Normes d'idéaux dans la tour cyclotomique et conjecture de Greenberg

Georges Gras

NORMES D'IDÉAUX DANS LA TOUR CYCLOTOMIQUE ET CONJECTURE DE GREENBERG

(HYPOTHÈSES P-ADIQUES SUR LES NORMES D'IDÉAUX)

GEORGES GRAS

Résumé. Pre-print d'un article publé dans "Annales mathématiques du Québec". Soit k un corps de nombres totalement réel et soit k_∞ sa $\mathbb{Z}_p$-extension cyclotomique. Ce travail prolonge notre article « Approche p-adique de la conjecture de Greenberg pour les corps totalement réels » au moyen d'heuristiques sur le comportement p-adique de normes d'idéaux dans k_∞/k ; en effet, cette conjecture (sur la nullité des invariants λ et μ d'Iwasawa) dépend d'images de ces normes dans le groupe de torsion $\mathcal{T}_k$ du groupe de Galois de la pro-p-extension abélienne p-ramifiée maximale de k, donc de leurs symboles d'Artin dans une extension finie F/k obtenue par descente galoisienne de $\mathcal{T}_k$. Une hypothèse naturelle de répartition de ces symboles implique $\lambda = \mu = 0$. Des statistiques dans le cas quadratique confirment la probable exactitude de telles propriétés qui constituent l'obstruction fondamentale à une preuve de la conjecture de Greenberg dans le seul cadre de la théorie d'Iwasawa.

Abstract Pre-print of a publication in " Annales mathématiques du Québec ". Let k be a totally real number field and let k_∞ be its cyclotomic $\mathbb{Z}_p$-extension. This work continues our article «Approche p-adique de la conjecture de Greenberg pour les corps totalement réels » by means of heuristics on the p-adic behavior of ideal norms in k_∞/k ; indeed, this conjecture (on the nullity of the Iwasawa invariants λ, μ) depends on some images of these norms in the torsion group $\mathcal{T}_k$ of the Galois group of the maximal abelian p-ramified pro-p-extension of k, thus of their Artin symbols in a finite extension F/k obtained by Galois descent of $\mathcal{T}_k$. A natural assumption of distribution of these Artin symbols implies $\lambda = \mu = 0$. Statistics in the quadratic case confirm the probable exactness of such properties which constitute the fundamental obstruction for a proof of Greenberg's conjecture in the sole framework of Iwasawa's theory.

Mots-clés Greenberg's conjecture, Iwasawa's theory, p-class groups, class field theory, p-adic regulators, Fermat quotients of algebraic numbers

Mathematics Subject Classification 2010 11R23, 11R29, 11R37, 11Y40

Table des matières

1. Introduction – Contexte « Conjecture de Greenberg »

Dans [6], nous avons posé une hypothèse de répartition « uniforme » de symboles d'Artin convenables de normes $\mathrm{N}_{k_n/k}(\mathfrak{A})$ d'idéaux $\mathfrak{A}$ des étages k_n de la tour cyclotomique $k_\infty = \bigcup_{n\geq 0} k_n$ d'un corps de nombres totalement réel k relativement à un nombre premier donné $p > 2$ totalement décomposé. En effet, on constate qu'il existe des obstructions p-adiques à une preuve, dans le seul cadre de la théorie d'Iwasawa algébrique, de la conjecture de Greenberg sur la nullité des invariants λ et μ pour les corps *totalement réels* [11, Theorems 1 and 2], [12, Conjecture 3.4], étant entendu que cette conjecture se pose quelle que soit la décomposition de p d'après le point de vue de Jaulent [14]. Cette hypothèse de répartition met en jeu le groupe de torsion $\mathcal{T}_k$ (fini) de la pro-p-extension abélienne p-ramifiée maximale H_k^{pr} de k par l'intermédiaire de sa descente galoisienne comme groupe de Galois d'une extension abélienne finie F/k, pouvant être explicitée. Cette hypothèse peut se résumer par le fait que dans l'algorithme de « dévissage » du p-groupe des classes de k_n, les idéaux $\mathfrak{A}$ représentant ces classes sont tels que les symboles d'Artin $\left(\frac{F/k}{\mathrm{N}_{k_n/k}(\mathfrak{A})}\right)$ engendrent $\mathrm{Gal}(F/k)$ en un nombre d'étapes (de l'algorithme) indépendant de $n \gg 0$. Sous ces conditions (cf. Hypothèses (H) énoncées à la fin du § 3), la conjecture de Greenberg en résulte.

Pour un historique sur la conjecture de Greenberg, et sur les travaux précurseurs de Ozaki et Taya [16], [17], [20], se reporter à [6] et à sa bibliographie, ainsi qu'aux récents points de vue de Jaulent [14] et Nguyen Quang Do [15].

2. Pro-p-extension abélienne p-ramifiée maximale – Le groupe $\mathcal{T}_k$

Soit k un corps de nombres galoisien réel, de degré d, et de groupe de Galois g. Soit $S_k := \{\mathfrak{p} \mid p\}$ l'ensemble des p-places de k. Sous la conjecture de Leopoldt pour p dans k_∞, on obtient le schéma ci-après (dit de la *p-ramification abélienne*). Dans toute la suite, on suppose $p > 2$ totalement décomposé dans k.

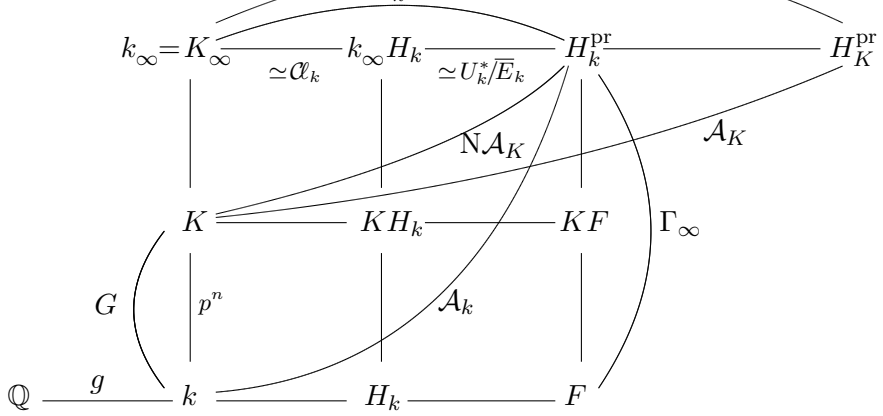
On désigne par $\mathcal{C}\ell_k$ le p-groupe des classes de k et par E_k le groupe des unités globales p-principales $\varepsilon \equiv 1 \pmod p$ de k. Soit $U_k := \bigoplus_{\mathfrak{p}\in S_k} U^1_{\mathfrak{p}}$ le $\mathbb{Z}_p$-module (de $\mathbb{Z}_p$-rang d) des unités locales p-principales où chaque $U^1_{\mathfrak{p}}$ est le groupe des unités $\overline{\mathfrak{p}}$-principales de la complétion $k_{\mathfrak{p}}$ de k en $\mathfrak{p} \in S_k$, et $\overline{\mathfrak{p}}$ l'ideal maximal pour $k_{\mathfrak{p}}$. Par hypothèse, $U_k \simeq (\mathbb{Z}_p^\times)^d = (1 + p\,\mathbb{Z}_p)^d$.

Soit $K := k_n$, de degré p^n sur k, le n-ième étage de la $\mathbb{Z}_p$-extension cyclotomique k_∞ de k ; comme c'est une extension galoisienne *réelle* de $\mathbb{Q}$, sous la conjecture

de Leopoldt le composé de ses $\mathbb{Z}_p$-extensions (corps des fixes de $\mathcal{T}_K$) est réduit à $K_\infty = k_\infty$. Soient $H_k^{\rm pr}$ et $H_K^{\rm pr}$ les pro-p-extensions abéliennes p-ramifiées (i.e., non ramifiées en dehors de p) maximales, de k et K. Dans le schéma, H_k est le p-corps de classes de Hilbert de k et, comme p est non ramifié dans k, $H_k \cap k_\infty = k$ et il existe une extension F de k, contenant H_k, telle que $H_k^{\rm pr}$ soit le composé direct de F et k_∞ sur k. On pose $\Gamma_\infty = {\rm Gal}(H_k^{\rm pr}/F)$.

Les groupes $\mathcal{A}_k := {\rm Gal}(H_k^{\rm pr}/k)$ et $\mathcal{A}_K := {\rm Gal}(H_K^{\rm pr}/K)$ sont des $\mathbb{Z}_p$-modules de sous-modules de torsion $\mathcal{T}_k$ et $\mathcal{T}_K$. Comme k est réel, $\#\mathcal{T}_k$ est donné, sous la conjecture de Leopoldt, par la formule du résidu de la fonction ζ p-adique de k ([2], [3], [19]). Mais on peut affirmer, comme nous l'avons expliqué dans [10], que l'analytique p-adique classique n'apporte actuellement aucune information, aussi nous en resterons aux caractérisations *arithmétiques* de $\mathcal{T}_k$.

Soit $\overline{E}_k$ l'adhérence de l'image diagonale $\iota(E_k)$ de E_k dans U_k ; d'après le corps de classes, on a ${\rm Gal}(H_k^{\rm pr}/H_k) \simeq U_k/\overline{E}_k$. On vérifie, puisque ${\rm rg}_{\mathbb{Z}_p}(\overline{E}_k) = d-1$, que ${\rm tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) = U_k^*/\overline{E}_k$ où U_k^* est le noyau de la norme absolue.



Rappelons ce qui résulte de la conjecture de Leopoldt et qui justifie le schéma :

Théorème 2.1. *([7, § 4]). Soient k un corps de nombres totalement réel et $p \geq 2$ quelconques. Sous la conjecture de Leopoldt pour p dans k on a en toute généralité les suites exactes :*

$$1 \longrightarrow {\rm tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) \longrightarrow \mathcal{T}_k \longrightarrow {\rm Gal}(k_\infty H_k/k_\infty) \longrightarrow 1,$$

$$1 \to {\rm tor}_{\mathbb{Z}_p}(U_k)/\iota(\mu_k) \longrightarrow {\rm tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) \longrightarrow {\rm tor}_{\mathbb{Z}_p}(\log(U_k)/\log(\overline{E}_k)) \to 1,$$

où μ_k est le groupe des racines de l'unité d'ordre puissance de p de k, et où l'on a posé ${\rm tor}_{\mathbb{Z}_p}(\log(U_k)/\log(\overline{E}_k)) =: \mathcal{R}_k$ *qui est appelé le régulateur p-adique normalisé de k.*

Corollaire 2.2. *Ces suites exactes se résument, dans le cas $p > 2$ totalement décomposé (où ${\rm tor}_{\mathbb{Z}_p}(U_k) = 1$), au moyen de la suite exacte :*

$$1 \longrightarrow U_k^*/\overline{E}_k \simeq \mathcal{R}_k \longrightarrow \mathcal{T}_k \longrightarrow \mathcal{C}\ell_k \longrightarrow 1. \tag{2.1}$$

Introduisons les symboles d'Artin $(\frac{H_k^{\rm pr}/k}{\cdot})$ et $(\frac{H_K^{\rm pr}/K}{\cdot})$, respectivement sur $\mathcal{J}_k := I_k \otimes \mathbb{Z}_p$ et $\mathcal{J}_K := I_K \otimes \mathbb{Z}_p$, où I_k et I_K sont les groupes des idéaux étrangers à p de k et K. Leurs images sont les groupes de Galois $\mathcal{A}_k$ et $\mathcal{A}_K$; leurs noyaux sont les groupes d'idéaux principaux infinitésimaux $\mathcal{P}_{k,\infty} \subset \mathcal{J}_k$ et $\mathcal{P}_{K,\infty} \subset \mathcal{J}_K$, où $\mathcal{P}_{k,\infty}$ est

l'ensemble des idéaux principaux (x_∞) où $x_\infty \in k^\times \otimes \mathbb{Z}_p$ est étranger à p et d'image diagonale triviale dans U_k, et de même avec K ([4, Theorem III.2.4, Proposition III.2.4.1] et [13, § 2]).

Le lien entre les normes d'idéaux dans K/k et le groupe de torsion $\mathcal{T}_k$ est donné par le résultat suivant :

Théorème 2.3. *Soit $\mathfrak{A} \in I_K$ (idéal ordinaire vu dans $\mathcal{J}_K$ pour $K = k_n$). Alors il existe des idéaux $\mathfrak{a}, \mathfrak{t} \in \mathcal{J}_k$ et $(x_\infty) \in \mathcal{P}_{k,\infty}$, tels que :*

$$\mathrm{N}_{K/k}(\mathfrak{A}) = \mathfrak{a}^{p^n} \cdot \mathfrak{t} \cdot (x_\infty), \quad \text{avec } \Big(\frac{H_k^{\rm pr}/k}{\mathfrak{a}}\Big) \in \Gamma_\infty,\ \Big(\frac{H_k^{\rm pr}/k}{\mathfrak{t}}\Big) \in \mathcal{T}_k.$$

Pour $n \gg 0$, $\mathfrak{a}^{p^n}$ est principal de la forme (α), $\alpha \in k^\times \otimes \mathbb{Z}_p$, où l'image diagonale $\iota(\alpha)$ de α dans U_k vérifie $\iota(\alpha) \equiv 1 \pmod{p^{n'}}$ pour $n' \to \infty$ avec n, et $\mathfrak{t}$ est d'ordre fini modulo $\mathcal{P}_{k,\infty}$.

Démonstration. L'application norme arithmétique $\mathrm{N}_{K/k}$, définie sur $\mathcal{J}_K$, induit via les symboles d'Artin la restriction (ou projection) $\mathcal{A}_K \to \mathcal{A}_k$ (notée encore $\mathrm{N}_{K/k}$) qui s'exprime par la suite exacte suivante (cf. Schéma) :

$$1 \to \mathrm{Gal}(H_K^{\rm pr}/H_k^{\rm pr}) \longrightarrow \mathcal{A}_K \xrightarrow{\mathrm{N}_{K/k}} \mathrm{N}_{K/k}(\mathcal{A}_K) = \Gamma_\infty^{p^n} \oplus \mathcal{T}_k \to 1. \tag{2.2}$$

Il en résulte que le symbole d'Artin de $\mathrm{N}_{K/k}(\mathfrak{A})$ dans $\mathcal{A}_k$ se décompose de façon unique sur $\Gamma_\infty^{p^n} \oplus \mathcal{T}_k$ sous la forme $\Big(\frac{H_k^{\rm pr}/k}{\mathrm{N}_{K/k}(\mathfrak{A})}\Big) = \Big(\frac{H_k^{\rm pr}/k}{\mathfrak{a}}\Big)^{p^n} \cdot \Big(\frac{H_k^{\rm pr}/k}{\mathfrak{t}}\Big)$, et ainsi $\mathrm{N}_{K/k}(\mathfrak{A})$ peut s'écrire dans $\mathcal{J}_k$ comme indiqué dans l'énoncé. □ □

Le fait que les $\mathrm{N}_{K/k}(\mathfrak{A})$ interviennent de façon cruciale pour la conjecture de Greenberg est justifié, dans la sous-section suivante, au moyen du « calcul du p-groupe des classes de $K = k_n$ » par l'algorithme de dévissage classique qui n'utilise que les propriétés élémentaires de ces normes, la conjecture de Greenberg étant équivalente au fait que ces algorithmes sont bornés indépendamment de n (Théorème 3.3). Il suffit alors d'hypothèses naturelles gouvernant ces normes pour en déduire cette propriété.

Or on verra que $\mathrm{N}_{K/k}(\mathfrak{A}) = (\alpha \cdot x_\infty) \cdot \mathfrak{t}$ ne dépend que de $\mathfrak{t}$ sur le plan p-groupe de classes de k ($\mathrm{N}_{K/k}(\mathfrak{A})$ et $\mathfrak{t}$ définissent la même classe) et sur le plan p-adique ($\iota(\alpha \cdot x_\infty) = \iota(\alpha)$ est arbitrairement proche de 1 et $\mathfrak{t}$ d'ordre fini modulo $\mathcal{P}_{k,\infty}$). Lorsque $\mathfrak{t}$ est principal, le lien subtil entre $\mathfrak{t}$ et le régulateur $\mathcal{R}_k$, est précisé dans la Remarque 3.4 suivant le Théorème 3.3.

Tout ceci est essentiel car $\mathrm{N}_{K/k}(\mathfrak{A})$ ne dépend alors (via le Corollaire 2.2) que des invariants $\mathcal{C}\ell_k$ et $\mathcal{R}_k$ du groupe *fini* $\mathcal{T}_k$ qui devient, quel que soit $K = k_n$, $n \gg 0$, un espace probabilisé explicite (numériquement parlant).

3. Filtration des $\mathcal{C}\ell_{k_n}$ – Facteur classes et facteur normique

Soit $K := k_n \subset k_\infty$ de degré p^n sur k et soit $G := G_n := \mathrm{Gal}(K/k) =: \langle\sigma\rangle$. Dans le cadre de l'algorithme général de calcul du p-groupe des classes $\mathcal{C}\ell_K$ de K par dévissage, on dispose d'une filtration, au moyen de sous-groupes $M_i^n := \mathcal{C}\ell_K(\mathcal{I}_i^n)$, $i \geq 0$, $\mathcal{I}_i^n \subset I_K$, ainsi définie avec $M^n := \mathcal{C}\ell_K$ et $M_0^n := 1$ (d'après [6, § 6.1]) :

Définition 3.1. Pour $n \geq 1$ fixé, $(M_i^n)_{i\geq 0}$ est la i-suite de sous-G-modules de M^n définie par $M_{i+1}^n/M_i^n := (M^n/M_i^n)^G$, 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., tel que $M_{i+1}^n = M_i^n$).

On a alors classiquement :

Théorème 3.2. *La filtration précédente a les propriétés suivantes :*

(i) Pour $i = 0$, $M_1^n = (M^n)^G$ (groupe des classes ambiges dans K/k).

(ii) On a $M_i^n = \{c \in M^n,\ c^{(1-\sigma)^i} = 1\}$, pour tout $i \geq 0$.

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

On en déduit que les groupes $\mathrm{N}_{K/k}(\mathcal{I}_i^n)$, qui représentent $\mathrm{N}_{K/k}(M_i^n) \subseteq \mathcal{C}\ell_k$, sont engendrés, modulo des (α) « quasi-infinitésimaux » (i.e., $\iota(\alpha)$ très proche de 1 dans U_k), par des $\mathfrak{t} \in \mathcal{I}_k$ d'ordre fini modulo $\mathcal{P}_{k,\infty}$ (Théorème 2.3), et que les groupes de nombres :

$$\Lambda_i^n := \{x \in k^\times,\ (x) \in \mathrm{N}_{K/k}(\mathcal{I}_i^n)\}, \tag{3.1}$$

qui contiennent E_k, sont obtenus via les idéaux principaux (x) de la forme :

$$(x) = (\alpha \cdot x_\infty) \cdot \mathfrak{t}_{(x)},$$

où $\mathfrak{t}_{(x)} =: (x')$ est un idéal principal d'ordre fini modulo $\mathcal{P}_{k,\infty}$.

Rappelons que, pour $n \geq 1$ fixé, une généralisation de la formule des classes ambiges de Chevalley, que nous avons redémontrée dans [5], conduit à la i-suite d'entiers définie, au moyen des groupes $\mathrm{N}_{K/k}(M_i^n)$ et Λ_i^n, par :

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

où : (3.2)

$$\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{K/k}(M_i^n)} \quad \& \quad \frac{p^{n\cdot(d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{K/k}(K^\times))}$$

sont appelés respectivement *le facteur classes* et *le facteur normique* à l'étape i de l'algorithme dans k_n. La propriété essentielle de ces facteurs est que le premier est trivialement un diviseur de $\#\mathcal{C}\ell_k$ tandis que le second est (non trivialement) un diviseur de $\#\mathcal{R}_k$ [6, Théorème 4.8 (iii)]. Ils sont indépendants du choix des éléments des $\mathcal{I}_i^n$ modulo des idéaux principaux de K. Comme $\#\mathcal{C}\ell_K = \prod_{i=0}^{m_n-1} \#(M_{i+1}^n/M_i^n)$, la conjecture de Greenberg revient à estimer le nombre de pas m_n de l'algorithme. Or on a à ce sujet le résultat essentiel suivant [6, Théorème 6.3], qui montre déjà le rôle crucial joué par $\mathcal{T}_k$:

Théorème 3.3. *Pour tout $n \gg 0$, on a les inégalités suivantes (pour $\mathcal{T}_k \neq 1$)*[1] *:*

$$\lambda \cdot n + \mu \cdot p^n + \nu \ \geq\ m_n \ \geq\ \frac{1}{v_p(\#\mathcal{T}_k)}\,(\lambda \cdot n + \mu \cdot p^n + \nu), \tag{3.3}$$

où λ, μ, ν sont les invariants d'Iwasawa et v_p la valuation p-adique.

Par conséquent, on a $\lambda = \mu = 0$ si et seulement si le nombre de pas m_n de l'algorithme dans k_n est borné indépendamment de n.

Or m_n (pour n fixé) dépend de la i-progression des deux facteurs de (3.2) et on constate, en pratique, que sous réserve de probabilités naturelles de répartition sur les composantes $\mathcal{C}\ell_k$ et $\mathcal{R}_k$ de $\mathcal{T}_k$, en relation avec le Théorème 2.3, chacun des deux facteurs est rapidement rendu trivial.

1. Le cas $\mathcal{T}_k = 1$ implique trivialement $\lambda = \mu = \nu = 0$; c'est même équivalent dans le cas p-décomposé. De fait, d'après [6, Théorème 4.7], on a $\#\mathcal{C}\ell_K^G = \#\mathcal{T}_k$ pour tout $n \gg 0$.

On rappelle les résultats suivants [6, Lemme 7.1], où i est ici fixé :

(i) La n-suite $\dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} =: p^{c_i^n}$ est *croissante* stationnaire à une valeur maximale $p^{c_i^\infty} \mid \#\mathcal{C}\ell_k$. Ce facteur est rapidement trivialisé (i.e., $p^{c_i^\infty} = 1$ pour tout $i \geq i_1$ convenable) sous réserve que les classes $c\ell_k(\mathrm{N}_{k_n/k}(\mathfrak{A})) = c\ell_k(\mathfrak{t})$ (où les $\mathfrak{A}$ sont des *idéaux aléatoires de* k_n associés à l'algorithme et $\mathfrak{t}$ la composante donnée par la relation du Théorème 2.3), se répartissent de façon uniforme dans le groupe des classes de k (i.e., le recouvrent selon les densités naturelles).

(ii) La n-suite $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))} =: p^{\rho_i^n}$ est *croissante* stationnaire à une valeur maximale $p^{\rho_i^\infty} \mid \#\mathcal{R}_k$. On a $(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)}$ (i.e., $p^{\rho_i^n} = 1$ pour tout $i \geq i_2$ convenable) dès que les symboles normiques de Hasse de *suffisamment* de $x \in \Lambda_i^n$ associés à l'algorithme engendrent le sous-groupe $\Omega(k_n/k)$ de $\bigoplus_{\mathfrak{p}\in S_k} I_\mathfrak{p} = G_n^d$ (où les $I_\mathfrak{p}$ sont les groupes d'inertie), formé des familles $\left(\left(\frac{x, k_n/k}{\mathfrak{p}}\right)\right)_{\mathfrak{p}\in S_k}$ vérifiant la formule du produit ; or chaque symbole dépend essentiellement du $\mathfrak{p}$-quotient de Fermat $\mathfrak{p}^{\delta_\mathfrak{p}(x)}$ de x, où l'on a posé :

$$\frac{x^{p-1}-1}{p} =: \prod_{\mathfrak{p}\in S_k} \mathfrak{p}^{\delta_\mathfrak{p}(x)} \cdot \mathfrak{b}_{(x)}, \quad \delta_\mathfrak{p}(x) \geq 0,\ \mathfrak{b}_{(x)} \text{ étranger à } p. \tag{3.4}$$

Voir [6, Théorème 4.4] pour le calcul de ces symboles. L'ordre de $\left(\frac{x, k_n/k}{\mathfrak{p}}\right)$ étant $p^{n-\delta_\mathfrak{p}(x)}$, ce symbole engendre G_n si et seulement si $\delta_\mathfrak{p}(x) = 0$, a priori de probabilité $1-\frac{1}{p}$, $\delta_\mathfrak{p}(x) \geq r$ étant de probabilité $\frac{1}{p^r}$. D'où aussi une probable trivialisation rapide du facteur normique au cours de l'algorithme.

Remarque 3.4. Nous ne revenons pas sur les résultats de [6, Théorèmes 4.7, 4.8, 4.10] montrant que les facteurs classes et normiques s'interprètent via $\mathcal{T}_k$, mais précisons l'aspect pratique et probabiliste pour les futures études numériques. Soit $x \in \Lambda_i^n$. On a $(x) = \mathrm{N}_{k_n/k}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}_i^n$ (cf. Théorème 3.2 & (3.1)), et d'après le Théorème 2.3, $(x) = (\alpha \cdot x_\infty) \cdot \mathfrak{t}_{(x)}$, $\left(\frac{H_k^{\mathrm{pr}}/k}{\mathfrak{t}_{(x)}}\right) \in \mathrm{Gal}(H_k^{\mathrm{pr}}/k_\infty H_k)$, ce qui conduit à $x = \alpha \cdot x_\infty \cdot x'$, où $(x') = \mathfrak{t}_{(x)}$ (pour tout n assez grand).

Ensuite, puisque $\mathrm{Gal}(H_k^{\mathrm{pr}}/k_\infty\, H_k) \simeq U_k^*/\overline{E}_k$ est d'exposant fini p^e, on a $x'^{p^e} = x'_\infty \cdot \varepsilon'$, $\varepsilon' \in E_k \otimes \mathbb{Z}_p$, x'_∞ infinitésimal, d'où $\mathrm{N}_{k/\mathbb{Q}}(\iota(x')) = 1$ dans $U_\mathbb{Q}$ et l'image de x' est définie dans $U_k^*/\overline{E}_k = \mathcal{R}_k$, donc ne prend qu'un nombre fini de valeurs.

Puisque dans U_k (pour n assez grand) $\delta_\mathfrak{p}(x) = \delta_\mathfrak{p}(\iota(x'))$, nous dirons, par abus, que la famille $(\delta_\mathfrak{p}(x))_{\mathfrak{p}\mid p}$, $x \in \Lambda_i^n/E_k$, varie dans le domaine (fini) défini par l'ensemble des familles $(\delta_\mathfrak{p}(\varepsilon))_{\mathfrak{p}\mid p}$, $\varepsilon \in E_k$; c'est un invariant canonique du corps k. Par exemple, dans le cas quadratique, d'unité fondamentale ε, pour $\delta_\mathfrak{p}(\varepsilon) = r > 0$ donné on écrira que $\delta_\mathfrak{p}(xE_k) \in [0, r]$ selon des probabilités naturelles.

Nous avons formulé dans [6, Hypothèse 7.9] les hypothèses suivantes, au sujet de la composante $\mathfrak{t}$ de $\mathrm{N}_{K/k}(\mathfrak{A})$ définie au Théorème 2.3, que nous nous proposons de tester numériquement :

Hypothèses (H) *On suppose que les idéaux $\mathfrak{A}$ (étrangers à p) de $K = k_n$, obtenus au cours de l'algorithme de calcul par dévissage de $\#\mathcal{C}\ell_K$, définissent une variable aléatoire, et qu'il en est de même pour la composante $\mathfrak{t}$ des $\mathrm{N}_{K/k}(\mathfrak{A})$. Enfin on suppose que les symboles d'Artin $\left(\frac{F/k}{\mathfrak{t}}\right)$ se répartissent uniformément dans* $\mathrm{Gal}(F/k) \simeq \mathcal{T}_k$.

Le terme « uniformément » doit être compris comme une propriété de recouvrement selon les densités (ou probabilités) naturelles en $\frac{1}{p^r}$. Si ces hypothèses sont vérifiées, ceci a les conséquences suivantes :

(i) Les classes des idéaux $\mathfrak{t}$ sont réparties uniformément dans $\mathcal{C}\ell_k$.

(ii) Dans le cas principal $\mathfrak{t} = (x')$, les images des x' dans $U_k^*/\overline{E}_k = \mathcal{R}_k$ parcourent uniformément cet ensemble fini.

(iii) L'heuristique principale de [6] est que les nombres de pas m_n des algorithmes dépendent grosso modo de lois binomiales sur l'espace de probabilité fini $\mathcal{T}_k$ et sont *presque sûrement uniformément bornés* lorsque $n \to \infty$.

Les limites $p^{c_i^\infty + \rho_i^\infty}$ des n-suites $\#(M_{i+1}^n/M_i^n)$, $n \to \infty$, constituent une i-suite *décroissante stationnaire* de diviseurs de $\#\mathcal{T}_k$ [6, Lemme 7.2]. Or si le diviseur limite est différent de 1, c'est que l'hypothèse de répartition précédente n'est pas vérifiée, ce qui, dans un ensemble fini, suppose l'existence d'une « condition étrange » au niveau des composantes $\mathfrak{t}$ successivement obtenues, ce que la pratique numérique que nous allons mettre en œuvre devrait rendre absurde ; en effet, ceci voudrait dire pratiquement que si $\lambda \geq 1$ ou $\mu \geq 1$ alors, pour n fixé *arbitrairement grand*, l'algorithme de dévissage « bouclerait » $O(\lambda \cdot n + \mu \cdot p^n)$ fois de suite (inégalités (3.3)), ce qui constitue un non-sens numérique mais suggère l'immense difficulté pour établir une contradiction effective conduisant à une preuve (certainement plus analytique qu'algébrique) de la conjecture de Greenberg.

4. Calcul des principaux invariants – Classes logarithmiques

On se place dans le cas quadratique réel $k = \mathbb{Q}(\sqrt{D})$, d'unité fondamentale ε, avec $p > 2$ décomposé, et on utilise des programmes PARI [18] pour les calculs. Ici $\Omega(k_n/k) \simeq \mathbb{Z}/p^n\mathbb{Z}$ et les questions normiques ne dépendent que des $\delta_{\mathfrak{p}}(x)$. Mais $\delta_{\mathfrak{p}}(x)$, noté $\delta_p(x)$, ne dépend pas de $\mathfrak{p} \in S_k$ lorsque x *est étranger à* p [6, Définition 4.1 & § 5.1]. Le contexte non trivial est $\delta_p(\varepsilon) > 0$ (sinon $\mathcal{R}_k = 1$ et seul le facteur classes est concerné). Ensuite, pour les x, de l'algorithme, $\delta_p(x)$ ne dépend que de l'idéal (x) si $\delta_p(x) < \delta_p(\varepsilon)$; en effet, si $\delta_p(\varepsilon) = r$ et $\delta_p(x) < r$, alors $\delta_p(x \cdot \varepsilon') = \delta_p(x)$ quelle que soit $\varepsilon' \in E_k$. Enfin le facteur normique se trivialise dès qu'on obtient $x \in \Lambda_i^n$ avec $\delta_p(x) = 0$.

Rappelons que les $x \in \Lambda_i^n$, par nature normes d'idéaux étrangers à p dans k_n/k, sont partout normes locales en dehors de p, auquel cas, $\mathrm{N}_{k/\mathbb{Q}}(x) \equiv 1 \pmod{p^{n+1}}$ (en effet, $\mathrm{N}_{k/\mathbb{Q}}((x))$ peut s'écrire $\mathrm{N}_{\mathbb{Q}_n/\mathbb{Q}}(\mathfrak{B})$ pour un idéal $\mathfrak{B}$ de $\mathbb{Q}_n$, or le groupe de normes associé à $\mathbb{Q}_n/\mathbb{Q}$ par le corps de classes est l'ensemble des $(1 + a \cdot p^{n+1})$, $a \in \mathbb{Z}$). En pratique il n'est pas nécessaire de prendre n très grand car les $\delta_p(\varepsilon)$ sont limités, et dans le cas quadratique, le régulateur p-adique normalisé est $\mathcal{R}_k \sim \frac{1}{p}\log(\varepsilon) \sim p^{\delta_p(\varepsilon)}$ (égalités à un facteur unité p-adique près) ; on fixe $n_0 := n + 1$ (on a alors $K = k_n$ et des congruences modulo p^{n_0} pour les calculs des symboles normiques). Mais on fera en sorte que $n > \delta_p(\varepsilon)$.

4.1. Programme de calcul de h, $\delta_p(\varepsilon)$, $\delta_{\mathfrak{p}}(\eta_p)$ – Condition suffisante.

Il donne la liste des discriminants D pour lesquels $k = \mathbb{Q}(\sqrt{D})$ répond à certaines spécifications destinées à tester l'influence des paramètres suivants : nombre de classes h, valeurs de $\delta_p(\varepsilon)$ et $\delta_{\mathfrak{p}}(\eta_p)$, où η_p est une S_k-unité fondamentale, donnée par $\mathfrak{p}^{h_0} = (\eta_p)$ où h_0 est l'ordre de la classe de $\mathfrak{p}$, et qui n'est utilisée que pour tester la condition suffisante [6, Théorème 3.4] conduisant à $\lambda = \mu = 0$ (condition qui équivaut à la trivialité du groupe des classes logarithmiques $\widetilde{\mathcal{C}\ell_k}$ [14, Théorème 17],

invariant sur lequel nous reviendrons au § 4.2) ; elle suppose la réalisation des deux conditions suivantes :

(i) $\mathcal{C}\ell_k^{S_k} = 1$ (i.e., $\mathfrak{p}$ engendre le p-groupe des classes de k), ce qui équivaut à $v_p(h_0) = v_p(h)$,

(ii) $\delta_p(\varepsilon) = 0$ ou $\delta_{\mathfrak{p}}(\eta_p) = 0$.

Si (i) (resp. (ii)) n'a pas lieu, le programme indique la nature du problème par PB-CLASSES (resp. PB-NORMIQUE). En l'absence des deux alertes, la condition suffisante a lieu et k vérifie la conjecture de Greenberg, ce qui fournit beaucoup d'exemples avec des invariants $\mathcal{C}\ell_k$ et $\mathcal{R}_k$ non triviaux.

On peut fixer un ordre de grandeur à $\delta_p(\varepsilon)$ pour les discriminants retenus en écrivant dans le programme $\mathsf{zmax} = 1/p^g$ pour $\delta_p(\varepsilon) \geq g \geq 0$, et de même on peut imposer des conditions sur h comme par exemple $h \equiv 0 \pmod p$ qui se traduit par $\mathsf{vh} > 0$. L'unité ε est donnée dans E et η_p dans Eta. On doit enfin choisir le nombre premier $\mathsf{p} = p$ et les bornes bD, BD du discriminant :

```
================================================================================
{p=3;bD=2;BD=5*10^5;n=8;n0=n+1;zmax=1/p^2;y=x;
for(D=bD,BD,e=valuation(D,2);M=D/2^e;if(core(M)!=M,next);
if((e==1||e>3)||(e==0 & Mod(M,4)!=1)||(e==2 & Mod(M,4)==1)
|| kronecker(D,p)!=1,next);Q=x^2-D;K=bnfinit(Q,1);
h=component(component(bnrinit(K,1),5),1);vh=valuation(h,p);if(vh>=1,
E=component(component(component(K,8),5),1);Su=bnfsunit(K,idealprimedec(K,p));
pi1=component(component(Su,1),1);pi2=component(pi1,2)*x-component(pi1,1);
Pi1=pi1^n0;Pi2=pi2^n0;Z=bezout(Pi1,Pi2);U1=component(Z,1);U2=component(Z,2);
P=y^2-Mod(D,p^n0);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);
XPpi=Mod(A1*B1+A2*B2*b2,P);XPe=Mod(A1*B1+A2*B2*e,P);x=y;
hs=norm(Mod(pi1,Q));h0=valuation(hs,p);vh0=valuation(h0,p);delta=vh-vh0;
npi=norm(XPpi)^(p-1);ne=norm(XPe)^(p-1);zpi=znorder(npi)/p^n;
ze=znorder(ne)/p^n;if(ze<=zmax,if(delta!=0,print("PB-CLASSES"));
if(zpi+ze<1,print("PB-NORMIQUE"));print("D=",D," h=",h," E=",E);
print("p=",p," Eta=",pi1);print(zpi," ",ze);print(" "))))}
================================================================================
```

Les valeurs $\frac{1}{p^{\delta_{\mathfrak{p}}(\eta_p)}}$ et $\frac{1}{p^{\delta_p(\varepsilon)}}$ sont données dans zpi et ze.

Dès que p croît, il y a raréfaction des cas exceptionnels ; par exemple pour $p = 11$, $D \leq 3 \cdot 10^5$, $h \equiv 0 \pmod{11}$, $\mathsf{zmax} = \frac{1}{11^2}$, on obtient au total 4 cas :

```
PB-NORMIQUE
D=73217 h=11 E=4007500*x - 1084374999
p=11 Eta=441257*x - 119399338
1/11  1/121

D=83689 h=11 E=8962870747239371437765*x - 2592873462296714584831032
p=11 Eta=-5270913810*x - 1524825351767
1     1/1331

D=201997 h=11 E=1781*x + 800454
p=11 Eta=-64391/2*x - 28959651/2
1     1/14641

D=265681 h=44 E=2400852*x - 1237501225
p=11 Eta=22449438752038446508 92*x - 1159999283951803336111535
1     1/121
```

4.2. **Comparaison avec le groupe des classes logarithmiques $\widetilde{\mathcal{C}\ell}_k$.** Le p-groupe des classes logarithmiques a été introduit par Jaulent [13] et utilisé pour

la conjecture de Greenberg, en ceci qu'il donne la condition nécessaire et suffisante suivante, sous la seule conjecture de Leopoldt :

Théorème 4.1. *(*[14, Théorème 7, § 1.4]*). Le corps totalement réel k vérifie la conjecture de Greenberg si et seulement si son groupe des classes logarithmiques $\widetilde{\mathcal{C}\ell}_k$ capitule dans k_∞.*

Ceci est la généralisation de la condition suffisante du § 4.1 disant que $\widetilde{\mathcal{C}\ell}_k = 1$ entraîne la conjecture de Greenberg. Bien que non asymptotique, ce critère est non effectif quant au n_0 à partir duquel l'application d'extension des classes $\widetilde{j}_{k_{n_0}/k}$: $\widetilde{\mathcal{C}\ell}_k \longrightarrow \widetilde{\mathcal{C}\ell}_{k_{n_0}}$ est d'image nulle et il serait intéressant de faire un rapprochement avec l'algorithme de dévissage des $\mathcal{C}\ell_{k_n}$.

On définit les p-groupes $\widetilde{\mathcal{C}\ell}_k$, $\widetilde{\mathcal{C}\ell}_k^{[p]}$, et $\mathcal{C}\ell'_k := \mathcal{C}\ell_k^{S_k} := \mathcal{C}\ell_k/\langle \mathfrak{cl}_k(\mathfrak{p}),\ \mathfrak{p} \in S_k\rangle$, par la suite exacte :

$$1 \longrightarrow \widetilde{\mathcal{C}\ell}_k^{[p]} \longrightarrow \widetilde{\mathcal{C}\ell}_k \longrightarrow \mathcal{C}\ell'_k \longrightarrow 1,$$

qui permet la comparaison avec $\mathcal{C}\ell'_k$, le groupe des S_k-classes de k associé au corps de Hilbert p-décomposé, dont la nullité est la première partie de la condition suffisante du § 4.1 pour la conjecture de Greenberg. La seconde ($\delta_p(\varepsilon) = 0$ ou $\delta_{\mathfrak{p}}(\eta_p) = 0$), sous la première, équivaut donc à la nullité de $\widetilde{\mathcal{C}\ell}_k = \widetilde{\mathcal{C}\ell}_k^{[p]}$. Pour k fixé et $p \gg 0$, il est clair que $\mathcal{C}\ell'_k = 1$ et que la nullité de $\widetilde{\mathcal{C}\ell}_k$ équivaut à $\delta_p(\varepsilon) = 0$ ou $\delta_{\mathfrak{p}}(\eta_p) = 0$.

En utilisant la fonction $\mathsf{bnflog}(\mathsf{K}, \mathsf{p})$ de PARI, décrite dans [1], on peut calculer la structure du p-groupe des classes logarithmiques. Pour le cas des corps quadratiques réels (mais sans l'hypothèse de p-décomposition que l'on peut rajouter via la condition $(\frac{D}{p}) = 1$ sur D) on obtient le programme suivant (ne retenant que les cas où $\widetilde{\mathcal{C}\ell}_k \neq 1$) :

```
================================================================================
{p=3;for(D=10^4,10^4+10^3,e=valuation(D,2);M=D/2^e;if(core(M)!=M,next);
if((e==1||e>3)||(e==0 & Mod(M,4)!=1)||(e==2 & Mod(M,4)==1),next);
P=x^2-D;K=bnfinit(P,1);H=bnflog(K,p);if(component(H,1)!=[],print(D," ",H)))}
================================================================================
```

Donnons les courts extraits suivants de cas non triviaux pour $p = 3$ et 5 (selon les notations $[[\widetilde{\mathcal{C}\ell}_k],\ [\widetilde{\mathcal{C}\ell}_k^{[p]}],\ [\mathcal{C}\ell'_k]]$ de [1, § 4]) :

```
p=3
 D     structures          D     structures          D     structures
10040 [[3], [],  [3]]    10585 [[3], [3], []]     10849 [[27], [27], []]
10060 [[3], [3], []]     10636 [[3], [3], []]     10865 [[3],  [],   [3]]
10077 [[3], [],  [3]]    10641 [[3], [],  [3]]    10889 [[3],  [],   [3]]
10153 [[3], [3], []]     10661 [[3], [],  [3]]    10904 [[3],  [],   [3]]
10172 [[3], [],  [3]]    10664 [[3], [],  [3]]    10929 [[3],  [],   [3]]
10213 [[3], [3], []]     10712 [[3], [],  [3]]    10941 [[3],  [],   [3]]
10301 [[3], [],  [3]]    10721 [[9], [],  [9]]    10949 [[3],  [],   [3]]
10353 [[3], [],  [3]]    10733 [[3], [],  [3]]    10972 [[3],  [3],  []]
10357 [[3], [3], []]     10812 [[3], [],  [3]]    10997 [[3],  [],   [3]]
10457 [[3], [],  [3]]    10844 [[3], [],  [3]]

p=5
 D     structures           D     structures           D      structures
10284 [[25], [25], []]    10408 [[5], [],  [5]]     10649 [[5], [5], []]
10301 [[5],  [5],  []]    10561 [[5], [5], []]      10821 [[5], [5], []]
10396 [[5],  [5],  []]    10613 [[5], [],  [5]]     10885 [[5], [],  [5]]
```

Pour $p = 5$, il y a rapidement raréfaction des cas non triviaux, le cas de $D = 10284$ étant assez exceptionnel.

Quant à $p = 29$, on trouve par exemple $D = 4 \cdot 683, 4 \cdot 890, 4 \cdot 1271, 4349, 4 \cdot 7858$, pour lesquels $\widetilde{\mathcal{C}\ell}_k = \widetilde{\mathcal{C}\ell}_k^{[p]} \simeq \mathbb{Z}/29\mathbb{Z}$.

On constate plus généralement l'identité des résultats numériques donnés par le programme précédent avec ceux donnés dans l'importante table (issue de [6, § 5.2], cas p-décomposé) : `https://www.dropbox.com/s/tcqfp41plzl3u60/R`

où l'indication de au moins l'une des mentions « PB-CLASSES » (i.e., $\mathcal{C}\ell_k^{S_k} \neq 1$) ou « PB-NORMIQUE » (i.e., $\delta_p(\varepsilon) \geq 1$ & $\delta_{\mathfrak{p}}(\eta_p) \geq 1$), caractérise un groupe de classes logarithmiques non trivial, auquel cas on ne sait pas conclure.

4.2.1. *Remarques sur le groupe des classes logarithmiques.* (i) On notera que pour un corps k totalement réel, dès que le corps de classes de Hilbert H_k est linéairement disjoint de K_∞, la *p-rationalité* de k (i.e., $\mathcal{T}_k = 1$) implique la trivialité du groupe des classes logarithmiques (i.e., $\widetilde{\mathcal{C}\ell}_k = 1$), mais que la réciproque est largement fausse.

De façon précise, sous nos hypothèses (k totalement réel, p-décomposé, $p > 2$), on a (cf. suite exacte (2.1)) :

$$\#\mathcal{T}_k = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k,$$

tandis que :

$$\#\widetilde{\mathcal{C}\ell}_k = \#\mathcal{C}\ell'_k \cdot \#\widetilde{\mathcal{C}\ell}_k^{[p]};$$

or $\widetilde{\mathcal{C}\ell}_k^{[p]}$ est isomorphe à un quotient de $\mathcal{R}_k$ induit par les S_k-unités [14, Schéma § 2.3], ce qui montre que $\mathcal{T}_k = 1$ équivaut ici à $\mathcal{C}\ell_k = 1$ et $\delta_p(\varepsilon) = 0$ (i.e., $\mathcal{R}_k = 1$), tandis que $\widetilde{\mathcal{C}\ell}_k = 1$ équivaut à $\mathcal{C}\ell'_k = 1$ & ($\delta_p(\varepsilon) = 0$ ou $\delta_{\mathfrak{p}}(\eta_p) = 0$).

En dépit de la notation, $\widetilde{\mathcal{C}\ell}_k^{[p]}$ doit être considéré comme un « régulateur logarithmique », donc l'invariant essentiel puisque $\mathcal{C}\ell'_k = 1$ pour $p \gg 0$.

(ii) Donnons des exemples de corps $k = \mathbb{Q}(\sqrt{m})$ (m sans facteur carré) tels que $\mathcal{T}_k \neq 1$ & $\widetilde{\mathcal{C}\ell}_k = 1$:

Corps k tels que $\mathcal{T}_k \neq 1$ & $\widetilde{\mathcal{C}\ell}_k = 1$ avec $\delta_p(\varepsilon) \geq 1$ et $\delta_{\mathfrak{p}}(\eta_p) = 0$:
$m = 43, 58, 79, 82, 85, 109, 151, 181, 199, 202, 247, 271, 310, 322, 331, 337, 391,\ 406, 457, \ldots$

Corps k pour lesquels $\mathcal{T}_k \neq 1$ & $\widetilde{\mathcal{C}\ell}_k = 1$ avec $\delta_p(\varepsilon) = 0$ et $\delta_{\mathfrak{p}}(\eta_p) \geq 1$:
$m = 142, 223, 235, 469, \ldots$

Corps k pour lesquels $\mathcal{T}_k \neq 1$ & $\widetilde{\mathcal{C}\ell}_k = 1$ avec $\delta_p(\varepsilon) = \delta_{\mathfrak{p}}(\eta_p) = 0$:
$m = 229, 346, 427, \ldots$

4.3. **Critère de p-rationalité (i.e., $\mathcal{T}_k = 1$).** Redonnons le programme [8, Programme I], qui détermine la p-rationalité d'un corps de nombres arbitraire défini par un polynôme unitaire irréductible $P \in \mathbb{Z}[x]$, et traitons le cas des corps quadratiques réels ; pour chaque discriminant D on donne le 3-rang de $\mathcal{T}_k$, le test de 3-rationalité et la structure du 3-groupe de classes de rayon 3^{nt}, $\mathsf{nt} \geq 2$ ($\mathsf{nt} = 2$ est suffisant pour le test de p-rationalité et nt assez grand donne la structure de $\mathcal{T}_k$) :

```
================================================================================
{p=3;bD=2;BD=10^5;nt=9;for(D=bD,BD,e=valuation(D,2);M=D/2^e;
if(core(M)!=M,next);if((e==1||e>3)||(e==0 & Mod(M,4)!=1)||(e==2 & Mod(M,4)==1),
next);P=x^2-D;K=bnfinit(P,1);Kpn=bnrinit(K,p^nt);
Hpn=component(component(Kpn,5),2);L=List;v=component(matsize(Hpn),2);
R=0;for(k=1,v-1,c=component(Hpn,v-k+1);if(Mod(c,p)==0,R=R+1;
listinsert(L,p^valuation(c,p),1)));
if(R>0,print("D=",D," rk(T)=",R," K is not ",p,"-rational ",L));
if(R==0,print("D=",D," rk(T)=",R," K is ",p,"-rational ",L)))}
================================================================================
```

On obtient, en se limitant aux corps non 3-rationnels 3-décomposés (rajouter au programme la condition kronecker(D,p) !=1) avec $\mathrm{rg}_3(\mathcal{T}_k) > 1$, les quelques exemples suivants (où le rang est 2) :

```
D=2917  List([9, 3])     D=10636  List([9, 3])      D=14668  List([3, 3])
D=6856  List([3, 3])     D=11293  List([9, 3])      D=15517  List([3, 3])
D=7465  List([9, 9])     D=13273  List([3, 3])      D=15529  List([27, 3])
D=8713  List([9, 3])     D=13564  List([27, 3])     D=15733  List([3, 3])
D=8920  List([3, 3])     D=13861  List([2187, 3])   D=17116  List([9, 3])
D=9052  List([3, 3])     D=14197  List([9, 3])      D=18541  List([3, 3])
```

Par rapport aux corps du point (ii) ci-dessus, on obtient les cas où l'on a simultanément $\mathcal{T}_k \neq 1$ & $\widetilde{\mathcal{C}\ell}_k \neq 1$ ($D = 4{\cdot}67,\ 4{\cdot}103,\ 4{\cdot}106, \ldots$).

5. Statistiques sur les symboles d'Artin des $\mathrm{N}_{K/k}(\mathfrak{A})$ – Exemples

Nous revenons au principe d'analyse, décrit Section 3, pour tester les Hypothèses (H), fin du § 3, sur les normes absolues d'idéaux *étrangers à p* dans la tour cyclotomique d'un corps quadratique réel p-décomposé. On va montrer que l'on peut toujours supposer les idéaux $\mathfrak{A}$ premiers pour effectuer les statistiques.

5.1. **Représentation des classes par des idéaux premiers.** On suppose désormais (pour les calculs) que $p = 3$. On désire établir des statistiques sur l'influence numérique des $\mathrm{N}_{K/k}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}_i^n$, de l'algorithme sur le facteur classes et sur le facteur normique de (3.2), pour $K = k_n$, sachant que l'algorithme détermine des $\mathfrak{A}$ successifs par le biais de « l'équation d'évolution $(y) = \mathfrak{B} \cdot \mathfrak{A}^{1-\sigma}$ », provenant de « $x = \mathrm{N}_{K/k}(y)$ & $(x) = \mathrm{N}_{K/k}(\mathfrak{B})$ », qui sera étudiée Section 6.

Toute classe d'idéaux de K peut se représenter par un idéal premier $\mathfrak{L}$ de K, totalement décomposé dans $K/\mathbb{Q}$ (théorème de Chebotarev dans $H_K/\mathbb{Q}$). Comme une relation de la forme $\mathfrak{A} = \mathfrak{L} \cdot (\alpha)$ dans K implique, dans k :

$$\mathrm{N}_{K/k}(\mathfrak{A}) = \mathrm{N}_{K/k}(\mathfrak{L}) \cdot (\mathrm{N}_{K/k}(\alpha)),$$

le fait de supposer les idéaux $\mathfrak{A}$ premiers est sans conséquences sur l'étude statistique des deux facteurs (3.2) ; en effet, le premier facteur est relatif aux *classes des* $\mathrm{N}_{K/k}(\mathfrak{A})$ aussi représentées par des $\mathrm{N}_{K/k}(\mathfrak{L})$, et le second est relatif aux *indices normiques* $(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{K/k}(K^\times))$, où $\Lambda_i^n := \{x \in k^\times,\ (x) \in \mathrm{N}_{K/k}(\mathcal{I}_i^n)\}$ (cf. (3.1)), qui ne dépendent pas du choix des $x \in \Lambda_i^n$, modulo $E_k \cdot \mathrm{N}_{K/k}(K^\times)$.

On considère donc un grand nombre de premiers ℓ totalement décomposés dans $K/\mathbb{Q}$ (i.e., $\ell \equiv \pm 1 \pmod{3^{n+1}}$ et $(\ell) =: \mathfrak{l} \cdot \mathfrak{l}'$ dans k). On suppose implicitement que $\mathfrak{L}$ et $\mathfrak{l} := \mathrm{N}_{K/k}(\mathfrak{L})$ sont les variables aléatoires qui « conduisent l'algorithme » à chaque étape.

On peut donc supposer $\mathrm{N}_{K/k}(\mathcal{I}_i^n)$ engendré par des $\mathfrak{l}_j = \mathrm{N}_{K/k}(\mathfrak{L}_j)$ du type précédent et $\Lambda_i^n = \{x \in k^\times, (x) \in \langle \mathfrak{l}_j \rangle_j\}$; le facteur classes dépend du sous-groupe $\langle cl_k(\mathfrak{l}_j)\rangle_j$ de $\mathcal{C}\ell_k$ dont la croissance algorithmique, en fonction du nombre de pas, est censée atteindre $\mathcal{C}\ell_k$ puisque $\mathcal{I}_{i+1}^n \supset \mathcal{I}_i^n$.

Si $x \in \Lambda_i^n$, on a donc $(x) = \prod_j \mathfrak{l}_j^{e_j}$, $e_j \in \mathbb{Z}$ (ce qui représente une relation entre les classes des $\mathfrak{l}_j$), et le facteur normique dépend alors des $\delta_3(x)$ et décroît dans la progression de l'algorithme puisque $\Lambda_{i+1}^n \supset \Lambda_i^n$.

Les relations étant nombreuses et inconnues pour faire des statistiques, on s'intéressera dans les sections suivantes au cas particulier des x qui sont des $\mathfrak{l}$-unités ; si r_ℓ est l'ordre de la classe de $\mathfrak{l}$, on posera $\mathfrak{l}^{r_\ell} = (\eta_\ell)$, où η_ℓ est une ℓ-unité (définie modulo E_k), puis on calculera $\delta_3(\eta_\ell)$. Comme $\mathrm{N}_{k/\mathbb{Q}}(\eta_\ell) = \pm \ell^{r_\ell} \equiv \pm 1 \pmod{3^{n+1+r_\ell}}$,

on pourra négliger la conjugaison dans $k/\mathbb{Q}$ et travailler avec un unique idéal premier $\mathfrak{l} \mid \ell$ et une unique η_ℓ.

Ensuite, si l'on constate que les entiers $\delta_3(\eta_\ell)$ ont (par rapport à $\delta_3(E_k)$) les répartitions attendues, alors une propriété analogue en résultera, a fortiori, pour les $\delta_3(x)$ (censés valoir 0 avec une probabilité non nulle) car les «relations» particulières $\mathfrak{l}^{r_\ell} = (\eta_\ell)$ ne donnent qu'une partie des $x \in \Lambda_i^n$ susceptibles d'être normes dans K/k.

On peut cependant donner un aperçu plus général de la question et faire des statistiques sur l'ensemble des relations en considérant un petit nombre de ℓ_j, donnés a priori, en testant si un produit $\prod_j \ell_j^{e_j}$, $e_j \geq 0$, est la norme d'un entier x sans facteur rationnel de $k = \mathbb{Q}(\sqrt{m})$, auquel cas on a la relation $\prod_j \mathfrak{l}_j^{e_j} = (x)$ entre les $\mathfrak{l}_j$ et on détermine la répartition des $\delta_3(x)$ obtenus de cette façon.

Pour simplifier, on a considéré un cas où $h = 3$ et où $\delta_3(\varepsilon) = 4$; la variable Npx compte le nombres de produits non principaux et Nn le nombre total de produits testés. Les e_j sont pris au hasard dans $\{0, 1, 2\}$, un grand nombre de fois ; il n'est pas nécessaire de connaître les ordres des classes des $\mathfrak{l}_j$ car on obtient des statistiques très stables, quel que soit l'ensemble de ℓ_j retenu. De fait le résultat est relativement naturel dans la mesure où caractériser $\delta_3(x)$ revient à faire des statistiques dans des groupes de classes généralisées (i.e., modulo un rayon puissance de p) ; or les théorèmes de densité conduisent à des répartitions canoniques.

On a considéré des $\ell_j \equiv 1 \pmod 9$, mais les résultats sont identiques pour des $\ell_j \equiv 1 \pmod{3^{n_0}}$, n_0 arbitraire, sauf que les produits $\prod_j \ell_j^{e_j}$ deviennent très grands ainsi que le temps de calcul :

```
================================================================================
{p=3;m=7249;Q=x^2-m;K=bnfinit(Q,1);B=10^3;Mp=p^2;listL=List;NlistL=0;L=1;
while(L<B,L=L+2*Mp;if(isprime(L)==1 & kronecker(m,L)==1,NlistL=NlistL+1;
listinsert(listL,L,1)));C0=0;C1=0;C2=0;Nn=0;Npx=0;for(n=1,10^3,PL=1;
for(k=1,NlistL,PL=PL*component(listL,k)^random(3));N=bnfisintnorm(K,PL);
d=matsize(N);d1=component(d,1);d2=component(d,2);if(d2==0,Npx=Npx+1);
if(d2!=0,for(j=1,d2,aa=component(N,j);if(aa!=1,a1=component(aa,1);
a2=component(aa,2);if(gcd(a1,a2)==1,a=Mod(aa,Q);Nn=Nn+1;A=(a^2-1)/3;
v=valuation(A,3);if(v==0,C0=C0+1);if(v==1,C1=C1+1);if(v>=2,C2=C2+1))))));
print(Nn," ",Npx," ",Npx/Nn+0.0);print(" ");
print(C0/Nn+0.0," ",C1/Nn+0.0," ",C2/Nn+0.0);print(" ")}
================================================================================
```

Pour l'exemple de $m = 7249$, on obtient les données suivantes (§ 4.1) :

```
m=7249, h=3, E=17052467702474466522 0*x+14518651659981320194199
p=3, Eta=131480821*x-11194416394
1   1/81
```

pour lesquelles $\delta_{\mathfrak{p}}(\eta_3) = 0$ et $\delta_3(\varepsilon) = 4$; on a testé la liste suivante de nombres premiers $\ell \equiv 1 \pmod 9$, décomposés dans k :

$$\mathsf{listL} = [937,\ 883,\ 811,\ 631,\ 487,\ 181,\ 163,\ 37].$$

On obtient (où $\mathsf{CJ} = \#\{x,\ \delta_3(x) = j\}$, $j = 0, 1$, $\mathsf{C2} = \#\{x,\ \delta_3(x) \geq 2\}$) :

```
Nn=11018  Npx=448  proportion=0.04066073
C0/Nn=0.66563804  C1/Nn=0.29606099  C2/Nn=0.03830096
```

Plusieurs passages du programme donnent : Nn = 10720, Npx= 454, et les proportions attendues de x tels que $\delta_3(x) = 0$:

$$0.666001,\ 0.666652,\ 0.668400,\ 0.667622,\ 0.667252,\ 0.666424,\ 0.666396.$$

Nous revenons à l'étude des facteurs classes et normique à partir des ℓ-unités du corps k pour un grand nombre de ℓ.

5.2. **Facteurs classes et normique de ℓ-unités pour $m = 72262$.** On a $\varepsilon = 632566365854478210\cdot\sqrt{m}+170043910956651732101$ et la 3-unité fondamentale $\eta_3 = -1037963\cdot\sqrt{m}+279020981$.

On a $\delta_{\mathfrak{p}}(\eta_3) = 0$, $\delta_3(\varepsilon) = 4$, $\mathcal{C}\ell_k \simeq \mathbb{Z}/9\,\mathbb{Z}$ est engendré par $\mathfrak{p} \mid 3$ (on a aussi $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/27\,\mathbb{Z}$ et $\mathcal{C}\ell_{k_2} \simeq \mathbb{Z}/81\,\mathbb{Z}$). La condition suffisante pour avoir $\lambda = \mu = 0$ est donc satisfaite et il est intéressant de voir si cela se traduit sur ces études de normes.

Le module 3^{8+1}, qui figure un calcul dans k_8/k pour des ℓ totalement décomposés, peut être modifié à volonté car on observe que les statistiques n'en dépendent pas.

5.2.1. *Programme.* Le programme est le suivant où r est une puissance de $p = 3$ divisant le nombre de classes de k (ici $r \in \{1, 3, 9\}$). Il calcule, pour chaque premier ℓ totalement décomposé dans $K/\mathbb{Q}$ (classés par $\ell \equiv 1 \pmod{3^{n+1}}$, puis $-1 \pmod{3^{n+1}}$), la $\mathfrak{l}$-unité fondamentale η_ℓ, où $\mathfrak{l}$ est un idéal premier de k au-dessus de ℓ, dont la classe est d'ordre r donné et il calcule $\delta_3(\eta_\ell)$; on aura donc $(\eta_\ell) = \mathfrak{l}^r$ (cas particulier de relations de principalité). Ici $n = 8$.

La répartition des ordres des classe des $\mathfrak{l}$ constitue la première partie du programme et seulement en seconde partie, on utilise la valeur de r fixée au début.

Le nombre NLr représente le nombre de premiers $\ell \leq \mathsf{BL} = 2\cdot 10^{12}$ totalement décomposés dans K/k tels que la classe de $\mathfrak{l} = \mathrm{N}_{K/k}(\mathfrak{L})$ soit d'ordre r. Les proportions sont comparées aux probabilités naturelles $\frac{1}{9}$, $\frac{2}{9}$, $\frac{6}{9}$.

On a $\mathsf{NL} = \mathsf{NL1} + \mathsf{NL3} + \mathsf{NL9}$ (nombre de ℓ considérés).

Pour chaque r, on désigne par $\mathsf{C0}, \mathsf{C1}, \mathsf{C2}, \mathsf{C3}, \mathsf{C4}, \mathsf{C5}$ les nombres de $\ell \leq \mathsf{BL}$ tels que $(\eta_\ell) = \mathfrak{l}^r$ et $\delta_3(\eta_\ell) = 0, 1, 2, 3, 4, \geq 5$ respectivement :

```
================================================================================
{r=3;p=3;m=72262;n=8;BL=2*10^12;M=p^(n+1);Q=x^2-m;K=bnfinit(Q,1);
C0=0;C1=0;C2=0;C3=0;C4=0;C5=0;CL1=0;CL3=0;CL9=0;NL=0;NLr=0;
for(t=-1,0,L=2*t+1;while(L<BL,L=L+2*M;if(isprime(L)==1 & kronecker(m,L)==1,
NL=NL+1;Su=bnfsunit(K,idealprimedec(K,L));F=component(component(Su,1),1);
Eta=Mod(F,Q);No=norm(Eta);vcl=valuation(No,L);if(vcl==1,CL1=CL1+1);
if(vcl==3,CL3=CL3+1);if(vcl==9,CL9=CL9+1);if(vcl==r,NLr=NLr+1;
A=F;B=(Mod(A,Q)^2-1)/3;v=valuation(B,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=",p," m=",m," n=",n," BL=",BL);
print("NLr=",NLr," C0=",C0," C1=",C1," C2=",C2," C3=",C3," C4=",C4," C5=",C5);
print(C0/NLr+0.0," ",C1/NLr+0.0," ",C2/NLr+0.0," ",C3/NLr+0.0," ",
C4/NLr+0.0," ",C5/NLr+0.0);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);print(" ");
print("r=",r);print("NL=",NL," CL1=",CL1," CL3=",CL3," CL9=",CL9);
print(CL1/NL+0.0," ",CL3/NL+0.0," ",CL9/NL+0.0);print(1./9," ",2./9," ",6./9)}
================================================================================
```

5.2.2. *Répartition des ordres des classes pour $m = 72262$.* On obtient $\mathsf{NL} = 5584183$, $\mathsf{NL1} = 620512, \mathsf{NL3} = 1240284, \mathsf{NL9} = 3723387$, et le tableau des proportions :

proportions	probabilités
$\mathsf{NL1}/\mathsf{NL} = 0.1111195675$	$\frac{2}{3^3} = 0.1111111111$
$\mathsf{NL3}/\mathsf{NL} = 0.2221066179$	$\frac{2}{3^2} = 0.2222222222$
$\mathsf{NL9}/\mathsf{NL} = 0.6667738145$	$\frac{2}{3^1} = 0.6666666666$

Il est clair que l'heuristique de répartition uniforme est vérifiée. Ceci traduit le comportement du facteur classes destiné à devenir rapidement trivial sous réserve du caractère aléatoire des $\mathfrak{L}$ obtenus par l'algorithme (nous y reviendrons au § 6.2).

5.2.3. *Répartition des $\delta_3(\eta_\ell)$ pour $m = 72262$.* Il reste à voir la répartition des $\delta_3(\eta_\ell)$ selon la valeur de r :

(i) Dénombrement des $\mathscr{C}\ell_k(\mathfrak{l})$ principales et calcul des $\delta_3(\eta_\ell)$.

On obtient $\mathsf{NL1} = 620512$ avec $\mathsf{C0} = 412997, \mathsf{C1} = 137911, \mathsf{C2} = 46166$, $\mathsf{C3} = 15833, \mathsf{C4} = 5090, \mathsf{C5} = 2515$, et le tableau :

proportions	probabilités
$\mathsf{C0}/\mathsf{NL1} = 0.6655745577$	$\frac{2}{3} = 0.6666666666$
$\mathsf{C1}/\mathsf{NL1} = 0.2222535583$	$\frac{2}{3^2} = 0.2222222222$
$\mathsf{C2}/\mathsf{NL1} = 0.0743998504$	$\frac{2}{3^3} = 0.0740740740$
$\mathsf{C3}/\mathsf{NL1} = 0.0255160254$	$\frac{2}{3^4} = 0.0246913580$
$\mathsf{C4}/\mathsf{NL1} = 0.0082029034$	$\frac{2}{3^5} = 0.0082304526$
$\mathsf{C5}/\mathsf{NL1} = 0.0040531045$	$\sum_{j\geq 6} \frac{2}{3^j} = 0.0041152264$

(ii) Dénombrement des $\mathscr{C}\ell_k(\mathfrak{l})$ d'ordre $r = 3$ et calcul des $\delta_3(\eta_\ell)$.

On obtient $\mathsf{NL3} = \mathsf{C0} = 1240284$, $\mathsf{C1} = \mathsf{C2} = \mathsf{C3} = \mathsf{C4} = \mathsf{C5} = 0$.

(iii) Dénombrement des $\mathscr{C}\ell_k(\mathfrak{l})$ d'ordre $r = 9$ et calcul des $\delta_3(\eta_\ell)$.

On obtient aussi $\mathsf{NL9} = \mathsf{C0} = 3723387$, $\mathsf{C1} = \mathsf{C2} = \mathsf{C3} = \mathsf{C4} = \mathsf{C5} = 0$.

Ceci s'explique par le fait que le 3-groupe des classes du « corps miroir » $k^* := \mathbb{Q}(\sqrt{-3 \cdot 72262})$ est d'ordre 3 et que, d'après le théorème de Scholz, puisque l'unité ε de k est 3-primaire, il ne peut y avoir d'autres « pseudo-unités » 3-primaires dans k, c'est-à-dire d'éléments $a \in k^\times \setminus k^{\times 3}$, non unités, tels que $(a) = \mathfrak{a}^3$ et $a \equiv \pm 1 \pmod 9$ dans k (i.e., $\delta_3(a) \geq 1$).

Ainsi, dans les cas $r = 3$ et $r = 9$, les $\delta_3(\eta_\ell)$ sont nécessairement nuls. Mais ceci dépend de l'arithmétique de k et ne concerne que des relations très particulières. De toutes façons cela va dans le bon sens pour le facteur normique car un tel η_ℓ donne un symbole normique d'ordre maximum.

5.3. **Facteurs classes et normique de ℓ-unités pour $m = 10942$.** On a $\varepsilon = 1106174761213722328 80 \cdot \sqrt{m} + 11571032155720815417599$ et une 3-unité fondamentale $\eta_3 = -890711 \cdot \sqrt{m} + 93171947$.

On a $\delta_{\mathfrak{p}}(\eta_3) = 1$, $\delta_3(\varepsilon) = 6$, $h = 3$, $\mathcal{C}\ell_k \simeq \mathbb{Z}/3\,\mathbb{Z}$ et $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/3\,\mathbb{Z} \times \mathbb{Z}/3\,\mathbb{Z}$.

Il s'agit d'un cas où la condition suffisante pour avoir $\lambda = \mu = 0$ n'est pas satisfaite en raison de l'aspect normique, mais le groupe des classes de k est engendré par un idéal premier au-dessus de 3.

Le programme est similaire au précédent avec $r \in \{1, 3\}$, les nombres $\mathsf{NL1}$, $\mathsf{NL3}$ représentent le nombre de premiers $\ell \leq \mathsf{BL} = 2 \cdot 10^{12}$, totalement décomposés dans K/k, tels que la classe de $\mathfrak{l} = \mathrm{N}_{K/k}(\mathfrak{L})$ soit d'ordre $r = 1, 3$ respectivement. Les proportions correspondantes sont comparées aux probabilités naturelles qui sont ici $\frac{1}{3}$, $\frac{2}{3}$. Les variables $\mathsf{C0}, \mathsf{C1}, \mathsf{C2}, \mathsf{C3}, \mathsf{C4}, \mathsf{C5}$ sont les nombres de premiers ℓ tels que $\delta_3(\eta_\ell) = 0, 1, 2, 3, 4, \geq 5$ respectivement et on a $\mathsf{NL} = \mathsf{NL1} + \mathsf{NL3}$.

5.3.1. *Répartition des ordres des classe pour $m = 10942$.* Les données sur la répartition des classe sont les mêmes pour les valeurs de $r \in \{1, 3\}$, à savoir $\mathsf{NL} = 5587470, \mathsf{NL1} = 1862666, \mathsf{NL3} = 3724804$, et pour les proportions :

proportions	probabilités
$\mathsf{NL1}/\mathsf{NL} = 0.333364832$	$\frac{2}{3} = 0.3333333333$
$\mathsf{NL3}/\mathsf{NL} = 0.666635167$	$\frac{2}{3^2} = 0.6666666666$

L'heuristique de répartition uniforme est encore vérifiée pour les classes.

5.3.2. *Répartition des $\delta_3(\eta_\ell)$ pour $m = 10942$.* Il y a deux cas à examiner :

(i) Dénombrement des $\mathcal{C}\ell_k(\mathfrak{l})$ principales et calcul des $\delta_3(\eta_\ell)$.

On obtient $\mathsf{NL1} = 1862666$, $\mathsf{C0} = 1241224$, $\mathsf{C1} = 414270$, $\mathsf{C2} = 138044$, $\mathsf{C3} = 45829$, $\mathsf{C4} = 15475$, $\mathsf{C5} = 7824$ et le tableau :

proportions		probabilités
$\mathsf{C0}/\mathsf{NL1} = 0.6663696014$	$\frac{2}{3}$	$= 0.6666666666$
$\mathsf{C1}/\mathsf{NL1} = 0.2224070230$	$\frac{2}{3^2}$	$= 0.2222222222$
$\mathsf{C2}/\mathsf{NL1} = 0.0741109785$	$\frac{2}{3^3}$	$= 0.0740740740$
$\mathsf{C3}/\mathsf{NL1} = 0.0246039816$	$\frac{2}{3^4}$	$= 0.0246913580$
$\mathsf{C4}/\mathsf{NL1} = 0.0083079843$	$\frac{2}{3^5}$	$= 0.0082304526$
$\mathsf{C5}/\mathsf{NL1} = 0.0042004309$	$\sum_{j\geq 6} \frac{2}{3^j}$	$= 0.0041152264$

(ii) Dénombrement des $\mathcal{C}\ell_k(\mathfrak{l})$ d'ordre 3 et calcul des $\delta_3(\eta_\ell)$.

On obtient $\mathsf{NL3} = 3724804$, $\mathsf{C0} = 0$, $\mathsf{C1} = 2484070$, $\mathsf{C2} = 827554$, $\mathsf{C3} = 275264$, $\mathsf{C4} = 91971$, $\mathsf{C5} = 45945$ et le tableau :

proportions		probabilités
$\mathsf{C0}/\mathsf{NL3} = 0.0000000000$	0	$= 0.0000000000$
$\mathsf{C1}/\mathsf{NL3} = 0.6668995200$	$\frac{2}{3}$	$= 0.6666666666$
$\mathsf{C2}/\mathsf{NL3} = 0.2221738378$	$\frac{2}{3^2}$	$= 0.2222222222$
$\mathsf{C3}/\mathsf{NL3} = 0.0739002642$	$\frac{2}{3^3}$	$= 0.0740740740$
$\mathsf{C4}/\mathsf{NL3} = 0.0246915005$	$\frac{2}{3^4}$	$= 0.0246913580$
$\mathsf{C5}/\mathsf{NL3} = 0.0123348772$	$\frac{2}{3^5}$	$= 0.0123450517$

Les densités et probabilités doivent être décalées en raison de l'impossibilité, lorsque la classe de $\mathfrak{l}$ est d'ordre 3, du cas $\delta_3(\eta_\ell) = 0$ qui s'explique comme suit (noter que, ici encore, la relation $\mathfrak{l}^3 = (\eta_\ell)$ n'est qu'un cas très particulier de relation, et que la plupart des relations $\prod_j \mathfrak{l}_j^{e_j} = (x)$ peuvent conduire à $\delta_3(x) = 0$) :

Pour le corps miroir $k^* = \mathbb{Q}(\sqrt{-3 \cdot 10942})$ le nombre de classes est $216 = 8 \cdot 27$ et le 3-groupe de classes est isomorphe à $\mathbb{Z}/9\,\mathbb{Z} \times \mathbb{Z}/3\,\mathbb{Z}$, ce qui explique que dans k, on doit avoir deux pseudo-unités indépendantes 3-primaires ; l'une est toujours donnée par l'unité fondamentale puisque $\delta_3(\varepsilon) = 6$ et une autre au moyen d'un $\mathfrak{l}$ convenable dont la classe est d'ordre 3 et tel que $\mathfrak{l}^3 = (b)$, $\delta_3(b) \geq 1$. Plus précisément :

Soit $L = \mathbb{Q}(\sqrt{10942}, \sqrt{-3})$ contenant le corps miroir k^* ; comme 3 est ramifié dans $k^*/\mathbb{Q}$ et décomposé dans k, le 3-rang de $\mathcal{T}_L$ est égal à :

$$\mathrm{rg}_3(\mathcal{C}\ell_L^{S_L}) + \#S_L - 1 = \mathrm{rg}_3(\mathcal{C}\ell_L^{S_L}) + 1$$

[4, Proposition III.4.2.2], où S_L est l'ensemble des 3-places de L.

Or $\mathcal{C}\ell_L^{S_L}$ est la somme directe de $\mathcal{C}\ell_k^{S_k} = 1$ (car S_k engendre $\mathcal{C}\ell_k$) et de $\mathcal{C}\ell_{k^*}$ (car S_{k^*} est réduit à une unique 3-place de carré (3)).

Donc $\mathrm{rg}_3(\mathcal{T}_L) = 3$ puis, comme $\mathcal{T}_L = \mathcal{T}_k \bigoplus \mathcal{T}_{k^*}$ et comme $\mathrm{rg}_3(\mathcal{T}_k) = 1$ [4, Corollary III.4.2.3], on a $\mathrm{rg}_3(\mathcal{T}_{k^*}) = 2 = \mathrm{rg}_3(\mathcal{C}\ell_{k^*})$, et toute extension cyclique 3-ramifiée de degré 3 de k^* est nécessairement contenue dans le corps de Hilbert de k^* et est donc non ramifiée ; d'où le fait que pour tout $\mathfrak{l}$ dont la classe est d'ordre 3 avec $\mathfrak{l}^3 = (b)$, nécessairement b est 3-primaire (i.e., $\delta_3(b) \geq 1$), ce qui explique que exceptionnellement $\mathsf{C0} = 0$.

Mais bien entendu, pour les $\mathfrak{l} = (b)$ principaux, on a vu que la propriété de répartition uniforme des $\delta_3(b)$ reste vraie en toute circonstance ; ainsi la condition $\delta_3(\eta_\ell) = 0$ suppose de plus $\mathfrak{l}$ principal (probabilité $\frac{1}{3}$).

5.4. **Exemples de corps k avec $\mathcal{C}\ell_k^{S_k} \neq 1$, $\delta_3(\varepsilon) \geq 1$ & $\delta_{\mathfrak{p}}(\eta_3) \geq 1$.** On a trouvé les cas suivants (avec $h = 3$), pour lesquels aucun des deux points de la condition suffisante de nullité de λ et μ n'est vérifié ; on donne en outre la structure du groupe des classes de k_1 :

(i) $m = 26893, \varepsilon = 142445225/2 \cdot x + 23359714011/2$,
$\eta_3 = -x - 164$,
$\delta_3(\varepsilon) = 3$ & $\delta_{\mathfrak{p}}(\eta_3) = 3$, structure=[36, [18, 2]].

(ii) $m = 31069, \varepsilon = 933602804601721/2 \cdot x + 164560570852019805/2$,
$\eta_3 = -23257 \cdot x + 4099372$,
$\delta_3(\varepsilon) = 3$ & $\delta_{\mathfrak{p}}(\eta_3) = 1$, structure=[27, [3, 3, 3]].

(iii) $m = 92269, \varepsilon = 18203996613665268026218473748508 5/2 \cdot x$
$+5529611923714904129168219124378596 1/2$,
$\eta_3 = -3397805798209/2 \cdot x - 1032111126747851/2$,
$\delta_3(\varepsilon) = 3$ & $\delta_{\mathfrak{p}}(\eta_3) = 1$, structure=[9, [9]]

(iv) $m = 94918, \varepsilon = 1881606172088175003974358115094 34 \cdot x$
$+5796996235321435886132945573590819 7$,
$\eta_3 = -8591 \cdot x - 2646781$,
$\delta_3(\varepsilon) = 3$ & $\delta_{\mathfrak{p}}(\eta_3) = 2$, structure=[27, [9, 3]]

(v) $m = 171061, \varepsilon = 900555961068792369443990032360047045/2 \cdot x$
$+3724656343009482428090591903809686492 73/2$,
$\eta_3 = 902353/2 \cdot x - 373208881/2$,
$\delta_3(\varepsilon) = 4$ & $\delta_{\mathfrak{p}}(\eta_3) = 4$, structure=[9, [9]].

5.4.1. *Remarques sur les exemples précédents.* (i) Pour $m = 31069$ et $r = 3$, on trouve des résultats analogues à ceux du second exemple où $\mathsf{C0} = 0 : \mathsf{NL3} = 3721754$, $\mathsf{C0} = 0$, $\mathsf{C1} = 2480548$, $\mathsf{C2} = 826613$, $\mathsf{C3} = 276142$, $\mathsf{C4} = 92283$, $\mathsf{C5} = 46168$.

(ii) Pour $m \in \{26893, 92269, 94918, 171061\}$ et $r = 3$, on trouve comme pour le premier exemple : $\mathsf{C0} = \mathsf{NL3}$, $\mathsf{C1} = \mathsf{C2} = \mathsf{C3} = \mathsf{C4} = \mathsf{C5} = 0$.

6. Equation d'évolution $(y) = \mathfrak{B} \cdot \mathfrak{A}^{1-\sigma}$ – Obstruction p-adique

Cette section est consacrée à l'observation du passage de l'étape i de l'algorithme à l'étape $i+1$, c'est-à-dire à l'obtention de nouveaux idéaux pour constituer $\mathcal{I}_{i+1}^n$ à partir de $\mathcal{I}_i^n$ (cf. Théorème 3.2 & (3.1)) et sur la question de savoir si ces idéaux et leurs normes sont « aléatoires » ou non par rapport aux précédents.

6.1. **Point fondamental de l'algorithme de calcul des $\#\mathcal{C}\ell_{k_n}$.** Une fois le groupe Λ_i^n déterminé, l'étape suivante de l'algorithme consiste à trouver les $x \in \Lambda_i^n$ normes locales en p, ce qui résulte des valeurs des $\delta_p(x)$ (Relation (3.4)). On pose alors, en vertu du théorème des normes de Hasse :

$$x = \mathrm{N}_{K/k}(y), \quad y \in K^\times, \ \text{défini modulo } K^{\times 1-\sigma},$$

et comme un tel x est par définition norme dans K/k d'un idéal $\mathfrak{B} \in \mathcal{I}_i^n$, on a l'existence de $\mathfrak{A}$ étranger à p, tel que :

$$(y) = \mathfrak{B} \cdot \mathfrak{A}^{1-\sigma},$$

et le but est de vérifier, au moyen de statistiques numériques, l'indépendance du nouveau pas $i+1$ de l'algorithme par rapport au pas i précédent (autrement dit, que $\mathfrak{A}$ n'a aucune relation *algébrique* avec $\mathfrak{B}$ et constitue un nouveau « tirage probabiliste »). Comme $\mathfrak{A}$ peut être défini au produit près par $(\mathfrak{a}) \cdot (z)$, où $(\mathfrak{a})$ est l'étendu

d'un idéal de k et $z \in K^\times$, $\mathrm{N}_{K/k}(\mathfrak{A})$ est défini au produit près par $\mathfrak{a}^{p^n} \cdot \mathrm{N}_{K/k}(z)$ dont le symbole d'Artin dans F/k est trivial pour $n \gg 0$, d'où l'aspect intrinsèque du processus. Ce point est l'élément crucial de l'analyse heuristique de la conjecture de Greenberg.

Ensuite on s'intéresse à $\mathfrak{A}$ pour construire $\mathcal{I}_{i+1}^n$, puis on considère sa norme $\mathrm{N}_{K/k}(\mathfrak{A}) \in \mathrm{N}_{K/k}(\mathcal{I}_{i+1}^n)$ pour obtenir $\Lambda_{i+1}^n \supseteq \Lambda_i^n$, afin de prendre les $x' \in \Lambda_{i+1}^n$ tels que x' soit la norme d'un $y' \in K^\times$, etc., sachant que sous reserve des Hypothèses (H), fin du § 3, on aura statistiquement des $x \in \Lambda_{i+1}^n$ tels que $\delta_p(x) < \delta_p(\Lambda_i^n)$, ce qui fait décroître le facteur normique tandis que les classes des composantes $\mathfrak{t}$ des $\mathrm{N}_{K/k}(\mathfrak{A})$ font décroître le facteur classes.

6.1.1. *Remarques sur :* « *entiers normes locales* » *vs* « *normes d'entiers* ». (i) Le théorème des normes de Hasse pour les extensions cycliques est, au plan numérique, assez problématique et influence fortement notre démarche heuristique puisque il n'existe (à notre connaissance) aucune formule permettant de passer du local au global ; autrement dit, à supposer que les solutions locales y_w dans les complétés K_w au-dessus de v à l'équation normique $x = \mathrm{N}_{K_w/k_v}(y_w)$, soient connues pour toute place v de k et $w \mid v$ de K, il n'est pas possible d'en déduire une solution globale y.

(ii) La relation $x = \mathrm{N}_{K/k}(y)$, pour $x \in k^\times$ partout norme locale dans K/k et *entier* (cas auquel on peut toujours se ramener), est assez subtile car (x) est norme d'un idéal *entier* $\mathfrak{B}$, et s'il existe une solution y *entière*, alors $(y) = \mathfrak{B}$ est principal dans K ; dans le cas contraire, on peut écrire $y = \frac{z}{\Delta}$, $\Delta \in \mathbb{Z}$, z *entier* de K, et il est facile de constater que l'idéal $\mathfrak{A}$ de la relation $(y) = \mathfrak{B} \cdot \mathfrak{A}^{1-\sigma}$ est essentiellement construit avec les idéaux premiers au-dessus de Δ dans K. Ce dénominateur définit de fait le caractère aléatoire de l'algorithme.

(iii) Il faut signaler le cas trivial $x = 1$ et l'équation $\mathrm{N}_{K/k}(y) = 1$ qui conduit, par le Théorème 90 de Hilbert, à $y = z^{1-\sigma}$, $z \in K^\times$, où une solution z_0 est donnée, pour une extension cyclique de degré N, par une résolvante de Hilbert de la forme :

$$z_0 = t + y \cdot t^\sigma + \cdots + y^{1+\sigma+\cdots+\sigma^{i-1}} \cdot\ t^{\sigma^i} + \cdots + y^{1+\sigma+\cdots+\sigma^{N-2}} \cdot\ t^{\sigma^{N-1}}$$

pour $t \in K^\times$ convenable rendant z_0 non nul ; mais l'aspect additif suggère justement une part totalement aléatoire. Dans le cas de l'application du théorème des normes de Hasse et de l'équation norme en idéaux qui en résulte, il n'y a pas de résolvante explicite, mais on peut penser qu'il y a une complexité du même ordre.

Lemme 6.1. *Sans modifier l'algorithme ni les statistiques, on peut supposer que $\mathfrak{B}$ est un idéal premier $\mathfrak{L}$ totalement décomposé dans $K/\mathbb{Q}$. Dans la relation $(y) = \mathfrak{L} \cdot \mathfrak{A}^{1-\sigma}$ qui s'en déduit, on peut supposer que $\mathfrak{A}$ est un idéal premier $\mathfrak{Q}$, totalement décomposé dans $K/\mathbb{Q}$.*

Démonstration. Dans l'algorithme, on peut modifier tout élément $x \in \Lambda_i^n$ modulo $\mathrm{N}_{K/k}(K^\times)$, ce qui est équivalent à choisir $\mathfrak{B}$ modulo un idéal principal ; on peut donc supposer $\mathfrak{B} = \mathfrak{L}$ premier, totalement décomposé dans $K/\mathbb{Q}$.

Il est clair que y peut être modifié modulo $K^{\times 1-\sigma}$ puisque seul $\mathrm{N}_{K/k}(\mathfrak{A})$ est utilisé ; par conséquent, $\mathfrak{A}$ peut être aussi défini modulo un idéal principal, et on peut supposer que $\mathfrak{A} = \mathfrak{Q}$, premier totalement décomposé dans $K/\mathbb{Q}$. Ceci équivaut au fait que $\mathrm{N}_{K/k}(\mathfrak{Q}) =: \mathfrak{q}$ est un idéal premier au-dessus de $q \equiv \pm 1 \pmod{p^{n+1}}$ dont la composante $\mathfrak{t}$ est inchangée. □ □

6.1.2. *Remarques sur le calcul de PARI.* (i) Dans les calculs, PARI ne donne pas directement $\mathfrak{A} = \mathfrak{Q}$, mais le plus souvent un idéal $\mathfrak{A}$ de la forme $\mathfrak{Q}^{\omega}$, $\omega \in \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ non nécessairement égal à 1, ce qui conduit à la relation :

$$\mathrm{N}_{K/k}(\mathfrak{A}) = \mathrm{N}_{K/k}(\mathfrak{Q})^{\omega(1)} =: \mathfrak{q}^{\omega(1)},$$

où $\mathfrak{q}$ est l'idéal premier de k au-dessous de $\mathfrak{Q}$ et $\omega(1) \in \mathbb{Z}$ l'image de ω dans l'application d'augmentation. On a donc à résoudre, en un idéal premier $\mathfrak{Q}$:

$$(y) = \mathfrak{L} \cdot \mathfrak{Q}^{\omega \cdot (1-\sigma)},$$

où $\mathfrak{L}$, idéal premier de K totalement décomposé, est donné tel que :

$$\mathrm{N}_{K/k}(\mathfrak{L}) = \mathfrak{l} =: (x) = (\mathrm{N}_{K/k}(y)) \tag{6.1}$$

(idéal premier principal de k au-dessous de $\mathfrak{L}$).

(ii) L'aspect statistique devra vérifier que $\mathfrak{l} = \mathrm{N}_{K/k}(\mathfrak{L})$ et $\mathfrak{q}^{\omega(1)} = \mathrm{N}_{K/k}(\mathfrak{Q}^{\omega})$ sont *indépendants* du point de vue classes d'idéaux et propriétés p-adiques (au sens des sections précédentes). Ces calculs seront programmés au § 7.1.

6.2. **Remarques heuristiques fondamentales.** (i) On peut objecter que notre démarche pose question en ce sens que l'on peut concevoir logiquement les deux « implications » suivantes :

(a) C'est l'ensemble des groupes de classes des k_n (donc les valeurs de λ et μ) qui « préexistent » et qui « imposent », pour chaque n, les algorithmes numériques qui les déterminent et en particulier qui imposent, quel que soit n, le nombre de pas $m_n = O(1) \cdot (\lambda \cdot n + \mu \cdot p^n)$, non borné si λ ou μ est non nul, alors que la complexité de l'algorithme ne dépend que du groupe fini $\mathcal{T}_k$.

(b) On peut au contraire, *en examinant la nature des calculs*, se convaincre du fait que ce sont bien ces calculs imprévisibles (algébriquement parlant) qui conditionnent les résultats et dire que ce sont plutôt les algorithmes numériques qui « font exister » les groupes de classes pour chaque n, puis leur limite projective. Ces calculs sont fondés sur la résolution, en l'inconnue $\mathfrak{A}$, de l'équation précédente $(y) = \mathfrak{B} \cdot \mathfrak{A}^{1-\sigma}$ (cf. Remarques 6.1.1) et sur la détermination de quotients de Fermat $\left(\frac{x^{p-1}-1}{p}\right) =: \prod_{\mathfrak{p} \in S_k} \mathfrak{p}^{\delta_{\mathfrak{p}}(x)} \cdot \mathfrak{b}_{(x)}$, $\mathfrak{b}_{(x)}$ étranger à p, conduisant aux $\delta_{\mathfrak{p}}(x)$.

A priori, il n'y a pas d'obstruction à une répartition uniforme des composantes $\mathfrak{t} \in \mathcal{T}_k$ associées aux $\mathrm{N}_{K/k}(\mathfrak{A})$ en raison des propriétés du symbole d'Artin de $\mathrm{N}_{K/k}(\mathfrak{A})$ dans $\Gamma_{\infty}^{p^n} \oplus \mathcal{T}_k$ (Théorème 2.3 et suite exacte (2.2)) ou vu dans $\mathrm{Gal}(F/k)$. Or $\mathfrak{t}$ gère les deux facteurs (classes et normique) dans le cadre habituel du corps de classes associé aux théorèmes de densité. Par contre, la succession des idéaux de $\mathcal{I}_i^n$ à $\mathcal{I}_{i+1}^n$ n'est pas algébriquement prévisible.

Pour l'aspect statistique sur la donnée numérique du corps k, il est impossible de s'affranchir du fait que la structure arithmétique de K/k commande les étapes de l'algorithme. D'où la nécessité de considérer des familles de corps k.

(ii) Sur un plan mathématique, on peut penser que la notion de complexité algorithmique de ce type de calculs (équations précédentes et passage à la limite dans la tour) dépend de phénomènes de transcendance (complexe et/ou p-adique) comme pour le cas de la conjecture de Leopoldt que l'on peut considérer comme de nature proche de celle du point de vue (b) ci-dessus sur la conjecture de Greenberg :

En effet, pour la conjecture de Leopoldt, la complexité repose sur les calculs, modulo p^n, des déterminants des développements p-adiques des logarithmes d'une unité de Minkowski du corps k et de ses conjuguées. Ici, les algorithmes sont liés

par la condition (triviale) de réduction modulo p^n du calcul modulo p^{n+h}, $h \geq 0$ (voir [9] pour l'étude des régulateurs p-adiques).

(iii) Par ailleurs, l'influence de la complexité arithmétique du corps de base k et celle de p (quant à son ordre de grandeur) sont manifestes comme le montrent les exemples suivants :

(a) Pour la conjecture de Leopoldt, on peut trouver des régulateurs p-adiques arbitrairement proches de 0 en prenant par exemple des corps quadratiques $k = \mathbb{Q}(\sqrt{m})$ avec $m = a^2 \cdot p^{2\rho} + 1$, supposé sans facteur carré, auquel cas l'unité fondamentale de k est $\varepsilon = a \cdot p^\rho + \sqrt{m}$ dont le logarithme p-adique est équivalent à p^ρ, et cependant la conjecture de Leopoldt est ici trivialement vraie. Par exemple, $\varepsilon = 3^{26} + \sqrt{m}$, où $m = 2 \cdot 17 \cdot 193 \cdot 1249 \cdot 13729 \cdot 475356961 \cdot 78046433784644296785447886881 = 1 + 3^{52}$, pour laquelle $\delta_3(\varepsilon) = 25$).

(b) Le cas de la conjecture de Greenberg est plus délicat, mais les aspects numériques dépendent essentiellement du groupe de torsion $\mathcal{T}_k$ (qui conjugue p-groupe des classes $\mathcal{C}\ell_k$ et régulateur p-adique normalisé $\mathcal{R}_k = U_k^*/\overline{E}_k$) ; en particulier, on sait [6, Théorèmes 4.7, 4.8, 4.10] que l'exposant p^e du groupe $U_k^*/\overline{E}_k$ est une première mesure de la complexité. Enfin, d'après [14], cette complexité est aussi mesurée par le comportement du *groupe des classes logarithmiques* de k dans k_∞.

(iv) Il faut ajouter que, comme pour la conjecture de Leopoldt, les algorithmes de dévissage relatifs à la conjecture de Greenberg ne sont pas indépendants par rapport à n (en effet, c'est la théorie d'Iwasawa qui structure leur ensemble à partir d'un rang fini, ainsi que la théorie du corps de classes qui indique par exemple que, pour tout $h \geq 0$, $\mathrm{N}_{k_{n+h}/k_n}(\mathcal{C}\ell_{k_{n+h}}) = \mathcal{C}\ell_{k_n}$).

Ce lien est exprimé par le fait que, pour $i \geq 1$ fixé et tout $h \geq 1$, modulo des normes globales convenables dans les extensions k_{n+h}/k (ce qui ne modifie pas les indices $(\Lambda_i^{n+h} : \Lambda_i^{n+h} \cap \mathrm{N}_{k_{n+h}/k}(k_{n+h}^\times))$), on peut obtenir, à partir du schéma de g-modules (cf. Théorème 3.2 & (3.1)) :

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & M_i^{n+h} & \longrightarrow & M^{n+h} & \xrightarrow{(1-\sigma_{n+h})^i} & (M^{n+h})^{(1-\sigma_{n+h})^i} & \longrightarrow & 1 \\
 & & \downarrow & & \mathrm{N}_{k_{n+h}/k_n}\downarrow & & \mathrm{N}_{k_{n+h}/k_n}\downarrow & & \\
1 & \longrightarrow & M_i^{n} & \longrightarrow & M^{n} & \xrightarrow{(1-\sigma_{n})^i} & (M^{n})^{(1-\sigma_{n})^i} & \longrightarrow & 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}
\tag{6.2}
$$

les relations d'inclusions suivantes [6, § 7.1, Schéma & Relation (7.1)] :

$$
\begin{aligned}
&\mathrm{N}_{k_{n+h}/k}(\mathcal{I}_i^{n+h}) \subseteq \cdots \subseteq \mathrm{N}_{k_{n+1}/k}(\mathcal{I}_i^{n+1}) \subseteq \mathrm{N}_{k_n/k}(\mathcal{I}_i^n) \\
&E_k \subseteq \Lambda_i^{n+h} \subseteq \cdots \subseteq \Lambda_i^{n+1} \subseteq \Lambda_i^n,
\end{aligned}
$$

qui font que, en particulier, le sous-groupe engendré par les composantes $\mathfrak{t}$ des normes d'idéaux à l'étape i est localement constant lorsque n croît. Ce résultat provient des flèches verticales (à gauche) :

$$\mathrm{N}_{k_{n+h}/k_n} : M_i^{n+h} \longrightarrow M_i^n,$$

qui ne sont a priori ni injectives ni surjectives, et que c'est à ce niveau que se trouve l'obstruction fondamentale à une preuve *algébrique* de la conjecture de Greenberg, parfois outrepassée dans la littérature. En effet, si la conjecture est vraie, pour tout n assez grand, les flèches précédentes sont des isomorphismes pour tout i puisqu'alors, les N_{k_{n+h}/k_n} sont des isomorphismes de g-modules.

Il y a donc un lien entre la complexité des algorithmes pour chaque n et les valeurs de λ et μ ; en raison de la nature des calculs on peut penser que de tels algorithmes ont une complexité semblable pour tout corps k et tout n, ceci étant renforcé par l'idée que les données numériques essentielles se lisent dans le corps de base.

7. Programmation de l'équation d'évolution – Exemples pour $p = 3$

7.1. **Programme général de recherche de $\mathfrak{A}$ tel que $(y) = \mathfrak{B} \cdot \mathfrak{A}^{1-\sigma}$.** Il est impossible de faire des statistiques avec K arbitrairement grand dans la tour. Nous allons cependant examiner, au moyen d'un programme, le principe général d'obtention de $\mathfrak{A} = \mathfrak{O}^\omega$ et $\mathrm{N}_{K/k}(\mathfrak{A}) = \mathrm{N}_{K/k}(\mathfrak{O}^\omega) = \mathfrak{q}^{\omega(1)}$ à partir de la relation (6.1) du § 6.1 $\mathrm{N}_{K/k}(y) = \mathrm{N}_{K/k}(\mathfrak{L}) = \mathfrak{l} =: (x)$, où $\mathfrak{l} \mid \ell$ est un idéal premier principal de k et où $x =: \eta_\ell$ est norme locale en p, donc norme globale dans l'extension K/k. Ici η_ℓ est donc la $\mathfrak{l}$-unité fondamentale (de valuation 1), déterminée à une unité près.

Nous nous limitons à prendre $K = k_1$, ce qui reste significatif car l'algorithme de filtration de $\mathcal{C}\ell_{k_1}$ reste non trivial ; en effet, si la formule de Chevalley donne un premier ordre de grandeur, rien n'exige que l'algorithme soit borné de façon effective.

Le programme général I, qui détermine la solution $y \in k_1^\times$ et la factorisation de $\mathfrak{A} = \mathfrak{O}^\omega$ dans $(y) = \mathfrak{L} \cdot \mathfrak{A}^{1-\sigma}$, se décompose en deux sous-programmes :

(i) le premier considère un idéal premier principal $\mathfrak{l} = (\eta_\ell)$ de k pour lequel η_ℓ est norme globale dans l'extension k_1/k ; on supposera ℓ totalement décomposé dans k_n/k, $n \geq 1$ (ici $n = 8$), donc, a fortiori, de la forme $\mathrm{N}_{k_1/k}(\mathfrak{L})$ pour $\mathfrak{L} \mid \mathfrak{l}$ dans k_1. Les résultats ne dépendent pas du choix de n, ce qui renforce les heuristiques.

(ii) le second utilise les η_ℓ précédents pour calculer (au moyen de la fonction rnfisnorminit de PARI dans l'extension relative k_1/k) $y \in k_1^\times$ tel que $(y) = \mathfrak{L} \cdot \mathfrak{A}^{1-\sigma}$, et donne la factorisation de l'idéal $\mathfrak{A} = \mathfrak{O}^\omega$ dont la norme $\mathfrak{q}^{\omega(1)}$ dans k_1/k contribue au pas suivant de l'algorithme.

7.1.1. *Programme I : Idéaux $\mathfrak{l} = (\eta_\ell)$ et $\mathfrak{A}$ tels que $(y) = \mathfrak{L} \cdot \mathfrak{A}^{1-\sigma}$.* On rappelle que $k = \mathbb{Q}(\sqrt{m})$, pour $m \equiv 1 \pmod 3$. La première partie du programme redonne les caractéristiques du corps k (nombre de classes h, unité fondamentale ε, S_k-unité fondamentale η_3, $\delta_{\mathfrak{p}}(\eta_3)$, $\delta_3(\varepsilon) \geq 1$, sous la forme $\frac{1}{3^{\delta_{\mathfrak{p}}(\eta_3)}}$, $\frac{1}{3^{\delta_3(\varepsilon)}}$) ; il calcule une liste de nombres premiers ℓ totalement décomposés dans $k_n/\mathbb{Q}$ tels que les idéaux premiers $\mathfrak{l} \mid \ell$ soient principaux de la forme (η_ℓ) où $\delta_3(\eta_\ell) \geq 1$ afin que η_ℓ soit partout norme locale dans k_1/k, donc norme globale.

On recherche les $\ell < \mathsf{B}$, $\ell \equiv \pm 1 \pmod{\mathsf{Mp} = 9}$ et $\mathfrak{l} = (\eta_\ell)$ dans k, où η_ℓ est calcué sous la forme $\mathsf{Mod}(\mathsf{a} * \mathsf{z} + \mathsf{b}, \mathsf{z}^2 - \mathsf{m})$, mais les $\delta_{\mathfrak{p}}(\eta_3)$ et $\delta_3(\varepsilon)$ nécessitent des calculs modulo une puissance de 3 suffisante. Il fournit les résultats suivants indiquant (ici pour $m = 67$) que $\delta_{\mathfrak{p}}(\eta_3) = 1$ et $\delta_3(\varepsilon) = 2$:

```
PB-NORMIQUE
m=67,h=1,E=5967*z+48842
p=3,Eta=z+8
1/3  1/9

List([67,9,List([991,883,487,379,953,773,683,557,251]),
Mod(4*z-9,z^2-67),Mod(31*z-252,z^2-67),Mod(-32*z+261,z^2-67),
Mod(5*z-36,z^2-67),Mod(4*z+45,z^2-67),Mod(-122*z+999,z^2-67),
Mod(18*z-145,z^2-67),Mod(-14*z-117,z^2-67),Mod(-45*z+368,z^2-67)])
```

La liste obtenue contient dans l'ordre, m, le nombre de ℓ trouvés, et enfin la liste des η_ℓ qui sera exploitée par la troisième partie du programme. La factorisation

de (y) se fait en définissant k_1 au moyen du polynôme irréductible R de $X = (\zeta_9 + \zeta_9^{-1}) \cdot \sqrt{m}$, où ζ_9 est une racine primitive 9-ième de l'unité :

$$R = x^6 - 6m\,x^4 + 9m^2x^2 - m^3.$$

On obtient (toujours avec $m = 67$) la factorisation de (y) en idéaux premiers, ce qui permet d'en déduire $\mathfrak{A}$ et $\mathrm{N}_{k_1/k}(\mathfrak{A})$:

```
================================================================================
{p=3;m=67;n=8;n0=n+1;B=10^5;y=z;Q=z^2-m;K=bnfinit(Q,1);
h=component(component(bnrinit(K,1),5),1);
E=component(component(component(K,8),5),1);
Su=bnfsunit(K,idealprimedec(K,p));
pi1=component(component(Su,1),1);
pi2=component(pi1,2)*z-component(pi1,1);
Pi1=pi1^n0;Pi2=pi2^n0;Z=bezout(Pi1,Pi2);
U1=component(Z,1);U2=component(Z,2);
Pk=y^2-Mod(m,p^n0);Y=Mod(y,Pk);z=Y;A1=eval(U1);A2=eval(U2);
B1=eval(Pi1);B2=eval(Pi2);b1=eval(pi1);b2=eval(pi2);e=eval(E);
XPpi=Mod(A1*B1+A2*B2*b2,Pk);XPe=Mod(A1*B1+A2*B2*e,Pk);
hs=norm(Mod(pi1,Q));h0=valuation(hs,p);vh0=valuation(h0,p);delta=vh-vh0;
npi=norm(XPpi)^(p-1);ne=norm(XPe)^(p-1);
zpi=znorder(npi)/p^n;ze=znorder(ne)/p^n;
if(delta!=0,print("PB-CLASSES"));if(zpi+ze<1,print("PB-NORMIQUE"));
print("m=",m," h=",h," E=",E);print("p=",p," Eta=",pi1);print(zpi," ",ze);

Mp=p^2;Nlist=0;list=List;listL=List;
for(t=-1,0,L=2*t+1;while(L<B,L=L+2*Mp;
if(isprime(L)==1 & kronecker(m,L)==1,
SuL=bnfsunit(K,idealprimedec(K,L));F=component(component(SuL,1),1);
Eta=Mod(F,Q);No=norm(Eta);vcl=valuation(No,L);
if(vcl==1,A=(Mod(F,Q)^2-1)/3;v=valuation(A,3);
if(v>=1,Nlist=Nlist+1;listinsert(listL,L,1);listinsert(list,Eta,1))))));
listinsert(list,m,1);listinsert(list,Nlist,2);listinsert(list,listL,3);
print(list);

bnf=bnfinit(y^2-m);PK=polsubcyclo(9,3)+Mod(0,bnf.pol);
T=rnfisnorminit(bnf,PK,1);R=x^6-6*m*x^4+9*m^2*x^2-m^3;K=nfinit(R);
X=Mod(x,R);racm=m^2/(3*m*X-X^3);z=X^2/m-2;
for(j=1,Nlist,Z=component(list,j+3);ZZ=component(Z,2);
ZZ1=component(ZZ,1);ZZ2=component(ZZ,2);Z=Mod(ZZ1+ZZ2*y,y^2-m);
N=rnfisnorm(T,Z);nu=component(N,2);
if(nu==1,Y0=component(N,1);S=component(Y0,2);
S0=component(S,1);S1=component(S,2);S2=component(S,3);
if(S2==0,a1=0;a0=0);if(S2!=0,s2=component(S2,2);
a0=component(s2,1);a1=component(s2,2));
if(S1==0,b1=0;b0=0);if(S1!=0,s1=component(S1,2);
b0=component(s1,1);b1=component(s1,2));
if(S0==0,c1=0;c0=0);if(S0!=0,s0=component(S0,2);
c0=component(s0,1);c1=component(s0,2));
YY=(a1*racm+a0)*z^2+(b1*racm+b0)*z+c1*racm+c0;F=idealfactor(K,YY);
L=component(listL,j);print(" ");print(L);print(F) ));z=y}
================================================================================
```

La factorisation indique chaque idéal premier avec la donnée d'une $\mathbb{Z}$-base et, à l'extrémité droite, l'exposant de l'idéal ; la norme de l'idéal est le premier entier à gauche ; l'idéal $\mathfrak{L}$, qui figure par hypothèse, est listé en dernier. On obtient par exemple la décomposition triviale (i.e., $\mathfrak{A} = 1$) :

```
Mat([[991,[145,0,0,0,1,0]~,1,1,[385,-256,182,-61,334,-466]~],1])
```

qui décrit un idéal principal $\mathfrak{L}$ de k_1 au-dessus de $\ell = 991$. Ensuite on a, par exemple, une factorisation de la forme :

```
[[181,[-55,0,0,0,1,0]~,1,1,[-84,37,11,-9,88,-36]~],1;
[181,[-7,0,0,0,1,0]~,1,1,[-34,-45,-71,61,-63,-36]~],-1;
[487,[-110,0,0,0,1,0]~,1,1,[196,51,-28,226,-135,106]~],1]
```

qui décrit le produit de l'idéal premier $\mathfrak{L}$ au-dessus de 487 par $\mathfrak{Q}^{1-\sigma}$, où $\mathfrak{Q}$ est un idéal premier au-dessus d'un idéal $\mathfrak{q}$ de k divisant $q = 181$ choisi par PARI.

En résumé, on obtient, pour $m = 67$, les factorisations relatives à la liste des ℓ précédente :

```
l=991:
Mat([[991,[145,0,0,0,1,0]~,1,1,[385,-256,182,-61,334,-466]~],1])
l=883:
Mat([[883,[-395,0,0,0,1,0]~,1,1,[67,287,91,-236,-207,74]~],1])
l=487:
[[181,[-55,0,0,0,1,0]~,1,1,[-84,37,11,-9,88,-36]~],1;
[181,[-7,0,0,0,1,0]~,1,1,[-34,-45,-71,61,-63,-36]~],-1;
[487,[-110,0,0,0,1,0]~,1,1,[196,51,-28,226,-135,106]~],1]
l=379:
[[181,[-55,0,0,0,1,0]~,1,1,[-84,37,11,-9,88,-36]~],1;
[181,[-7,0,0,0,1,0]~,1,1,[-34,-45,-71,61,-63,-36]~],-1;
[379,[129,0,0,0,1,0]~,1,1,[-141,1,31,-12,-137,-59]~],1]
l=953:
[[181,[-55,0,0,0,1,0]~,1,1,[-84,37,11,-9,88,-36]~],2;
[181,[-7,0,0,0,1,0]~,1,1,[-34,-45,-71,61,-63,-36]~],-2;
[953,[-53,0,0,0,1,0]~,1,1,[202,374,-333,-215,-115,-276]~],1]
l=773:
Mat([[773,[-145,0,0,0,1,0]~,1,1,[-14,277,39,-355,343,-149]~],1])
l=683:
[[181,[-55,0,0,0,1,0]~,1,1,[-84,37,11,-9,88,-36]~],1;
[181,[-7,0,0,0,1,0]~,1,1,[-34,-45,-71,61,-63,-36]~],-1;
[683,[-240,0,0,0,1,0]~,1,1,[339,41,269,-141,-283,-292]~],1]
l=557:
[[181,[-55,0,0,0,1,0]~,1,1,[-84,37,11,-9,88,-36]~],1;
[181,[-7,0,0,0,1,0]~,1,1,[-34,-45,-71,61,-63,-36]~],-1;
[557,[-30,0,0,0,1,0]~,1,1,[-67,112,-124,111,-277,33]~],1]
l=251:
[[181,[-55,0,0,0,1,0]~,1,1,[-84,37,11,-9,88,-36]~],1;
[181,[-7,0,0,0,1,0]~,1,1,[-34,-45,-71,61,-63,-36]~],-1;
[251,[5,0,0,0,1,0]~,1,1,[-63,120,-106,-53,89,-29]~],1]
```

On constate que PARI utilise bien le même idéal premier $\mathfrak{Q} \mid 181$, ici avec $\omega = f$, $f \in \{0, 1, 2\}$, de sorte que $\mathfrak{A}$ est égal à $\mathfrak{Q}^0 = (1)$ ou à $\mathfrak{Q}$ ou à $\mathfrak{Q}^2$. Les 3 cas se présentent effectivement.

7.1.2. *Programme II : Idéaux $\mathfrak{A}$ tels que $(y) = \mathfrak{A}^{1-\sigma}$ & $\mathrm{N}_{k_1/k}(y) = \varepsilon$.* C'est un cas particulier du programme précédent qui permet de trouver les classes ambiges, autres que celles des idéaux invariants, et les $\delta_3(x)$, $x \in \Lambda_1^1$, très importants pour la suite de l'algorithme. On résoud l'équation $\mathrm{N}_{k_1/k}(y) = \varepsilon$ qui a toujours une solution dans la mesure où l'on suppose $\delta_3(\varepsilon) \geq 1$; on donne aussi la structure de $\mathcal{C}\ell_{k_1}$:

```
================================================================================
{m=67;bnf=bnfinit(y^2-m);E=component(component(component(bnf,8),5),1);
E=Mod(E,y^2-m);PK=polsubcyclo(9,3)+Mod(0,bnf.pol);
T=rnfisnorminit(bnf,PK,1);R=x^6-6*m*x^4+9*m^2*x^2-m^3;K=nfinit(R);
X=Mod(x,R);racm=m^2/(3*m*X-X^3);z=X^2/m-2;
N=rnfisnorm(T,E);nu=component(N,2);if(nu==1,Y=component(N,1);
S=component(Y,2);S0=component(S,1);S1=component(S,2);
S2=component(S,3);if(S2==0,a1=0;a0=0);if(S2!=0,s2=component(S2,2);
```

```
a0=component(s2,1);a1=component(s2,2));if(S1==0,b1=0;b0=0);
if(S1!=0,s1=component(S1,2);b0=component(s1,1);b1=component(s1,2));
if(S0==0,c1=0;c0=0);if(S0!=0,s0=component(S0,2);
c0=component(s0,1);c1=component(s0,2));
YY=(a1*racm+a0)*z^2+(b1*racm+b0)*z+c1*racm+c0;F=idealfactor(K,YY);print(Y);
print(F));H=bnrinit(bnfinit(R,1),1);print("structure=",component(H,5))}
==========================================================================
```

(i) Pour $m = 67$ ($h = 1, \delta_{\mathfrak{p}}(\eta_3) = 1, \delta_3(\varepsilon) = 2$, $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/3\mathbb{Z}$), y est :

```
Mod(Mod(872/181*y+7113/181,y^2-67)*x^2+Mod(104/181*y+850/181,y^2-67)*x
+Mod(-2313/181*y-18873/181,y^2-67),x^3-3*x+Mod(1,y^2-67))
```

L'idéal $\mathfrak{A}$ est l'idéal premier :

```
[181,[7,0,0,0,1,0]~,1,1,[34,45,71,61,-63,-36]~]
```

On vérifie que $181 = \mathrm{N}_{k/\mathbb{Q}}(3\sqrt{67}+28)$ pour lequel $\delta_3(3\sqrt{67}+28) = 0$. On a $M_1^1 = 3$ d'ordre 3, engendré par S_k et $\mathfrak{A}$; or $\mathrm{N}_{k_1/k}(M_1^1) = 1$ et $\Lambda_1^1 = \langle \varepsilon, \eta_3, 3\sqrt{67} + 28\rangle$ qui stope l'algorithme.

(ii) Pour $m = 6559$ ($h = 18, \delta_{\mathfrak{p}}(\eta_3) = 1, \delta_3(\varepsilon) = 3$, $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$), y est :

```
Mod(Mod(2603286587676/74632321*y-210708142484324/74632321,y^2-6559)*x^2
+Mod(904557609272/74632321*y-73082414174026/74632321,y^2-6559)*x
+Mod(-7493532286573/74632321*y+606807427105320/74632321,y^2-6559),
                                                    x^3-3*x+Mod(1,y^2-6559))
```

et l'idéal $\mathfrak{A}^{1-\sigma}$ est le produit :

```
[[53,[-9,0,0,0,1,0]~,1,1,[25,-11,-16,-3,-22,10]~],-2;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;
[163,[-49,0,0,0,1,0]~,1,1,[16,-52,38,23,-34,54]~],-2;
[163,[-41,0,0,0,1,0]~,1,1,[-35,22,-68,-21,-52,54]~],1;
[163,[-8,0,0,0,1,0]~,1,1,[-5,33,-57,-3,-78,54]~],-1;
[163,[8,0,0,0,1,0]~,1,1,[5,-33,57,-3,-78,54]~],2]
```

pour lequel il faudra déterminer les conjugaisons pour trouver ω.

(iii) Pour $m = 3259$ ($h = 1, \delta_{\mathfrak{p}}(\eta_3) = 0, \delta_3(\varepsilon) = 4$, $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/3\mathbb{Z}$), on trouve $\mathfrak{A} = (1)$ qui montre que ε est norme de l'unité de k_1 :

```
Mod(Mod(-4954528488777941091542720*y-28284239771961302173706384,y^2-3259)*x^2
+Mod(9311332184277189364259520*y+53156209050568241456130896,y^2-3259)*x
+Mod(-2636041891494632186254990*y-15048544190803267053864318,y^2-3259),
                                                    x^3-3*x+Mod(1,y^2-3259))
```

et par conséquent, les classes ambiges sont les classes des idéaux invariants, donc de S_k puisque $h = 1$. Or $\#M_1^1 = 3$, et comme $\Lambda_1^1 = \langle \varepsilon, \eta_3\rangle$ avec $\delta_{\mathfrak{p}}(\eta_3) = 0$, l'algorithme stope, ce qui est cohérent avec $\#\mathcal{C}\ell_{k_1} = 3$.

(iv) Pour $m = 1867$ ($h = 1, \delta_{\mathfrak{p}}(\eta_3) = 1, \delta_3(\varepsilon) = 5$, $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/3\mathbb{Z}$), on obtient respectivement pour y et $\mathfrak{A}$:

```
Mod(Mod(488982/107*y+21128286/107,y^2-1867)*x^2
+Mod(-778797/107*y-33650892/107,y^2-1867)*x
+Mod(442398/107*y+19115590/107,y^2-1867),x^3-3*x+Mod(1,y^2-1867))

[107,[40,0,0,0,1,0]~,1,1,[-16,36,-33,24,53,-50]~],1
```

où $\mathrm{N}_{k/\mathbb{Q}}(34086\sqrt{m} + 1472815) = -107$ et $\delta_3(34086\sqrt{m} + 1472815) = 0$.

Certains de ces exemples donnent au premier stade Λ_1^1 des $\delta_3(x)$ qui stopent l'algorithme ($m = 67, 3259, 1867$ pour lesquels $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/3\mathbb{Z}$).

7.2. **Evolution de la i-suite $\#(M^1_{i+1}/M^1_i)$ pour $k=\mathbb{Q}(\sqrt{6559})$.** Ce cas est particulièrement intéressant en raison du groupe de classes cyclique d'ordre 9 et du régulateur 3-adique normalisé $\#\mathcal{R}_k = 27$, ce qui donne un groupe $\mathcal{T}_k$ d'ordre 3^5, donc une grande variété de décompositions ; en outre, on a $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

7.2.1. *Utilisation du programme I, § 7.1.1.* Il donne les résultats suivants pour un ensemble de premiers ℓ totalement décomposés dans $k_1/\mathbb{Q}$ et tels que $\mathfrak{l}=(\eta_\ell)$ dans k :

```
PB-NORMIQUE
m=6559,h=18,E=81*z+6560
p=3,Eta=379*z-30694
1/3  1/27
```

indiquant que $\delta_{\mathfrak{p}}(\eta_3)=1$ et $\delta_3(\varepsilon)=3$. Noter que $\mathcal{C}\ell_k$ est engendré par $\mathfrak{p} \mid 3$.

On obtient la liste suivante des η_ℓ dans la troisième composante de la variable list :

```
List([6559,25,
List([92179,86239,70327,68743,58321,48907,47143,40519,30781,
28279,25237,12547,8011,1621,96461,96263,89009,88001,84653,
82457,77003,37781,27179,16361,2267]),

Mod(-70*z+5661,z^2-6559),Mod(65*z+5256,z^2-6559),Mod(-52*z+4203,z^2-6559),
Mod(16*z+1269,z^2-6559),Mod(-135*z-10936,z^2-6559),Mod(7*z-522,z^2-6559),
Mod(11*z-864,z^2-6559),Mod(29*z+2340,z^2-6559),Mod(-90*z-7291,z^2-6559),
Mod(20*z+1611,z^2-6559),Mod(9*z-746,z^2-6559),Mod(-2*z-117,z^2-6559),
Mod(-2*z-135,z^2-6559),Mod(-9*z-730,z^2-6559),Mod(61*z-4950,z^2-6559),
Mod(36*z+2899,z^2-6559),Mod(-20*z-1647,z^2-6559),Mod(-56*z-4545,z^2-6559),
Mod(-2*z-333,z^2-6559),Mod(11*z+936,z^2-6559),Mod(9*z+674,z^2-6559),
Mod(25*z-2034,z^2-6559),Mod(9*z+710,z^2-6559),Mod(-11*z-900,z^2-6559),
Mod(18*z+1457,z^2-6559)])
```

7.2.2. *Décomposition de (y) en idéaux, pour $k=\mathbb{Q}(\sqrt{6559})$.* Le Programme I du § 7.1.1 donne la solution $y \in k_1^\times$ telle que $\mathrm{N}_{k_1/k}(y)=\eta_\ell$ et la décomposition en idéaux de (y) ; le nombre $y \in k_1^\times$ (identifié par Y dans le programme) est décrit par PARI en termes polynomiaux (variables x et y, modulo y^2-m pour $k/\mathbb{Q}$ et modulo $x^3-3\,x+1$ pour l'extension k_1/k).

Par exemple, pour $\ell=86239$ et $\eta_\ell = 65\cdot\sqrt{m}+5256$ de norme ℓ, on a :

```
Y=Mod(Mod(10360342980398669850079376181283586668 7
                    87383048223271972729347563998405 29/418195493*y
-83905986619450594430758729898826369064512 49
                    97336879805688990412175278787 70/418195493,y^2-6559)*x^2
+Mod(-19471075694983430251815098361774199857 0
                    94130360149521202046343715858993 10/418195493*y
+15769167293211778079551042284522907830683899
                    94794690606318510018653360378 74/418195493,y^2-6559)*x
+Mod(55126233574835545800719913475586793 9
                    76450485647712522109931039905572 5544/418195493*y
-44645442969040311582101175795304512633193 33
                453086982650815899126340477136 0/418195493,y^2-6559),
                                                x^3-3*x+Mod(1,y^2-6559))
```

On aura en général $(y)=\mathfrak{L}\cdot\mathfrak{Q}^{\omega\cdot(1-\sigma)}$, $\omega \in \mathbb{Z}[\mathrm{Gal}(k_1/\mathbb{Q})]$, où $\mathrm{Gal}(k_1/\mathbb{Q})$ est engendré par σ d'ordre 3 et τ d'ordre 2. Le programme donne de fait le produit $\Omega := \omega\cdot(1-\sigma)$ effectué.

On obtient des résultats montrant le caractère aléatoire de Ω, dont les coefficients sont dans l'intervalle $[-9,+9]$ et où l'idéal $\mathfrak{A}=\mathfrak{Q}^\Omega$ est tel que $\mathfrak{Q} \mid 53$ où $\mathrm{N}_{k_1/k}(\mathfrak{Q})=$

$\mathfrak{q}$ dont la classe est d'ordre 9 (on rappelle que les $\ell \equiv \pm 1 \pmod{81}$ sont classés selon les deux congruences, par ordres décroissants, et que les $\mathfrak{l}$-unités η_ℓ sont données au § 7.2.1). On observe en particulier 2 cas d'idéaux $\mathfrak{Q}^\omega$ triviaux (donc lorsque l'idéal $\mathfrak{L}$ de k_1 est principal égal à y) :

```
1621
Mat([[1621,[-62,0,0,0,1,0]~,1,1,[119,-637,235,621,776,762]~],1])

27179
Mat([[27179,[-5996,0,0,0,1,0]~,1,1,[10104,8864,-2451,5717,-5400,-3876]~],1])
```

Mais trouver ω nécessite d'identifier numériquement les conjugués de $\mathfrak{Q}$.

7.2.3. *Détermination de* $\mathrm{Gal}(k_1/\mathbb{Q})$ *pour* $k = \mathbb{Q}(\sqrt{6559})$. On obtient, relativement au polynôme $R = x^6 - 39354\,x^4 + 387184329\,x^2 - 282171334879$, et en utilisant nfgaloisconj :

$$\begin{aligned}
\tau &\text{ défini par } x \mapsto -x,\\
\sigma &\text{ défini par } x \mapsto -1/43020481\,x^5 + 5/6559\,x^3 - 6\,x,\\
\tau\cdot\sigma^2 &\text{ défini par } x \mapsto -1/43020481\,x^5 + 5/6559\,x^3 - 5\,x,\\
\sigma^2 &\text{ défini par } x \mapsto 1/43020481\,x^5 - 5/6559\,x^3 + 5\,x,\\
\tau\cdot\sigma &\text{ défini par } x \mapsto 1/43020481\,x^5 - 5/6559\,x^3 + 6\,x.
\end{aligned}$$

On a alors calculé, dans l'ordre $1, \tau, \sigma, \tau\cdot\sigma^2, \sigma^2, \tau\cdot\sigma$, les conjugués correspondants de y et sa décomposition en idéaux, ce qui permet d'identifier les conjugués de l'idéal $\mathfrak{L}$ et de trouver Ω ; on se base une fois pour toutes sur le y obtenu pour $\ell = 28279$:

```
Id(y):
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],3;      Q1
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],4;         Q2
[53,[2,0,0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-2;    tau(Q2)
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;   tau(Q1)
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-7;        Q3
[28279,[3506,0,0,0,1,0]~,1,1,[356,7859,1221,-1277,3345,8122]~],1]

tau(y):
[[53,[-9,0,0,0,1,0]~,1,1,[25,-11,-16,-3,-22,10]~],-7;  tau(Q3)
[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],2;        Q1
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],-2;         Q2
[53,[2,0,0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],4;      tau(Q2)
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],3;    tau(Q1)
[28279,[-3506,0,0,0,1,0]~,1,1,[-356,-7859,-1221,-1277,3345,8122]~],1]

sigma(y):
[[53,[-9,0,0,0,1,0]~,1,1,[25,-11,-16,-3,-22,10]~],-2;  tau(Q3)
[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],-7;       Q1
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],3;          Q2
[53,[2,0,0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],2;      tau(Q2)
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],4;          Q3
[28279,[-7370,0,0,0,1,0]~,1,1,[5417,-865,-7503,12899,3500,8122]~],1]

tau.sigma^2(y):
[[53,[-9,0,0,0,1,0]~,1,1,[25,-11,-16,-3,-22,10]~],3;  tau(Q3)
[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],-2;       Q1
[53,[2,0,0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-7;     tau(Q2)
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],4;    tau(Q1)
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],2;          Q3
[28279,[-3864,0,0,0,1,0]~,1,1,[14138,-12920,-6282,12744,-10758,8122]~],1]
```

```
sigma^2(y):
[[53,[-9,0,0,0,1,0]~,1,1,[25,-11,-16,-3,-22,10]~],2;  tau(Q3)
[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],4;       Q1
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],-7;        Q2
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],-2;  tau(Q1)
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],3;         Q3
[28279,[3864,0,0,0,1,0]~,1,1,[-14138,12920,6282,12744,-10758,8122]~],1]

tau.sigma(y):
[[53,[-9,0,0,0,1,0]~,1,1,[25,-11,-16,-3,-22,10]~],4;  tau(Q3)
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],2;         Q2
[53,[2,0,0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],3;     tau(Q2)
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],-7;  tau(Q1)
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-2;        Q3
[28279,[7370,0,0,0,1,0]~,1,1,[-5417,865,7503,12899,3500,8122]~],1]
```

Ceci identifie les relations de conjugaison à partir de $\mathfrak{Q}_1$:

$$\mathfrak{Q}_1, \quad \mathfrak{Q}_1^{\sigma} = \mathfrak{Q}_2, \quad \mathfrak{Q}_1^{\sigma^2} = \mathfrak{Q}_3.$$

D'où, pour le cas de $\ell = 28279$, $\Omega = 3 + 2\tau + (4 - 2\tau)\sigma - 7\sigma^2$, puis $\omega = 7\sigma + 2\tau + 3$ et $\omega(1) = 10 + 2\tau$. Mais comme $\mathfrak{q}^{1+\tau} = (53)$, on obtiendra $\mathrm{N}_{k_1/k}(\mathfrak{A}) = (53)^2 \cdot \mathfrak{q}^8$; or la classe de $\mathfrak{q}$ est d'ordre 9, avec :

$$\mathfrak{q}^9 = (416167\sqrt{6559} + 66601422) \ \ \& \ \ \delta_3(416167\sqrt{6559} + 66601422) = 1.$$

Pour $\ell = 82457$, on obtient :

```
l=82457:
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],2;   Q1
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-2;     Q3
[82457,[-11462,0,0,0,1,0]~,1,1,[-12743,-34335,-22650,2405,35275,-22073]~],1]
```

qui conduit à $\omega(1) = 4$.

Pour $\ell = 2267$, il vient :

```
l=2267:
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],3;    Q1
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],1;       Q2
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-1; tau(Q2)
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],1; tau(Q1)
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-4;     Q3
[2267,[855,0,0,0,1,0]~,1,1,[433,150,-991,-60,-759,-378]~],1]
```

d'où $\omega = 4\sigma + 3 + \tau$, $\omega(1) = 7 + \tau$, et $\mathrm{N}_{k_1/k}(\mathfrak{A}) = (53) \cdot \mathfrak{q}^6$, qui donne une classe d'ordre 3.

Pour $\ell = 8011$ on obtient :

```
l=8011:
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],4;    Q1
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],3;       Q2
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-2; tau(Q2)
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2; tau(Q1)
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-7;     Q3
[8011,[-2063,0,0,0,1,0]~,1,1,[-2011,-1995,2900,979,-3590,1411]~],1]
```

pour lequel $\omega = 7\sigma + 4 + 2\tau$, $\omega(1) = 11 + 2\tau = 9 + 2(1 + \tau)$ qui conduit à l'idéal principal $\mathrm{N}_{k_1/k}(\mathfrak{A}) = (53)^2 \cdot \mathfrak{q}^9$.

Par conséquent, tous les cas intéressants de ω sont obtenus, ce qui suggère la répartition uniforme de la composante $\mathscr{cl}_k(\mathfrak{t})$ dans $\mathscr{Cl}_k$ relativement à la décomposition de $\mathrm{N}_{k_1/k}(\mathfrak{A})$ (Théorème 2.3).

7.2.4. *Evolution du facteur normique pour* $\mathbb{Q}(\sqrt{6559})$. Le 3-groupe des classes du corps $k^* = \mathbb{Q}(\sqrt{-3 \cdot 6559})$ est $\mathcal{C}\ell_{k^*} \simeq (\mathbb{Z}/3\,\mathbb{Z})^2$, ce qui fait que deux pseudo-unités 3-primaires indépendantes dans k sont nécessaires ; ceci explique que, outre l'unité fondamentale, tout a étranger à 3, tel que $(a) = \mathfrak{a}^3$, vérifie nécessairement $\delta_3(a) \geq 1$ (cas analogue au cas de $m = 10942$ du § 5.3).

Considérons le groupe des classes ambiges M_1^1 d'ordre 27 ; il est engendré par les classes de $\mathfrak{P} \mid 3$ dans k_1 et de $\mathfrak{A} = \mathfrak{Q}_{53}^{-2} \cdot \mathfrak{Q}_{163}^{-2+(\tau-2)\cdot\sigma}$ provenant de la résolution de $\varepsilon = \mathrm{N}_{k_1/k}(y)$ (Programme II), après identification des conjugués et utilisation de $\mathfrak{A}^{1-\sigma}$ donné par :

```
[[53,[-9,0,0,0,1,0]~,1,1,[25,-11,-16,-3,-22,10]~],-2;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;
[163,[-49,0,0,0,1,0]~,1,1,[16,-52,38,23,-34,54]~],-2;
[163,[-41,0,0,0,1,0]~,1,1,[-35,22,-68,-21,-52,54]~],1;
[163,[-8,0,0,0,1,0]~,1,1,[-5,33,-57,-3,-78,54]~],-1;
[163,[8,0,0,0,1,0]~,1,1,[5,-33,57,-3,-78,54]~],2]
```

On remarque que $(\sqrt{6559}+80) = \mathfrak{p} \cdot \mathfrak{q}_{53}$; par conséquent $\mathfrak{q}_{53}$ et $\mathfrak{q}_{163}$ sont équivalents à une puissance de $\mathfrak{p}$. Donc $\mathrm{N}_{k_1/k}(M_1^1)$ est engendré par les classes dans k de $\mathfrak{p} \mid 3$ (car $\mathcal{C}\ell_k(\mathfrak{p})$ engendre $\mathcal{C}\ell_k$), de $\mathfrak{q}_{53}$ et $\mathfrak{q}_{163}$ (rajoutés par commodité). On trouve avec PARI un $y \in k_1$ qui a pour norme relative le nombre entier $x \in k$ suivant :

```
Mod(6832355788476479176909088393511957025*y
                    -131997425842264293218558754198040661024,y^2-6559)
```

de norme $-3^3 \cdot 53^{21} \cdot 163^{18}$, dont la décomposition en idéaux est :

```
[[3,[1,1]~,1,1,[-1,1]~]3]          P3
[[53,[26,1]~,1,1,[-26,1]~]21]      Q53
[[163,[56,1]~,1,1,[-56,1]~]18]     Q163
```

et qui fournit une élément de Λ_1^1 norme dans k_1/k (le symbole de Hasse de x, non étranger à 3, est de calcul plus complexe ; y pourrait permettre le pas suivant de l'algorithme). Donc $\#(M_2^1/M_1^1) = 3$ car le facteur classes a été trivialisé puisque $\mathrm{N}_{k_1/k}(M_1^1) = \mathcal{C}\ell_k$. D'où $\#M_2^1 = 81$, et comme PARI donne $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, on a fin de l'algorithme (normalement on devrait déterminer M_3^1/M_2^1 à partir du calcul de Λ_2^1 pour constater la fin).

7.2.5. *Remarques sur l'algorithme pour* $\mathbb{Q}(\sqrt{6559})$. (i) On vérifie que pour $k = \mathbb{Q}(\sqrt{6559})$ le 3-groupe des classes de k_2 est isomorphe à $\mathbb{Z}/27\,\mathbb{Z} \times \mathbb{Z}/9\,\mathbb{Z}$. Le temps de calcul devient important et il semble illusoire d'effectuer les calculs précédents dans k_2/k.

(ii) On rappelle, d'après [6, Théorème 4.7], que l'exposant 3^e de $U_k^*/\overline{E}_k$ indique l'étage (ici égal à $e = 3$) à partir duquel le nombre de classes ambiges dans k_n/k est égal à $\#\mathcal{T}_k = 3^5$ pour tout $n \geq e$. Nous ignorons si la stabilisation s'effectue à l'étage 3, mais il est normal que le 3-groupe des classes croisse au moins jusqu'à l'ordre 3^5.

Au-delà de cette borne, on aura $\#M_2^n = 3^{e_1^n} \cdot \#M_1^n = 3^{e_1^n} \cdot 3^5$, où $e_1^n \in \{0, 1\}$ ne dépend que du facteur normique selon les modalités abordées au niveau $n = 1$.

(iii) Comme pour tous les $h \geq 0$, les normes $\mathrm{N}_{k_{n+h}/k_n} : \mathcal{C}\ell_{k_{n+h}} \longrightarrow \mathcal{C}\ell_{k_n}$ sont surjectives, $\#\mathcal{C}\ell_{k_n}$ est fonction croissante de n, mais avec la contrainte $\#M_1^n = \#\mathcal{C}\ell_{k_n}^{\mathrm{Gal}(k_n/k)} = 3^5$ pour tout $n \geq 3$ et le fait, rappelé à la fin de la Section 1, que la i-suite des $\#(M_{i+1}^n/M_i^n) =: 3^{c_i^n+\rho_i^n}$ est décroissante à partir de $\#M_1^n = 3^5$, stationnaire, de limite un diviseur de $\#\mathcal{T}_k$.

Pour $m = 6559$ où $\mathrm{N}_{k_n/k}(S_{k_n}) = S_k$ engendre $\mathcal{C}\ell_k$, le facteur classes est toujours trivialisé et tout dépend de la i-suite décroissante $3^{\rho_i^n} \mid (U_k^* : \overline{E}_k) = 3^3$.

8. Descente galoisienne de $\mathcal{T}_k$ via $\mathrm{Gal}(F/k)$

Bien que la descente galoisienne de $H_k^{\rm pr}/k_\infty$, en F/k, ne soit pas nécessaire au plan théorique, donnons d'abord un exemple numérique montrant le caractère « fini explicite » des conditions de répartition des symboles d'Artin $\left(\frac{F/k}{\mathrm{N}_{k_n/k}(\mathfrak{A})}\right)$ des normes $\mathrm{N}_{k_n/k}(\mathfrak{A})$ dans la tour cyclotomique. Ensuite nous montrerons que cette répartition des symboles d'Artin ne dépend pas du choix de F qui, en un sens, définit un « corps gouvernant » pour la conjecture de Greenberg.

8.1. **L'extension F/k pour $k=\mathbb{Q}(\sqrt{1714})$, $p=3$.** Pour $m=1714$ et $p=3$, le programme du § 4.3 permet de montrer que $\mathcal{T}_k\simeq\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ avec $\mathcal{C}\ell_k\simeq\mathbb{Z}/3\mathbb{Z}$; le corps $k^*=\mathbb{Q}(\sqrt{-3\cdot m})$ a un 3-groupe des classes isomorphe à $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ et il existe $\alpha,\beta\in k^*$, cubes d'idéaux non principaux, tels que α soit par exemple 3-primaire pour engendrer l'extension de Kummer non ramifiée $H_k(\mu_3)=k(\mu_3)(\sqrt[3]{\alpha})$, β donnant une extension cyclique de degré 3 ramifiée en 3.

Rappelons que si $(\gamma)=\mathfrak{c}^3$ dans k^*, avec $\mathrm{N}_{k^*/\mathbb{Q}}(\gamma)=N_\gamma^3$ et $\mathrm{Tr}_{k^*/\mathbb{Q}}(\gamma)=T_\gamma$, alors l'extension cyclique de degré 3 de k qui lui correspond est donnée par le polynôme :

$$P_\gamma=x^3-3\,N_\gamma\cdot x-T_\gamma.$$

On obtient les données suivantes :

$$\alpha=2593+15\cdot\sqrt{-5142},\quad\text{avec } N_\alpha=199,$$
$$\beta=157+\sqrt{-5142},\qquad\text{avec } N_\beta=31,$$

$P_\alpha=x^3-3\cdot199\,x-2\cdot2593$ (non ramification sur k), $P_\beta=x^3-3\cdot31\,x-2\cdot157$ (ramification en 3) ; en utilisant :

$$\mathsf{polcompositum}(\mathsf{x}^3-3*199*\mathsf{x}-2*2593,\mathsf{x}^3-3*31*\mathsf{x}-2*157),$$

on obtient que F est engendrée sur k par une racine de :

```
x^9-2070*x^7+14616*x^6+1261737*x^5-17516520*x^4-136713960*x^3
                                  +3712697856*x^2-22102948224*x+40749585408
```

pour lequel on vérifie que $D_{F/\mathbb{Q}}=D_k^9\cdot3^{27}$. Ainsi le symbole d'Artin d'un idéal premier $\mathfrak{L}$ (par exemple totalement décomposé) de k_n, obtenu au cours de l'algorithme, se lit sur la décomposition, dans F/k, de l'idéal $\mathfrak{l}$ de k au-dessous de $\mathfrak{L}$. Plus généralement les symboles des $\mathrm{N}_{k_n/k}(\mathfrak{A})$ en résultent.

8.2. **Invariance par rapport au choix de F/k.** L'extension F/k n'est pas unique mais on a le résultat suivant qui conforte ces questions d'ordre heuristique et numérique :

Théorème 8.1. *L'étude statistique des symboles d'Artin $(\frac{F/k}{\mathrm{N}_{k_n/k}(\mathfrak{A})})$, où les idéaux $\mathfrak{A}$ sont obtenus dans l'algorithme de dévissage dans k_n, est intrinsèque pour tout n assez grand et ne dépend pas du choix de F.*

Démonstration. Soit F'/k une autre solution ; alors en se référant aux expressions du Théorème 2.3, il vient, avec des notations évidentes pour F et F', $\mathrm{N}_{K/k}(\mathfrak{A})=\mathfrak{a}^{p^n}\cdot\mathfrak{t}\cdot(x_\infty)=\mathfrak{a}'^{p^n}\cdot\mathfrak{t}'\cdot(x'_\infty)$, ce qui conduit, dès que n est assez grand, à $\mathfrak{t}'\cdot\mathfrak{t}^{-1}=(z)$, où l'image de z dans U_k est arbitrairement proche de 1. Comme $\mathfrak{t}$ et $\mathfrak{t}'$ sont d'ordre fini modulo $\mathcal{P}_{k,\infty}$, on obtient, pour $e'\geq0$ convenable, $\mathfrak{t}'^{p^{e'}}\cdot\mathfrak{t}^{-p^{e'}}=(z^{p^{e'}})=(t_\infty)\in\mathcal{P}_{k,\infty}$. Donc $z^{p^{e'}}=t_\infty\cdot\varepsilon$, $\varepsilon\in E_k\otimes\mathbb{Z}_p$ d'image arbitrairement proche de 1 dans U_k, donc de la forme $\varepsilon'^{p^{e'}}$, $\varepsilon'\in E_k\otimes\mathbb{Z}_p$ (conjecture de Leopoldt), ce qui fait que $z':=z\cdot\varepsilon'^{-1}$

est tel que $z'^{p^{e'}} = t_\infty$. L'image de z' dans U_k est dans $\mathrm{tor}_{\mathbb{Z}_p}(U_k) = 1$ et z' est infinitésimal (cf. § 2). D'où $(z) = (z') \in \mathcal{P}_{k,\infty}$ et $\mathfrak{t}' \cdot \mathfrak{t}^{-1} \in \mathcal{P}_{k,\infty}$. □ □

Remarque 8.2. Soit $p^{e'}$, $e' \geq e \geq 0$, l'exposant de $\mathcal{T}_k$ (où l'on rappelle que p^e est l'exposant de $U_k^*/\overline{E}_k$), et pour tout $n \geq 0$, soit $F_n = k_n F = KF$ le sous-corps de H_k^{pr} fixé par $\Gamma_\infty^{p^n}$ (se reporter au schéma du § 2). Alors, pour tout $n \geq e'$, la restriction $\mathcal{T}_k \longrightarrow \mathrm{Gal}(KF/K)$ est un isomorphisme de g-modules. En effet, $\mathcal{A}_k$ est normal dans $\mathrm{Gal}(H_k^{\mathrm{pr}}/\mathbb{Q})$, et $\mathcal{A}_k^{p^n} = \Gamma_\infty^{p^n}$ est normal et fixe KF qui est galoisien sur $\mathbb{Q}$. Autremant dit, g et $\mathrm{Gal}(K/\mathbb{Q})$ opèrent par conjugaison sur $\mathcal{T}_k$ de façon cohérente.

Ainsi, si F (ou Γ_∞) n'est pas unique, $F_{e'}$ est canonique comme sous-corps de H_k^{pr} fixe par $\mathcal{A}_k^{p^{e'}}$, ce qui rend canonique, pour tout $n \geq e'$, la décomposition en idéaux $\mathrm{N}_{K/k}(\mathfrak{A}) = \mathfrak{a}^{p^n} \cdot \mathfrak{t} \cdot (x_\infty)$, $\mathfrak{a}, \mathfrak{t} \in \mathcal{J}_k$, et précise le théorème précédent.

9. Conclusion

Pour k et p fixés, les expérimentations suggèrent que, pour tout $n \gg 0$ fixé, les probabilités de trivialité de chacun des deux facteurs de la i-suite $\#(M_{i+1}^n/M_i^n)$, pour i croissant, *tendent rapidement vers* 1, *indépendamment de* n, selon des lois binomiales sur les pas successifs, $1 \leq i \leq m_n$. Une estimation précise est difficile en raison de la présence de plusieurs paramètres de type corps de classes comme certains exemples l'ont montré aux §§ 5.2, 5.3.

Ceci rend crédible l'hypothèse et les heuristiques que nous avions données dans [6, Hypothèse 7.9, Heuristiques 7.5, 7.6] dont nous rappelons l'essentiel pour un corps k de degré d, totalement réel et p-décomposé :

(i) *Soit* $c \in \mathcal{C}\ell_k$ *; 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* $\frac{1}{\#\mathcal{C}\ell_k}$. *La probabilité que, pour* $x \in \Lambda_i^n$, *on ait* $\delta_{\mathfrak{p}}(x) \geq r$, *pour tout* $\mathfrak{p} \in S_k$, *est* : $\frac{1}{p^{\,r\,(d-1)}}$; *d'où celle de* $x \in \mathrm{N}_{k_n/k}(k_n^\times)$.

(ii) *Il existe* $i_0 \gg 0$, *indépendant de* n, *tel que* l'on ait $\mathrm{N}_{k_n/k}(M_{i_0}^n) = \mathcal{C}\ell_k$ et $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_{i_0}^n : \Lambda_{i_0}^n \cap \mathrm{N}_{k_n/k}(k_n^\times))} = 1$, pour tout $n \gg 0$.

Ce que l'on peut résumer de la façon approximative suivante (d'autant plus que les probabilités précédentes sont conjecturalement des majorants) :

Pour λ *ou* μ *non nuls, la probabilité de* $\#\mathcal{C}\ell_{k_n} = p^{\lambda\cdot n+\mu\cdot p^n+\nu}$ *est au plus en* $\frac{1}{p^{\,O(1)\,\cdot\,(\lambda\cdot n+\mu\cdot p^n)}}$, pour tout $n \gg 0$.

L'existence de $i_0 \gg 0$, *indépendant de* $n \to \infty$, stopant les algorithmes, peut paraître arbitraire car les liens numériques entre les étages n et $n+h$ semblent difficilement analysables, à l'exeption du schéma (6.2) du § 6.2 (iv) qui tient compte à la fois des pas i et des étages $n+h$ pour tout $h \geq 0$; mais cette existence est renforcée par le fait que k vérifie la conjecture de Greenberg si et seulement si $\widetilde{\mathcal{C}\ell}_k$ capitule dans k_∞ (cf. § 4.2). En effet, si $\widetilde{\mathcal{C}\ell}_k$ capitule dans k_n, il capitule dans k_{n+h} pour tout $h \geq 0$. Il y a probablement un lien concret entre le k_{n_0} de capitulation de $\widetilde{\mathcal{C}\ell}_k$ et i_0 qui pourrait être lié au nombre de pas m_{n_0} correspondant. De plus, une capitulation est progressive de k à k_{n_0}, ce qu'il serait utile d'interpréter en termes d'algorithme de dévissage des M_i^n.

On pourrait traiter le cas d'un unique idéal premier dans k au-dessus de p car alors le facteur normique est toujours trivial et l'algorithme ne porte que sur le facteur classes. Quant au cas d'une décomposition partielle, il est clair que les mêmes

heuristiques s'appliquent, le résultat de Jaulent étant général et les formules 3.2 pouvant être modifiées en conséquence selon [5].

En conclusion, le comportement des $\mathcal{C}\ell_{k_n}$ dans la tour ne dépend pas uniquement de *circonstances algébriques à la Iwasawa*, ni même de la théorie du corps de classes ou de celle des fonctions L_p, mais d'autres phénomènes arithmétiques p-adiques subtils qui se lisent de façon probabiliste au moyen des invariants habituels du corps k, sauf que la stabilisation précise de $\#\mathcal{C}\ell_{k_n}$, lorsque $n \to \infty$, semble aléatoire et certainement *non bornée sur l'ensemble des corps de nombres totalement réels*, à p constant.

Par contre, à k constant, nous avons conjecturé dans [9, Conjecture 8.11] que k est p-rationnel (i.e., $\mathcal{T}_k = 1$) pour tout $p \gg 0$, en notant que, pour p assez grand, $\mathcal{T}_k$ est réduit au régulateur $\mathcal{R}_k$ (suite exacte (2.1)) qui reste l'invariant crucial.

Comme déjà dit, la non-p-rationalité d'un corps de nombres k (principalement totalement réel) semble être une obstruction irréductible (à l'heure actuelle) à la preuve de nombreuses conjectures en théorie de Galois sur k. On peut penser que cela provient, quel que soit le cadre théorique, de la nature des fonctions L_p correspondantes, obtenues par interpolation de valeurs complexes, auquel cas, comme l'avait remarqué Washington en 1980/81 dans le cas de $\mathcal{T}_k$ (voir la bibliographie de [10]), la présence de «Siegel zeroes» (i.e., très proches de 1) rend ce type d'invariants cohomologiques problématiques, notamment lorsque p varie ou tend vers l'infini.

Références

[1] K. Belabas, K., Jaulent, J-F. : The logarithmic class group package in PARI/GP. Publ. Math. Besançon, 5–18 (2016) http://pmb.univ-fcomte.fr/2016/Belabas_Jaulent.pdf

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

[3] Colmez, P. : Résidu en $s = 1$ des fonctions zêta p-adiques. Invent. Math. **91**, 371–389 (1988) http://gdz.sub.uni-goettingen.de/dms/load/img/?PID=GDZPPN002104911

[4] Gras, G. : Class Field Theory : from theory to practice, corr. 2nd ed. Springer Monographs in Mathematics, Springer, xiii+507 pages (2005)

[5] Gras, G. : Invariant generalized ideal classes–Structure theorems for p-class groups in p-extensions. Proc. Math. Sci. **127**, no. 1, 1–34 (2017)
http://link.springer.com/article/10.1007/s12044-016-0324-1

[6] Gras, G. : Approche p-adique de la conjecture de Greenberg pour les corps totalement réels. Annales Mathématiques Blaise Pascal **24**, no. 2, 235–291 (2017)
http://ambp.cedram.org/cedram-bin/article/AMBP_2017__24_2_235_0.pdf

[7] Gras, G. : The p-adic Kummer–Leopoldt Constant : Normalized p-adic Regulator. International Journal of Number Theory, **14**, no. 2, 329–337 (2018)
https://doi.org/10.1142/S1793042118500203

[8] Gras, G. : On p-rationality of number fields. Applications – PARI/GP programs. Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 2017/2018 (to appear)
https://arxiv.org/pdf/1709.06388.pdf

[9] Gras, G. : Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques. Canadian Journal of Mathematics **68**(3), 571–624 (2016)
http://dx.doi.org/10.4153/CJM-2015-026-3 https://arxiv.org/pdf/1701.02618.pdf

[10] Gras, G. : Heuristics and conjectures in direction of a p-adic Brauer–Siegel theorem. Math. Comp. (2018) (to appear) https://doi.org/10.1090/mcom/3395

[11] Greenberg, R. : On the Iwasawa invariants of totally real number fields. Amer. J. Math. **98**, no. 1, 263–284 (1976)
http://www.jstor.org/stable/2373625?seq=1#page_scan_tab_contents

[12] Greenberg, R. : Iwasawa theory - past and present. Class field theory - its centenary and prospect (Tokyo, 1998). Advanced Studies in Pure Math., Math. Soc. Japan **30**, 335–385 (2001) https://sites.math.washington.edu/~greenber/iwhi.ps

[13] Jaulent, J-F. : Théorie ℓ-adique globale du corps de classes. J. Théorie des Nombres de Bordeaux **10**, no. 2, 355–397 (1998)

http://www.numdam.org/article/JTNB_1998__10_2_355_0.pdf

[14] Jaulent, J-F. : Note sur la conjecture de Greenberg. J. Ramanujan Math. Soc. (2017) http://jrms.ramanujanmathsociety.org/in-publication/in-publication-list/note-sur-la-conjecture-de-greenberg

[15] Nguyen Quang Do, T. : Formules de genres et conjecture de Greenberg. Ann. Math. Québec, **42**, no. 2, 267–280 (2018) https://doi.org/10.1007/s40316-017-0093-y

[16] Ozaki, M., Taya, H. : A note on Greenberg's conjecture for real abelian number fields. Manuscripta Math. 88, no. 1, 311–320 (1995)

http://link.springer.com/article/10.1007/BF02567825

[17] Ozaki, M. : The class group of $\mathbb{Z}_p$-extensions over totally real number fields. Tohoku Math. J. **49**, 431-435 (1997)

https://projecteuclid.org/download/pdf_1/euclid.tmj/1178225114

[18] The PARI Group : PARI/GP version 2.9.0. Université de Bordeaux (2016)

http://pari.math.u-bordeaux.fr/.

[19] Serre, J-P. : Sur le résidu de la fonction zêta p-adique d'un corps de nombres. C.R. Acad. Sci. Paris **287**, Série I, 183–188 (1978).

[20] Taya, H. : On cyclotomic $\mathbb{Z}_p$-extensions of real quadratic fields. Acta Arithmetica **74**, no. 2, 107–119 (1996) http://matwbn.icm.edu.pl/ksiazki/aa/aa74/aa7422.pdf

Villa la Gardette, chemin Château Gagnière, 38520 Le Bourg d'Oisans, http://www.researchgate.net/profile/Georges_Gras

E-mail address: g.mn.gras@wanadoo.fr