if(w == 4, C4 = C4 + 1); if(w >= 5, C5 = C5 + 1);$
$print(m,"",CM,"",C2,"",C3,"",C4,"",C5);))));$
$print(C2/CM + 0.0,"",C3/CM + 0.0,"",C4/CM + 0.0,"",C5/CM + 0.0);$
$S = 1 - (p^2 - 1.0)/p^2 - (p^2 - 1.0)/p^4 - (p^2 - 1.0)/p^6 - (p^2 - 1.0)/p^8;$
$print((p^2 - 1.0)/p^2,"",(p^2 - 1.0)/p^4,"",(p^2 - 1.0)/p^6,"",(p^2 - 1.0)/p^8,"",S)\}$

On obtient alors les résultats numériques suivants pour $m \leq 10^6$, $C_M = 4703$, $C_2 = 4232$, $C_3 = 417$, $C_4 = 52$, $C_5 = 3$:

proportions		probabilités
$\frac{C_2}{C_M} = 0.8998511588$	$\frac{8}{9}$	$= 0.8888888888$
$\frac{C_3}{C_M} = 0.0886668084$	$\frac{8}{9^2}$	$= 0.0987654320$
$\frac{C_4}{C_M} = 0.0110567722$	$\frac{8}{9^3}$	$= 0.0109739368$
$\frac{C_5}{C_M} = 0.0006378907$	$\sum_{j\geq 0} \frac{8}{9^{4+j}}$	$= 0.0013717421$

7. Statistiques et Heuristiques sur les $\delta_{\mathfrak{p}}(x)$, $x \in k^\times$

Le point essentiel, abordé au § 6.3, est le comportement, pour n fixé, des "quotients de Fermat" $\mathfrak{p}^{\delta_{\mathfrak{p}}(\alpha_i)}$, $\delta_{\mathfrak{p}}(\alpha_i) \geq 0$ (Définition 4.1), pour les $\alpha_i \in \Lambda_i^n$ tels que $(\alpha_i) = \mathrm{N}_{k_n/k}(\mathfrak{A}_i)$, où les $\mathfrak{A}_i \in \mathcal{I}_i^n$ (choisis convenablement) représentent toutes les classe de M_i^n. On a alors $\omega_n(\Lambda_i^n) = \Omega(k_n/k)$ pour $i = m_n$.

L'étape de l'algorithme calculant le $(i+1)$-ième sous-groupe M_{i+1}^n de la filtration repose sur le calcul des α_{i+1} à partir des $x_i = \mathrm{N}_{k_n/k}(y_i) \in \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times)$ qui sont par définition tels que $(x_i) = \mathrm{N}_{k_n/k}(\mathfrak{B}_i)$, $\mathfrak{B}_i \in \mathcal{I}_i^n$, ce qui conduit à une relation de la forme : $\mathfrak{A}_{i+1}^{1-\sigma_n} \cdot \mathfrak{B}_i = (y_i)$, avec $\mathfrak{A}_{i+1}$ convenable choisi étranger à p (cf. § 6.2). Lorsque par exemple $\mathcal{C}\ell_k = 1$, on a alors $\mathrm{N}_{k_n/k}(\mathfrak{A}_{i+1}) = (\alpha_{i+1})$ dont on calcule les $\delta_{\mathfrak{p}}(\alpha_{i+1})$ comparés aux $\delta_{\mathfrak{p}}(\alpha)$, $\alpha \in \Lambda_i^n$.

D'après le Théorème 6.4, en supposant $\mathcal{T}_k \neq 1$, l'hypothèse $\lambda \geq 1$ doit conduire à au moins $\frac{1}{v_p(\#\mathcal{T}_k)}\,(\lambda \cdot n + \mu \cdot p^n + \nu)$ valeurs consécutives de l'indice i (de $i = 1$ à $i = m_n$) pour lesquelles tous les α_i sont tels que $\delta_{\mathfrak{p}}(\alpha_i) \geq 1$ pour tout $\mathfrak{p} \mid p$, ce qui rend indispensable la confrontation avec d'expérimentation numérique, d'autant plus que ces propriétés se lisent dans k ; pour cela on se place dans un cadre simple mais non trivial, utilisant des $\mathfrak{A}_i$ premiers.

7.1. **Représentation des classes de la filtration par des idéaux premiers $\mathfrak{L}_i$.** Pour un corps quadratique réel, on souhaite observer le comportement des $\delta_p(\alpha_i)$ dont seule la nullité est susceptible de terminer l'algorithme ; on est alors en "dimension" 1 pour $\Omega(k_\infty/k)$ et un seul $\mathfrak{p} \mid p$ est utilisé, et comme on a ici $\mu = 0$, $m_n \geq \frac{1}{v_p(\#\mathcal{T}_k)}\,(\lambda \cdot n + \nu)$ tend vers l'infini comme $\lambda \cdot n$ si $\lambda \geq 1$. On reprend ici les même hypothèse simplificatrices faites au § 6.3 :
(i) Le corps $k = \mathbb{Q}(\sqrt{m})$ est principal ;
(iii) les entiers $\delta_p(\varepsilon)$ et/ou $\delta_{\mathfrak{p}}(\pi)$ sont non nuls, de telle sorte que la condition suffisante 3.1 ne s'applique pas (en réalité, les résultats n'en dépendent pas, sauf en ce qui concerne le dénombrement des corps k par rapport à certaines propriétés, cf. Remarque 7.2).

Montrons qu'il existe une infinité d'idéaux premiers $\mathfrak{L}$ de k_n représentant une classe donnée c de k_n et totalement décomposés dans l'extension Galoisienne $k_n/\mathbb{Q}$. En effet, d'après le théorème de Tchebotarev, il existe une infinité de nombres premiers ℓ tels que $\left(\frac{H_{k_n}/\mathbb{Q}}{\mathfrak{L}'}\right)$, pour $\mathfrak{L}' \mid \ell$ dans H_{k_n}, soit l'élément de $\mathrm{Gal}(H_{k_n}/k_n)$ qui correspond à c par le corps de classes sur k_n ; comme H_{k_n}/k_n est Abélienne, ce Frobenius ne dépend que de l'idéal premier $\mathfrak{L}$ de k_n au-dessous de $\mathfrak{L}'$. L'image de $\left(\frac{H_{k_n}/k_n}{\mathfrak{L}}\right)$ dans $\mathrm{Gal}(H_{k_n}/k_n)$ est encore c et c est représentée par $\mathfrak{L}$ totalement décomposé dans $k_n/\mathbb{Q}$.
Par ce choix, on ne modifie pas les $\delta_p(\alpha_i)$ provenant de $c_i = c\ell_{k_n}(\mathfrak{A}_i) \in M_i^n$ puisque la relation $\mathfrak{L}_i = \mathfrak{A}_i \cdot (\gamma_i)$ implique $\mathrm{N}_{k_n/k}(\mathfrak{L}_i) = (\alpha_i) \cdot (\mathrm{N}_{k_n/k}(\gamma_i))$ et que $\delta_p(\mathrm{N}_{k_n/k}(\gamma_i)) \geq n$.

Autrement dit, en se limitant à des idéaux premiers $\mathfrak{L}$ totalement décomposés dans $k_n/\mathbb{Q}$ et en considérant $\mathfrak{l} = (\alpha)$ pour l'idéal premier $\mathfrak{l} = \mathrm{N}_{k_n/k}(\mathfrak{L})$ de k en-dessous de $\mathfrak{L}$, on peut effectuer des statistiques sur les valeurs prises par $\delta_p(\alpha)$ *indépendamment de tout contexte conjecture de Greenberg* puisque les $\mathfrak{L}_i$ seront aléatoirement certains $\mathfrak{L}$ particuliers.
Le nombre α est un entier de k (unique à une unité près) de norme $\ell = \mathfrak{l} \cap \mathbb{Z}$ sur $\mathbb{Q}$, où $\ell^{p-1} \equiv 1 \pmod{p^{n+1}}$. On a $\alpha^{p-1} = 1 + p \cdot p^{\delta_p(\alpha)} \cdot \beta$, β étranger à p, si $\delta_p(\alpha) < n$.

7.1.1. *Cas $p = 3$.* Dans l'expérimentation numérique pour $p = 3$, on prend n assez grand, de sorte que l'on compte les cas où $\delta_p(\alpha) = k$, où k varie de 0 à $n-1$ au plus et on compare le résultat aux probabilités naturelles $\frac{2}{3}$, $\frac{2}{3^2}$, $\cdots$, $\frac{2}{3^k}$, $\cdots$.

Le programme compte dans C_k les proportions de nombres premiers $\ell \equiv \pm 1 \pmod{3^{n+1}}$ tels que $\delta_p(\alpha) = k$:

$\{p = 3; m = 397; n = 12; B = 10^{13}; M = p^{(n+1)}; Q = x^2 - m; K = bnfinit(Q, 1);$
$C0 = 0; C1 = 0; C2 = 0; C3 = 0; C4 = 0; C5 = 0; NL = 0;$
$for(t = -1, 0, L = 2 * t + 1; while(L < B, L = L + 2 * M;$
$if(isprime(L) == 1 \& kronecker(L, m) == 1, NL = NL + 1;$
$Sm = bnfisintnorm(K, -L); Sp = bnfisintnorm(K, L);$
$if(component(matsize(Sm), 2) > 1, A = component(Sm, 1));$
$if(component(matsize(Sp), 2) > 1, A = component(Sp, 1));$
$AA = (Mod(A, Q)^2 - 1)/3; v = valuation(AA, 3);$
$if(v == 0, C0 = C0 + 1); if(v == 1, C1 = C1 + 1);$
$if(v == 2, C2 = C2 + 1); if(v == 3, C3 = C3 + 1);$
$if(v == 4, C4 = C4 + 1); if(v >= 5, C5 = C5 + 1))));$
$print(p, "", m, "", n, "", B); print(NL, "", C0, "", C1, "", C2, "", C3, "", C4, "", C5);$
$print(""); print(C0/NL + 0.0, "", C1/NL + 0.0, "", C2/NL + 0.0, "", C3/NL + 0.0, "",$
$C4/NL + 0.0, "", C5/NL + 0.0); print(""); S = 0.0; for(j = 1, 8, S = S + (p - 1.0)/p^{(5+j)});$
$print(2./3, "", 2./9, "", 2./27, "", 2./81, "", 2./243, "", S)\}$

On obtient la remarquable confirmation du fait que les $\delta_p(\alpha)$ se répartissent de façon indépendante de la condition très forte $\ell \equiv \pm 1 \pmod{3^{n+1}}$, quel que soit le niveau n.
On considère l'exemple ci-dessous, pour lequel $\delta_p(\varepsilon) = 1$:

$$p = 3,\ \ m = 103,\ \ n = 12,\ \ \ell \equiv \pm 1 \pmod{3^{13}},\ \ 1 < \ell < 10^{13}.$$

Il y a alors $N_L = 325791$ nombres premiers ℓ dans l'intervalle, dont respectivement

$C_0 = 217142$, $C_1 = 72364$, $C_2 = 24287$, $C_3 = 8140$, $C_4 = 2581$ et $C_5 = 1277$, sont tels que $\delta_p(\alpha) = 0, 1, 2, 3, 4$ et $\delta_p(\alpha) \geq 5$.

proportions		probabilités
$C_0 = 0.6665070551$	$\frac{2}{3}$	$= 0.6666666666$
$C_1 = 0.2221178608$	$\frac{2}{3^2}$	$= 0.2222222222$
$C_2 = 0.0745477929$	$\frac{2}{3^3}$	$= 0.0740740740$
$C_3 = 0.0249853433$	$\frac{2}{3^4}$	$= 0.0246913580$
$C_4 = 0.0079222569$	$\frac{2}{3^5}$	$= 0.0082304526$
$C_5 = 0.0039196908$	$\sum_{j\geq 6} \frac{2}{3^j}$	$= 0.0041152263$

Le même calcul pour $m = 2149$, où $\delta_p(\varepsilon) = 3$, conduit à des résultats similaires :

$N_L = 325538$, $C_0 = 216955$, $C_1 = 72406$, $C_2 = 24145$, $C_3 = 8060$, $C_4 = 2680$, $C_5 = 1292$.

Enfin en prenant $m = 397$, et des $\ell \equiv \pm 1 \pmod{3^{101}}$, on obtient toujours des valeurs très stables : $N_L = 12174$, $C_0 = 8119$, $C_1 = 2659$, $C_2 = 898$, $C_3 = 337$, $C_4 = 101$, $C_5 = 60$, conduisant par exemple à la proportion 0.6669130934 de $\delta_p(\alpha)$ nuls.

On peut même observer que les résultats sont analogues si l'on considère des nombres premiers $\ell \equiv \pm 1 \pmod{p^{n_0+1}}$, $n_0 \geq 1$ fixé. Mais dans notre contexte avec $n \gg n_0$, $\delta_p(\alpha) \to \infty$ avec n ; autrement dit cette question semble être un problème d'arithmétique indépendant de la conjecture de Greenberg, et probablement accessible.

7.1.2. *Cas général.* On suppose toujours p décomposé dans k et $\mathcal{C}\ell_k = 1$. Le programme est un peu plus complexe car on souhaite obtenir tous les ℓ vérifiant la condition $\ell^{p-1} \equiv 1 \pmod{p^{n+1}}$ (on utilise les puissances ρ^k, $1 \leq k \leq p-1$, d'une racine primitive $(p-1)$-ième de l'unité $\rho \pmod{p^{n+1}}$).

$\{p = 7; m = 44853; n = 5; B = 10^{12}; M = p^{(n+1)};$
$Q = x^2 - m; K = bnfinit(Q, 1); ro = znprimroot(M)^{(p^n)};$
$C0 = 0; C1 = 0; C2 = 0; C3 = 0; C4 = 0; C5 = 0; NL = 0;$
$for(k = 1, p-1, R = Mod(ro, M)^k; L = component(R, 2);$
$while(L < B, L = L + M;$
$if(isprime(L) == 1 \& kronecker(L, m) == 1, NL = NL + 1;$
$Sm = bnfisintnorm(K, -L); Sp = bnfisintnorm(K, L);$
$if(component(matsize(Sm), 2) > 1, A = component(Sm, 1));$
$if(component(matsize(Sp), 2) > 1, A = component(Sp, 1));$
$AA = (Mod(A, Q)^{(p-1)} - 1)/p; v = valuation(AA, p);$
$if(v == 0, C0 = C0 + 1); if(v == 1, C1 = C1 + 1);$
$if(v == 2, C2 = C2 + 1); if(v == 3, C3 = C3 + 1);$
$if(v == 4, C4 = C4 + 1); if(v >= 5, C5 = C5 + 1))));$
$print(p, "", m, "", n, "", B);$
$print(NL, "", C0, "", C1, "", C2, "", C3, "", C4, "", C5); print("");$
$print(C0/NL + 0.0, "", C1/NL + 0.0, "", C2/NL + 0.0, "",$
$C3/NL + 0.0, "", C4/NL + 0.0, "", C5/NL + 0.0); print("");$
$S = 0.0; for(j = 1, 10, S = S + (p - 1.0)/p^{(5+j)});$
$print((p - 1.0)/p, "", (p - 1.0)/p^2, "", (p - 1.0)/p^3, "",$
$(p - 1.0)/p^4, "", (p - 1.0)/p^5, "", S)\}$

On considère dans l'exemple ci-dessous, pour lequel $\delta_p(\varepsilon) = 1$:

$$p = 7,\ \ m = 44853,\ \ n = 5,\ \ \ell^{p-1} \equiv 1 \pmod{7^6},\ \ 1 < \ell < 10^{12}.$$

Il y a alors $N_L = 1118955$ nombres ℓ dans l'intervalle, dont respectivement $C_0 = 959051$, $C_1 = 137487$, $C_2 = 19121$, $C_3 = 2841$, $C_4 = 381$ et $C_5 = 74$, sont tels que $\delta_p(\alpha) = 0, 1, 2, 3, 4$ et $\delta_p(\alpha) \geq 5$.

proportions		probabilités
$C_0 = 0.8570952361$	$\frac{6}{7}$	$= 0.8571428571$
$C_1 = 0.1228708929$	$\frac{6}{7^2}$	$= 0.1224489795$
$C_2 = 0.0170882653$	$\frac{6}{7^3}$	$= 0.0174927113$
$C_3 = 0.0025389760$	$\frac{6}{7^4}$	$= 0.0024989587$
$C_4 = 0.0003404962$	$\frac{6}{7^5}$	$= 0.0003569941$
$C_5 = 0.0000661331$	$\sum_{j\geq 6} \frac{6}{7^j}$	$= 0.0000059499$

On considère enfin le cas suivant pour lequel $\delta_p(\varepsilon) = 1$:

$$p = 29,\ \ m = 683,\ \ n = 5,\ \ \ell^{p-1} \equiv 1 \pmod{29^6},\ \ 1 < \ell < 10^{15}.$$

Il y a alors $N_L = 728880$ nombres ℓ dans l'intervalle, dont respectivement $C_0 = 703535$, $C_1 = 24450$, $C_2 = 857$, $C_3 = 38$, $C_4 = 0$ et $C_5 = 0$, sont tels que $\delta_p(\alpha) = 0, 1, 2, 3, 4$ et $\delta_p(\alpha) \geq 5$.

proportions		probabilités
$C_0 = 0.9652274722$	$\frac{28}{29}$	$= 0.9655172413$
$C_1 = 0.0335446163$	$\frac{28}{29^2}$	$= 0.0332936979$
$C_2 = 0.0011757765$	$\frac{28}{29^3}$	$= 0.0011480585$
$C_3 = 0.0000521347$	$\frac{28}{29^4}$	$= 0.0000395882$
$C_4 = 0$	$\frac{28}{29^5}$	$= 0.0000013651$
$C_5 = 0$	$\sum_{j\geq 6} \frac{28}{29^j}$	$= 0.0000000487$

Ainsi on observe que, statistiquement, il n'y a pas d'obstruction au niveau de la finitude de la i-suite des groupes $\Lambda_i^n = \{x_i \in k^\times,\ \ (x_i) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)\}$, $1 \leq i \leq m_n$, qui sont (dans le contexte particulier étudié) de la forme $\Lambda_i^n = \langle \varepsilon, \alpha_1, \ldots, \alpha_i \rangle$ (cf. (11)) pour lesquels la probabilité d'avoir au plus m_n générateurs (outre l'unité ε) suit une loi binomiale *indépendamment de la valeur de* $n \to \infty$.

On peut alors en déduire, sur un plan heuristique, la nullité de la probabilité d'avoir un nombre de pas $m_n \geq \frac{1}{v_p(\#\mathcal{T}_k)}\,(\lambda \cdot n + \nu)$ pour $\lambda \geq 1$ (cf. Théorème 6.4 et Remarque 7.2).

7.2. **Statistiques sur m_n – Indépendance des α_i.** Considérons un corps quadratique k et le n-ième étage k_n de k_∞ pour lequel on souhaite tester l'indépendance des $\delta_p(\alpha_i) \geq 0$, $\alpha_i \in \Lambda_i^n$, obtenus successivement par l'algorithme de calcul de $\mathcal{C}\ell_{k_n}$. On suppose pour les calculs que $c\ell_k = 1$.

Rappelons alors que si $x_i = \mathrm{N}_{k_n/k}(y_i) \in \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times)$, où $(x_i) = \mathrm{N}_{k_n/k}(\mathfrak{B}_i) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)$, la relation $\mathfrak{A}_{i+1}^{1-\sigma_n} \cdot \mathfrak{B}_i = (y_i)$ fournit le nouvel $\mathfrak{A}_{i+1}$ dont on calcule $\mathrm{N}_{k_n/k}(\mathfrak{A}_{i+1}) =: (\alpha_{i+1})$, $\alpha_{i+1} \in \Lambda_{i+1}^n$, puis $\delta_p(\alpha_{i+1})$, etc.

La recherche par programme des idéaux $\mathfrak{A}_i$ de l'algorithme et des $\alpha_i \in k^\times$ tels que $(\alpha_i) = \mathrm{N}_{k_n/k}(\mathfrak{A}_i)$ étant particulièrement difficile par programme, on se place dans les conditions pour lesquelles le nombre de classes ambiges dans k_n/k est égal à p, donc avec la seule hypothèse :

$$(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p,$$

qui équivaut au fait que le régulateur $R_k = \frac{1}{p} \cdot \log(\varepsilon)$, de l'unité fondamentale ε de k, est égal à p. Il en résulte qu'il est équivalent de faire des statistiques sur l'ordre de $\mathcal{C}\ell_{k_n}$ lorsque $k = \mathbb{Q}(\sqrt{m})$ varie, ce que PARI effectue assez rapidement ; en effet, on a la filtration correspondante $(M_i^n)_{i\geq 0}$, de $M^n = \mathcal{C}\ell_{k_n}$, telle que $\#(M_{i+1}^n/M_i^n) = p$ pour $0 \leq i \leq m_1 - 1$, et telle que :

$$\#\mathcal{C}\ell_{k_n} = \prod_{i=0}^{m_n-1} \#(M_{i+1}^n/M_i^n) = p^{m_n}.$$

On a $M^n = M_1^n$ si et seulement si $M_2^n = M_1^n$, ce qui est équivalent à $\delta_p(\alpha_1) = 0$, de probabilité $1 - \frac{1}{p}$. Ensuite, on a $M^n = M_2^n$ si et seulement si $M_2^n \neq M_1^n$ et $M_3^n = M_2^n$, ce qui est équivalent à $\delta_p(\alpha_1) \geq 1$ et $\delta_p(\alpha_2) = 0$, de probabilité $(1 - \frac{1}{p}) \cdot \frac{1}{p}$, etc.

Remarque 7.1. Noter que puisque $\mathrm{N}_{k/\mathbb{Q}}(\varepsilon) = 1$, la condition $R_k \equiv 0 \pmod{p}$ est équivalente à $\delta_p(\varepsilon) \geq 1$ (cf. Lemme 5.1 et Remarque 5.2) et est donc de probabilité $\frac{1}{p}$, alors que pour $x \in k^\times$ arbitraire, la condition $\delta_{\mathfrak{p}}(x) \geq 1$ pour tout $\mathfrak{p} \mid p$ est de probabilité $\frac{1}{p^2}$.

Plus généralement, si $\alpha = 1 + p \cdot p^r \cdot \beta$, $0 \leq r < n$, est tel que $\mathrm{N}_{k/\mathbb{Q}}(\alpha) \equiv 1 \pmod{p^{n+1}}$ (ce qui est le cas lorsque α est norme d'un idéal de k_n) on a la relation exceptionnelle :

$$\beta + \beta' + p^{r+1} \cdot \beta\,\beta' = u \cdot p^{n-r}$$

qui reflète la formule du produit et qui modifie la probabilité de p-divisibilité de β en $\frac{1}{p}$ au lieu de $\frac{1}{p^2}$ puisque $p \mid \beta$ équivaut à $p \mid \beta'$, et donc modifie les probabilités pour $\delta_p(\alpha)$.

Si α est une unité ε, on a la relation $\beta' + \beta \cdot \varepsilon' = 0$ qui rend la propriété ci-dessus vraie pour tout n.

Les deux programmes suivants pour $k = \mathbb{Q}(\sqrt{7})$ et $p = 3$ justifient à nouveau le phénomène pour un $\alpha \in k^\times$ étranger à p selon la proximité de $\mathrm{N}_{k/\mathbb{Q}}(\alpha)$ avec 1 (cf. Lemme 5.1, Remarques 5.2 et 7.1) :

(i) Cas où l'on impose que la norme de l'élément aléatoire y soit assez proche de 1 (on peut remplacer 9 par toute puissance de 3 plus grande, le résultat est inchangé) :

$\{m = 7; Q = x^2 - m; X = Mod(x, Q); N = 10^4; B = 10^6; NY = 0.0; NY0 = 0.0;$
$for(k = 1, B, a = random(N); b = random(N); Y = a * X + b; n = norm(Y);$
$if(Mod(n^2, 9) == 1, NY = NY + 1; Z = (Y^2 - 1)/3; z = norm(Z);$
$if(valuation(z, 3) == 0, NY0 = NY0 + 1))); print(NY0/NY)\}$

Densité de $\delta_p(y) = 0$ obtenue : $0.6667092445 \sim \frac{2}{3}$.

(ii) Cas sans conditions (i.e., aucune condition de norme locale en dehors de p pour y) :

$\{m = 7; Q = x^2 - m; X = Mod(x, Q); pi1 = X - 2; pi2 = X + 2;$
$N = 10^4; B = 10^6; NY = 0.0; NY0 = 0.0;$
$for(k = 1, B, a = random(N); b = random(N); Y = a * X + b;$
$n = norm(Y); if(Mod(n, 3)! = 0, NY = NY + 1;$
$Z = (Y^2 - 1)/3; Z1 = Z * pi1; Z2 = Z * pi2;$
$v1 = valuation(component(Z1, 2), 3); v2 = valuation(component(Z2, 2), 3);$
$v = min(v1, v2); if(v == 0, NY0 = NY0 + 1))); print(NY0/NY)\}$

Densité de $\min(\delta_{\mathfrak{p}}(y), \delta'_{\mathfrak{p}}(y)) = 0$ obtenue : $0.8881668501 \sim \frac{8}{9}$.

7.2.1. *Cas de m_1 & m_2.* Dans le cas $n = 1$, il suffit de supposer $R_k \equiv 0 \pmod p$, donc que k est tel que $\delta_p(\varepsilon) \geq 1$ (probabilité $\frac{1}{p}$). Autrement dit, $\varepsilon \in \Lambda_i$ est partout norme locale et n'intervient pas dans les raisonnements.

L'indépendance des α_i est alors mesurée par les probabilités $\frac{p-1}{p^h}$ d'avoir $\#\mathcal{C}\ell_{k_1} = p^h$, $h \geq 1$. En effet, puisque α_i est norme locale en dehors de p (i.e., $\mathrm{N}_{k/\mathbb{Q}}(\alpha_i)^{p-1} \equiv 1 \pmod{p^2}$), la probabilité que p divise $\frac{\alpha_i^{p-1}-1}{p}$ est $\frac{1}{p}$; la probabilité de $\delta_p(\alpha_i) = 0$ est donc $1 - \frac{1}{p}$. Pour $h \geq 1$ la probabilité de divisibilité par p^h est $\frac{1}{p^h}$, et par conséquent la probabilité que $\#\mathcal{C}\ell_{k_1} = p^h$ est $\left(1 - \frac{1}{p}\right) \cdot \frac{1}{p^{h-1}} = \frac{p-1}{p^h}$.

Le programme est valable pour tout $p > 2$, mais pour $p > 3$, le temps de calcul devient prohibitif si l'on veut traiter un nombre important de cas. Il est écrit pour $n = 1$; pour $n > 1$ remplacer $polsubcyclo(p^2, p)$ par $polsubcyclo(p^{n+1}, p^n)$:

$\{p = 3; Cyclo = polsubcyclo(p^2, p);$
$C1 = 0; C2 = 0; C3 = 0; C4 = 0; CM = 0;$
$b = 1; B = 3 * 10^5; m = b; while(m < b + B, m = m + 1;$
$if(core(m) == m \& kronecker(m, p) == 1,$
$M = m; t = Mod(m, 4); if(t! = 1, M = 4 * m);$
$h = qfbclassno(M); if(valuation(h, p) == 0, E = quadunit(M);$
$e1 = component(E, 2); e2 = component(E, 3); if(t == 1, e2 = e2/2; e1 = e1 + e2);$
$E = Mod(e1 + e2 * x, x^2 - m;); EE = component(E^{(p-1)} - 1, 2);$
$vale = valuation(EE, p) - 1; if(vale == 1, CM = CM + 1;$
$P = polcompositum(Cyclo, x^2 - m;); R = component(P, 1);$
$K = bnfinit(R, 1); H = bnrinit(K, 1);$
$G = component(component(H, 5), 1); w = valuation(G, p);$
$if(w == 1, C1 = C1 + 1); if(w == 2, C2 = C2 + 1);$
$if(w == 3, C3 = C3 + 1); if(w >= 4, C4 = C4 + 1)))));$
$print(CM, "", C1, "", C2, "", C3, "", C4); print(C1/CM + 0.0, "", C2/CM + 0.0, "",$
$C3/CM + 0.0, "", C4/CM + 0.0); S = 0.0; for(j = 0, 8, S = S + (p^2 - 1)/p^{(8+2*j)});$
$print((p^2 - 1.0)/p^2, "", (p^2 - 1.0)/p^4, "", (p^2 - 1.0)/p^6, "", S)\}$

Pour $p = 3$ et $B = 3 \cdot 10^5$ on obtient les valeurs numériques $C_M = 18928$, $C_1 = 16857$, $C_2 = 1814$, $C_3 = 221$, $C_4 = 36$ et le tableau suivant :.

proportions		probabilités
$\frac{C_1}{C_M} = 0.8905853761$	$\frac{8}{9}$	$= 0.8888888888$
$\frac{C_2}{C_M} = 0.0958368554$	$\frac{8}{9^2}$	$= 0.0987654320$
$\frac{C_3}{C_M} = 0.0116758241$	$\frac{8}{9^3}$	$= 0.0109739368$
$\frac{C_4}{C_M} = 0.0019019442$	$\sum_{j\geq 0} \frac{8}{9^{4+j}}$	$= 0.0013717421$

Remarque 7.2. La différence de nature entre d'une part les résultats numériques obtenus ici sur le comportement "fictif" des $\delta_p(\alpha_i)$ déduit du calcul effectif de $\#\mathcal{C}\ell_{k_n}$, et d'autre part les expérimentations du § 7.1 sur la représentation des classes par des idéaux premiers $\mathfrak{L}$ totalement décomposés dans $k_n/\mathbb{Q}$, provient des faits suivants :

Dans l'écriture $\varepsilon = \mathrm{N}_{k_n/k}(y_1)$ qui conduit à $(y_1) = \mathfrak{A}_1^{1-\sigma}$, comme $\mathfrak{A}_1$ est défini modulo les idéaux invariants, l'algorithme (non unique) reste valable si l'on prend $\mathfrak{A}_1 = \mathfrak{A}_1' \cdot \mathfrak{P}_1$, où $\mathfrak{A}_1'$ est étranger à p et où $\mathfrak{P}_1 \in \langle S_{k_n} \rangle$ peut être choisi arbitrairement ; on a alors $\mathrm{N}_{k_n/k}(\mathfrak{A}_1) = (\alpha_1)$ avec $\alpha_1 = \alpha_1' \cdot \eta_1$, où η_1 est une S_k-unité (arbitraire).

On a $\#\big(M_2^n/M_1^n\big) = \dfrac{p^n}{(\Lambda_1 : \Lambda_1 \cap \mathrm{N}_{k_n/k}({k_n}^\times))}$, où $\Lambda_1 = \langle \varepsilon, \alpha_1 \rangle$, et la condition $M^n = M_1^n$ a lieu si et seulement si $M_2^n = M_1^n$, soit $\delta_p(\alpha_1) = 0$; or si la S_k-unité η_1 *est non norme dans* k_n/k, quel que soit α_1' on peut faire en sorte que $\alpha_1 = \alpha_1' \cdot \eta_1$ soit norme, auquel cas on a au contraire $M_2^n \neq M_1^n$.

Autrement dit, cette statistique, dénombrant les corps k tels que $M^n = M_{m_n}^n$, $m_n \geq 1$, par l'algorithme utilisant des idéaux étrangers à p, élimine les corps k dont les S_k-unités sont normes ; ceci se propage pour chaque M_i^n, mais cet algorithme évite le calcul laborieux des S_k-unités non unités et de leurs symboles de Hasse.

On montre, pour $n = 1$, que l'on passe d'une statistique à l'autre en multipliant par $\frac{p+1}{p^k}$, $k \geq 1$, celle relative aux idéaux premiers $\mathfrak{L}$ totalement décomposés dans $k_1/\mathbb{Q}$; les vraies densités sont celles obtenues via la représentation "fictive" des classes de k_1 par les idéaux $\mathfrak{L}$ (e.g., densité des corps k ($\mathcal{C}\ell_k = 1$, $\delta_p(\varepsilon) \geq 1$), tels que $\#\mathcal{C}\ell_{k_1} = \#\mathcal{C}\ell_{k_1}^{G_1} = p$, égale à $\frac{p-1}{p}$).

Dans le cas $n = 2$ sous les hypothèses précédentes, la condition $\#M_1^2 = p$ suppose $\delta_p(\varepsilon) = 1$, et on a alors $\#(M_{i+1}^2/M_i^2) = p$ pour $0 \leq i \leq m_2 - 1$; pour obtenir m_2 il suffit encore de calculer $\#\mathcal{C}\ell_{k_2}$ (cf. § 6.5), mais les calculs sont longs, les statistiques moins précises et l'interprétation probabiliste plus délicate mais conduit à des résultats analogues.

7.2.2. *Heuristique finale.* Les Heuristiques 6.6, 6.7 se résument par l'existence de i_0 assez grand tel que $M_{i+1}^n/M_i^n = 1$ pour tout $i \geq i_0$ et tout $n \geq e_{i_0}$, où la suite finie des e_i, $1 \leq i \leq i_0$, est définie au § 6.5.1 et suggère la formule d'Iwasawa $\#\mathcal{C}\ell_{k_n} = p^\nu$ pour tout $n \geq e_{i_0}$. Ceci correspond à la succession des diviseurs t_i de $\#\mathcal{T}_k$, tendant vers 1, et définis comme les maximum sur n des $\#(M_{i+1}^n/M_i^n)$ pour chaque i fixé.

On peut donc proposer l'heuristique probabiliste suivante (on suppose, a priori, $\mu = 0$) :

Heuristique 7.3. *Soit k un corps de nombres totalement réel et soit $p > 2$ totalement décomposé dans $k/\mathbb{Q}$. On considère l'algorithme associé à la filtration de $\mathcal{C}\ell_{k_n}$, $n \geq 1$ fixé, et la i-suite des groupes Λ_i^n, $1 \leq i \leq m_n$, avec $m_n \geq \dfrac{1}{v_p(\#\mathcal{T}_k)} \big(\lambda \cdot n + \nu\big)$ (Théorème 6.4), où $\mathcal{T}_k$ est le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale de k (supposé $\neq 1$).*

(i) La probabilité que, pour un $\alpha_i \in \Lambda_i^n$ fixé, on ait $\delta_\mathfrak{p}(\alpha_i) \geq r$ pour tout $\mathfrak{p} \mid p$ est $\frac{1}{p^{r\cdot(d-1)}}$ et la probabilité que l'on ait $\delta_\mathfrak{p}(\alpha_i) = 0$ pour tout $\mathfrak{p} \mid p$ est $1 - \frac{1}{p^{d-1}}$.

(ii) Soit $c \in \mathcal{C}\ell_k$. Puisque $\mathrm{N}_{k_n/k}(\mathcal{C}\ell_{k_n}) = \mathcal{C}\ell_k$, la probabilité que, pour un idéal $\mathfrak{A}$ de k_n étranger à p, la p-classe de $\mathrm{N}_{k_n/k}(\mathfrak{A})$ soit égale à c, est $\frac{1}{\#\mathcal{C}\ell_k}$.

(iii) La probabilité que l'on ait $\#\mathcal{C}\ell_{k_n} = O\big(p^{\lambda\cdot n}\big)$, $\lambda \geq 1$, est $\frac{1}{p^{O(1)\cdot n}}$, lorsque $n \to \infty$.

Cette heuristique (même imparfaite) montre non seulement la légitimité de la conjecture de Greenberg mais aussi que la suite des $\#\mathcal{C}\ell_{k_n}$ est probablement très rapidement stationnaire, ce qui est plutôt un élément favorable pour une approche analytique éventuelle (e.g., exemples de stabilisations donnés dans [KS]).

Il semble difficile de trouver des arguments théoriques qui "obligeraient" les classes des normes $\mathrm{N}_{k_n/k}(\mathfrak{A})$ d'idéaux aléatoires $\mathfrak{A}$ de k_n à ne pas se répartir uniformément dans $\mathcal{C}\ell_k$, ou les quotients de Fermat successifs des $\alpha \in k^\times$ à ne pas avoir des probabilités de nullité en $1-\frac{1}{p}$, voire encore plus proches de 1 comme nous l'avons longuement analysé dans [Gra5, (2016)] et [Gra6, (2016)] pour les nombres algébriques en général.

Cette question risque de rester sans réponse, d'autant plus qu'un éminent mathématicien français m'avait affirmé, dans un échange au sujet des quotients de Fermat des entiers rationnels : *mais vous savez bien que l'on ne sait absolument rien en dire !*

Tout ceci explique en partie la difficulté exclusivement "théorie d'Iwasawa algébrique" de "calculer" les invariants d'Iwasawa de la limite projective des $\mathcal{C}\ell_{k_n}$.

8. Conclusion

Cette étude (qui a, au moins pour la première partie, des points communs avec par exemple les approches de [Fu1], [FuKo], [FuTa1], [FuTa2], [Gre], [I], [IS1], [IS2], [Su], [Ta1], [Ta2]) montre que la question de la conjecture de Greenberg est essentiellement p-adique et sans doute moins "théorie d'Iwasawa algébrique" qu'admis généralement, le cas Abélien pouvant être de nature plus particulière en raison des "formules analytiques" du nombre de classes introduisant les unités cyclotomiques et conduisant à de nombreux travaux spécifiques (voir [Fu2], [BeN], [BaN], [KS], [Ng1], [Ng2] et leurs références), bien que nous pensions que la version fonctions L p-adiques "élémentaire" (e.g., [Sin] et beaucoup d'autres) ne soit qu'une traduction de l'aspect "modules sur l'algèbre d'Iwasawa" ; le passage à la limite (algébrique ou analytique p-adique) est au demeurant plus concis que les calculs aux niveaux finis, pourtant nécessaires pour localiser les profonds phénomènes arithmétiques sous-jacents.

En effet, d'un point de vue théorie d'Iwasawa, le problème porte sur la détermination du quotient de Herbrand $q(\mathcal{X}_k) := \#(\mathcal{X}_k)^G/\#(\mathcal{X}_k)_G$ de $\mathcal{X}_k := \varprojlim_{n\to\infty} \mathcal{C}\ell_{k_n}$, où $(\mathcal{X}_k)^G$ (resp. $(\mathcal{X}_k)_G$) est le noyau (resp. le conoyau) de l'opération de $1-\sigma$ sur $\mathcal{X}_k$, où σ est un générateur topologique de $G := \mathrm{Gal}(k_\infty/k)$ (voir e.g., [Ja6, § 1 & § 4, Lemme 7] pour quelques rappels).

Si la détermination de $(\mathcal{X}_k)_G$ équivaut grosso modo aux résultats du § 4.3, c'est-à-dire à la théorie du corps de classes global, la détermination de $(\mathcal{X}_k)^G$ semble non triviale et probablement liée aux considérations p-adiques précédentes où l'on rencontre manifestement des problèmes de type "quotients de Fermat généralisés" de nombres algébriques dont les heuristiques impliquent facilement que les conjectures énoncées sont très raisonnables ; par exemple, la conjecture de Greenberg pour les corps totalement réels devient triviale lorsque le corps k est p-rationnel (i.e., $\mathcal{T}_k = 1$), mais autrement fort difficile à démontrer au vu de la situation actuelle de ces questions "analytico-diophantiennes p-adiques" qui semblent gouverner plusieurs aspects essentiels de la théorie algébrique des nombres.

Pour conclure, nous nous proposons de faire quelques remarques sur les groupes $\mathcal{T}_{k_n}$ dans la tour cyclotomique, ce qui nous paraît plus canonique en raison de la spécificité de ces groupes de torsion associés à la p-ramification Abélienne et plus susceptibles d'une approche essentiellement p-adique de la conjecture de Greenberg.

Pour tout n, on a encore $\#\mathcal{T}_{k_n} = \#\mathcal{C}\ell_{k_n} \cdot \#(U^*_{k_n}/\overline{E}_{k_n})$ avec des notations analogues à celles du § 4.3 où, au niveau n, les $\mathbb{Z}_p$-modules $U^*_{k_n}$ et $\overline{E}_{k_n}$ sont $\mathbb{Z}_p$-libres de $\mathbb{Z}_p$-rangs $d\cdot p^n - 1$. On peut également noter $R_{k_n} = \#(U^*_{k_n}/\overline{E}_{k_n})$ le régulateur convenablement normalisé de k_n.

Il resterait à étudier la formule d'Iwasawa $\#\mathcal{T}_{k_n} =: p^{\widetilde{\lambda}\cdot n+\widetilde{\nu}}$ (en supposant que $\widetilde{\mu}=0$) telle que $p^{\widetilde{\lambda}} := \dfrac{\#\mathcal{T}_{k_{n+1}}}{\#\mathcal{T}_{k_n}}$ lorsque $n\to\infty$; sous la conjecture de Greenberg, on a $\#\mathcal{C}\ell_{k_{n+1}} = \#\mathcal{C}\ell_{k_n} = p^\nu$,

pour tout n assez grand, auquel cas $p^{\widetilde{\lambda}} = \dfrac{R_{k_{n+1}}}{R_{k_n}}$. On a $\widetilde{\lambda} = 0$ si et seulement si $\mathcal{T}_k = 1$ (i.e., k est p-rationnel) pour les raisons suivantes :

Les "transferts" $j_{k_{n+h}/k_n} : \mathcal{T}_{k_n} \longrightarrow \mathcal{T}_{k_{n+h}}$ sont injectifs pour tous n, h (sous la conjecture de Leopoldt pour p dans la tour, cf., e.g., [Gra1, IV.2, Theorem 2.1]), on a en particulier $\mathcal{T}_{k_{n+h}}^{G_{n+h,n}} = j_{k_{n+h}/k_n}(\mathcal{T}_{k_n})$ puisque l'extension k_{n+h}/k_n est p-primitivement ramifiée ([Gra1, Theorem IV.3.3]). Considérons alors $\nu_{k_{n+h}/k_n} := j_{k_{n+h}/k_n} \circ \mathrm{N}_{k_{n+h}/k_n}$ (ici la norme arithmétique est surjective) ; si $\widetilde{\lambda} = 0$, on a $\mathcal{T}_{k_{n+h}} = j_{k_{n+h}/k_n}(\mathcal{T}_{k_n})$ d'ordre $p^{\widetilde{\nu}}$ constant et, pour h assez grand, on obtient :

$$\mathcal{T}_{k_n} \simeq \nu_{k_{n+h}/k_n}(\mathcal{T}_{k_{n+h}}) = \nu_{k_{n+h}/k_n}(j_{k_{n+h}/k_n}(\mathcal{T}_{k_n})) = j_{k_{n+h}/k_n}(\mathcal{T}_{k_n}^{p^h}) \simeq \mathcal{T}_{k_n}^{p^h},$$

d'où $\mathcal{T}_{k_n} = 1$, et comme $\mathcal{T}_{k_n}^{G_n} \simeq \mathcal{T}_k$, on a $\mathcal{T}_k = 1$.

Ainsi $\widetilde{\lambda} = 0$ implique $\mathcal{C}\ell_{k_n} = R_{k_n} = 1$ pour tout n (p-rationalité dans la tour), ce qui peut suggérer que $\widetilde{\lambda}$ a une certaine "canonicité".

On remarque que $\dfrac{\#\mathcal{T}_{k_n}}{\#\mathcal{T}_k} = \#(\mathcal{T}_{k_n}/\mathcal{T}_{k_n}^{G_n})$ et que le calcul de $(\mathcal{T}_{k_n}/\mathcal{T}_{k_n}^{G_n})^{G_n}$ serait le second pas de l'algorithme définissant la filtration habituelle dans le cadre différent de la p-ramification Abélienne qui, à notre connaissance, n'a pas été étudié.

Remerciements. Je remercie Jean-François Jaulent et Thong Nguyen Quang Do pour de nombreux échanges, commentaires et indications (techniques et bibliographiques) au sujet de ce texte.

Bibliographie

[BaN] R. Badino, T. Nguyen Quang Do, *Sur les égalités du miroir et certaines formes faibles de la conjecture de Greenberg*, Manuscripta Math. 116, 3 (2005), 323–340.

[BJ] K. Belabas, J-F. Jaulent, *The logarithmic class group package in PARI/GP*, Publ. Math. Fac. Sci. Besançon (Théorie des Nombres) 2016, 5–18.

[BeN] J.-R. Belliard, T. Nguyen Quang Do, *On modified circular units and annihilation of real classes*, Nagoya Math. J. 177 (2005), 77–115. http://projecteuclid.org/download/pdf_1/euclid.nmj/1114632159

[CN] L. Caputo, F.A.E. Nuccio, *A criterion for Greenberg's conjecture*, Proc. of the Amer. Math. Soc. 136, 8 (2008), 2741–2744. http://www.ams.org/journals/proc/2008-136-08/S0002-9939-08-09283-6/S0002-9939-08-09283-6.pdf

[Co] J. Coates, *p-adic L-functions and Iwasawa's theory*, In: *Algebraic Number Fields*, Proc. of Durham Symposium 1975, New York-London (1977), 269–353.

[Fu1] T. Fukuda, *Greenberg's Conjecture and Relative Unit Groups for Real Quadratic Fields*, Journal of number theory 65 (1997), 23–39. http://www.sciencedirect.com/science/article/pii/S0022314X97921260

[Fu2] T. Fukuda, *Cyclotomic Units and Greenberg's Conjecture for Real Quadratic Fields*, Mathematics of Computation (65), 215 (1996), 1339–1348. http://www.ams.org/journals/mcom/1996-65-215/S0025-5718-96-00730-2/S0025-5718-96-00730-2.pdf

[FuKo] T. Fukuda, K. Komatsu, *On $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Math. Soc. Japan 38 (1986), 95–102. https://www.jstage.jst.go.jp/article/jmath1948/38/1/38_1_95/_pdf

[FuTa1] T. Fukuda, H. Taya, *The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields*, Acta Arith. 69, 3 (1995), 277–292. http://matwbn.icm.edu.pl/ksiazki/aa/aa69/aa6936.pdf

[FuTa2] T. Fukuda, H. Taya, *Computational research on Greenberg's conjecture for real quadratic fields*, Mem. School Sci. Eng. Waseda Univ. 58 (1994), 175–203.

[Gra1] G. Gras, *Class Field Theory: from theory to practice*, SMM, Springer-Verlag, 2003; second corrected printing 2005.

[Gra2] G. Gras, *Classes généralisées invariantes*, J. Math. Soc. Japan 46, 3 (1994), 467–476. http://projecteuclid.org/euclid.jmsj/1227104692

[Gra3] G. Gras, *Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ, I*, Annales de l'Institut Fourier, 23, 3 (1973), 1–48, 23, 4 (1973), 1–44. http://archive.numdam.org/ARCHIVE/AIF/AIF_1973__23_3/AIF_1973__23_3_1_0/AIF_1973__23_3_1_0.pdf http://archive.numdam.org/ARCHIVE/AIF/AIF_1973__23_4/AIF_1973__23_4_1_0/AIF_1973__23_4_1_0.pdf

[Gra4] G. Gras, *Invariant generalized ideal classes – Structure theorems for p-class groups in p-extensions. A Survey* (2016), to appear in Proceedings – Mathematical Sciences, Indian Academy of Sciences. https://www.dropbox.com/s/oh00jtyxudj3ekt/invariant.generalized.classes.revision%20-%20copie.pdf?dl=0

[Gra5] G. Gras, *Nombre de φ-classes invariantes. Application aux classes des corps abéliens*, Bulletin de la Société Mathématique de France, 106 (1978), 337–364. http://archive.numdam.org/ARCHIVE/BSMF/BSMF_1978__106_/BSMF_1978__106__337_0/BSMF_1978__106__337_0

[Gra6] G. Gras, Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques, *Canadian Journal of Mathematics*, Vol. **68**, 3 (2016), 571–624. http://dx.doi.org/10.4153/CJM-2015-026-3

[Gra7] Gras, G., *No general Riemann-Hurwitz formula for relative p-class groups*, Journal of Number Theory 171 (2017), 213–226. https://www.researchgate.net/publication/288060081

[Gre] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. 98 (1976), 263–284. http://www.jstor.org/stable/2373625?seq=1#page_scan_tab_contents

[Hi] Y. Hiroshi, *On the iwasawa invariants of totally real number fields*, Manuscripta Mathematica (79), 6 (1993), 1–6. http://www.digizeitschriften.de/download/PPN365956996_0079/PPN365956996_0079___log4.pdf

[I] A. Inatomi, *On $\mathbb{Z}_p$-extensions of real Abelian fields*, Kodai Math. J. 12 (1989), 420–422. http://projecteuclid.org/download/pdf_1/euclid.kmj/1138039105

[IS1] H. Ichimura, H. Sumida, *On the Iwasawa invariants of certain real abelian fields, II*, Internat. J. Math. 7 (1996), 721–744. http://www.worldscientific.com/doi/pdfplus/10.1142/S0129167X96000384

[IS2] H. Ichimura, H. Sumida, *On the Iwasawa invariants of certain real abelian fields*, Tôhoku Math. J. 49 (1997), 203–215. http://projecteuclid.org/download/pdf_1/euclid.tmj/1178225147

[Iw] K. Iwasawa, *Riemann–Hurwitz formula and p-adic Galois representations for number fields*, Tohoku Math. J. 33, 2 (1981), 263–288. https://www.jstage.jst.go.jp/article/tmj1949/33/2/33_2_263/_pdf

[Ja1] J-F. Jaulent, *L'arithmétique des ℓ-extensions* (Thèse d'Etat, Université de Franche-Comté, Besançon), Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 1984/86.http://pmb.univ-fcomte.fr/1986/Jaulent_these.pdf

[Ja2] J-F. Jaulent, *Théorie ℓ-adique globale du corps de classes*, J. Théorie des Nombres de Bordeaux 10, 2 (1998), 355–397. http://www.math.u-bordeaux1.fr/~jjaulent/Articles/THCDC.pdf

[Ja3] J-F. Jaulent, *Classes logarithmiques des corps de nombres*, Théorie des Nombres de Bordeaux 6 (1994), 301Ð325.

[Ja4] J-F. Jaulent, *Normes cyclotomiques naïves et unités logarithmiques* (2016). http://arxiv.org/abs/1609.01901

[Ja5] J-F. Jaulent, *Sur les normes cyclotomiques et les conjectures de Leopoldt et de Gross-Kuz'min*, Annales. Math. Québec, 2016 (à paraître) https://arxiv.org/abs/1509.02743

[Ja6] J-F. Jaulent, *Note sur la conjecture de Greenberg* (2016).

[KS] J. S. Kraft, R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. 97 (1995), 135–155. http://imaging.uniroma2.it/~schoof/ks.pdf

[LMN] M. Le Floc'h, A. Movahhedi, T. Nguyen Quang Do, *On capitulation cokernels in Iwasawa Theory*, American Journal of Mathematics 127, 4 (2005), 851–877. http://www.unilim.fr/pages_perso/matthieu.lefloch/coker3.pdf

[Ng1] T. Nguyen Quang Do, *Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé*, Int. J. of Number Theory, 2, 1 (2006), 49–64. http://www.worldscientific.com/doi/pdf/10.1142/S1793042106000395

[Ng2] T. Nguyen Quang Do, *Sur une forme faible de la conjecture de Greenberg II*, https://www.researchgate.net/publication/278961782

[Ni] Y. Nishino, *On the Iwasawa Invariants of the Cyclotomic $\mathbb{Z}_2$-Extensions of Certain Real Quadratic Fields*, Tokyo J. Math. 29, 1 (2006), 239–245.

[OT] M. Ozaki, H. Taya, *A note on Greenberg's conjecture for real abelian number fields*, Manuscripta Math. 88, 3 (1995), 311–320. http://link.springer.com/article/10.1007/BF02567825

[P] K. Belabas and al., *Pari/gp, Version 2.5.3*, Laboratoire A2X, Université de Bordeaux I. http://sagemath.org/

[Su] H. Sumida, *On Capitulation of S-Ideals in $\mathbb{Z}_p$-Extensions*, Journal of Number Theory 86 (2001), 163–174. http://www.sciencedirect.com/science/article/pii/S0022314X00925617

[Sin] W. Sinnott, *On p-adic L-functions and the Riemann-Hurwitz genus formula*, Comp. Math. 53, 1 (1984), 3–17. http://archive.numdam.org/ARCHIVE/CM/CM_1984__53_1/CM_1984__53_1_3_0/CM_1984__53_1_3_0.pdf

[Ta1] H. Taya, *On cyclotomic $\mathbb{Z}_p$-extensions of real quadratic fields*, Acta Arithmetica LXXIV, 2 (1996), 107–119. http://matwbn.icm.edu.pl/ksiazki/aa/aa74/aa7422.pdf

[Ta2] H. Taya, *On p-adic zêta functions and $\mathbb{Z}_p$-extensions of certain totally real number fields*, Tohoku Math. J. 51, 1 (1999), 21–33. https://www.jstage.jst.go.jp/article/tmj1949/51/1/51_1_21/_pdf

[Ta3] H. Taya, *Iwasawa λ_5 and μ_5-invariants of a totally real cubic field with discriminant* 1396. http://id.nii.ac.jp/1138/00000408/

[Wa] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.http://link.springer.com/book/10.1007%2F978-1-4612-1934-7

Villa la Gardette, chemin Château Gagnière, F–38520 Le Bourg d'Oisans.
E-mail address: g.mn.gras@wanadoo.fr *url :* http://www.researchgate.net/profile/Georges_Gras