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

Georges Gras

▶ **To cite this version:**

Georges Gras. Normes d'idéaux dans la tour cyclotomique et conjecture de greenberg : hypothèses p-adiques sur les normes d'idéaux. 2017. hal-01546656v2

HAL Id: hal-01546656
https://hal.science/hal-01546656v2

Preprint submitted on 19 Sep 2017 (v2), last revised 4 Oct 2018 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

GEORGES GRAS

Abstract. Soit k un corps de nombres totalement réel et soit k_∞ sa $\mathbb{Z}_p$-extension cyclotomique pour p totalement décomposé dans k. Ce travail complète notre article : « Approche p-adique de la conjecture de Greenberg pour les corps totalement réels » (Annales Mathématiques Blaise Pascal), au moyen d'heuristiques sur le comportement p-adique des normes, dans k_n/k, des idéaux de k_n (n-ième étage de k_∞) ; en effet, la conjecture de Greenberg dépend d'images de ces normes dans le groupe de torsion (fini) $\mathcal{T}_k$ de la pro-p-extension abélienne p-ramifiée maximale de k. Une hypothèse de répartition de ces images dans $\mathcal{T}_k$ assurerait que les algorithmes de filtration des p-groupes des classes des k_n sont uniformément bornés (i.e., $\lambda = \mu = 0$). Plusieurs statistiques et exemples numériques dans le cas quadratique confirment la probable exactitude de telles propriétés.

Abstract. Let k be a totally real number field and let k_∞ be its cyclotomic $\mathbb{Z}_p$-extension for p totally split in k. This work completes our article: «Approche p-adique de la conjecture de Greenberg pour les corps totalement réels» (Annales Mathématiques Blaise Pascal), by means of heuristics on the p-adic behavior of the norms, in k_n/k, of the ideals of k_n (nth stage of k_∞); indeed, Greenberg's conjecture depends on some images of these norms in the (finite) torsion group $\mathcal{T}_k$ of the maximal abelian p-ramified pro-p-extension of k. An assumption of distribution of these images in $\mathcal{T}_k$ should ensure that the algorithms of filtration of the p-class groups of the k_n are uniformly bounded (i.e., $\lambda = \mu = 0$). Several statistics and numerical examples in the quadratic case confirm the probable exactness of such properties.

1. Rappel du contexte « Conjecture de Greenberg »

Dans [4], nous avons posé une hypothèse de répartition p-adique des normes $\mathrm{N}_{k_n/k}(\mathfrak{A})$ des 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, p-décomposé, pour analyser les obstructions p-adiques à une preuve, dans le seul cadre de la théorie d'Iwasawa algébrique, de la conjecture de Greenberg énoncée dans [6] : il s'agit de l'Hypothèse 1.3, rappelée à la fin du § 1.2, qui met en jeu le groupe de torsion $\mathcal{T}_k$ de la pro-p-extension abélienne p-ramifiée maximale de k.

Pour un historique sur la conjecture de Greenberg, et notament sur les travaux précurseurs de Ozaki [10] et Taya [13], se reporter à [4] et à sa bibliographie, ainsi qu'aux récents points de vue de Jaulent [8] et Nguyen Quang Do [9].

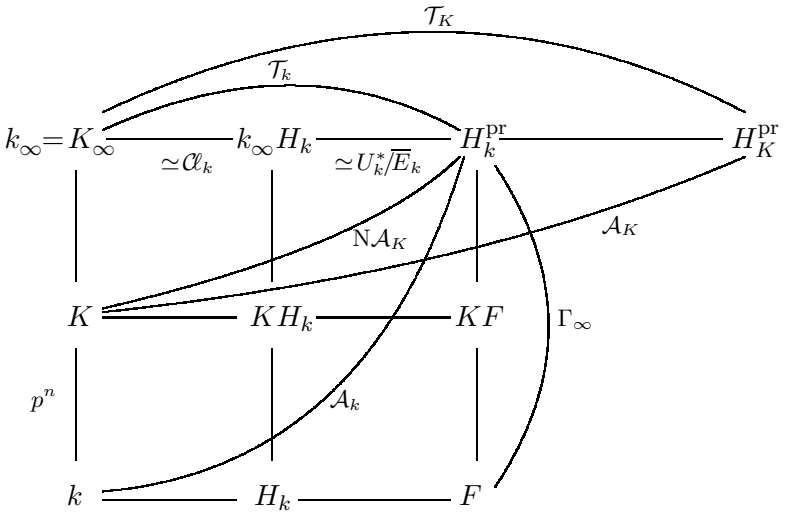
Date: 4 Septembre 2017.

1991 *Mathematics Subject Classification.* 11R23, 11R29, 11R37; 11Y40.

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

1.1. **Pro-p-extensions abéliennes p-ramifiées maximales.** Soit k un corps de nombres Galoisien réel de degré d et soit $p>2$ premier totalement décomposé dans k. Sous ces conditions, et sous la conjecture de Leopoldt pour p dans k_∞, on va obtenir le schéma ci-après (dit de la *p-ramification abélienne*), avec les notations suivantes :

Soit $K:=k_n$, de degré p^n sur k, le n-ième étage de la $\mathbb{Z}_p$-extension cyclotomique k_∞ de k (c'est une extension Galoisienne *réelle* de $\mathbb{Q}$ et par conséquent $K_\infty=k_\infty$), et 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. Enfin, soit H_k le p-corps de classes de Hilbert de k ; on a $H_k\cap k_\infty=k$ 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 $\Gamma_\infty={\rm Gal}(H_k^{\rm pr}/F)$:



On désigne par $\mathcal{C}\ell_k$ le p-groupe des classes de k et par E_k son groupe des unités. Soit $U_k:=\bigoplus_{\mathfrak{p}\mid p}U_\mathfrak{p}$ le $\mathbb{Z}_p$-module, de $\mathbb{Z}_p$-rang d, formé des unités locales principales de k en p, et soit U_k^* le sous-module de $\mathbb{Z}_p$-rang $d-1$ formé des $u\in U_k$ de norme 1 sur $\mathbb{Q}$ (sous nos hypothèses, ces $\mathbb{Z}_p$-modules sont libres et on a $U_\mathfrak{p}\simeq 1+p\,\mathbb{Z}_p$ pour tout $\mathfrak{p}\mid p$). D'après la conjecture de Leopoldt, l'adhérence $\overline{E}_k$ (vue comme image diagonale de $E_k\otimes\mathbb{Z}_p$ dans U_k^*) est d'indice fini dans U_k^*.

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 groupes de torsion $\mathcal{T}_k$ et $\mathcal{T}_K$. Comme k est réel, $\#\mathcal{T}_k$ est donné par la formule de Coates [1], en relation avec le résidu de la fonction ζ p-adique de k [12]. Les suites exactes classiques (où ${\rm tor}_{\mathbb{Z}_p}({\rm log}(U_k)/{\rm log}(\overline{E}_k))=:\mathcal{R}_k$ est le régulateur p-adique normalisé de k [5, § 4]) :

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

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

se résument ici, puisque ${\rm tor}_{\mathbb{Z}_p}(U_k)=1$, au moyen de la suite exacte :

$$1\longrightarrow U_k^*/\overline{E}_k\simeq\mathcal{R}_k\longrightarrow\mathcal{T}_k\longrightarrow\mathcal{C}\ell_k\longrightarrow 1. \tag{1.1}$$

Introduisons les symboles d'Artin $\left(\frac{H_k^{\rm pr}/k}{\cdot}\right)$ et $\left(\frac{H_K^{\rm pr}/K}{\cdot}\right)$ sur $\mathcal{J}_k := I_k \otimes \mathbb{Z}_p$ et $\mathcal{J}_K := I_K \otimes \mathbb{Z}_p$ respectivement, 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 (cf. [2, Theorem III.2.4, Proposition III.2.4.1] et [7, § 2]).

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

$$1 \longrightarrow \mathrm{Gal}(H_K^{\rm pr}/H_k^{\rm pr}) \longrightarrow \mathcal{A}_K \longrightarrow \mathrm{N}_{K/k}(\mathcal{A}_K) = \Gamma_\infty^{p^n} \oplus \mathcal{T}_k \longrightarrow 1. \tag{1.2}$$

Il en résulte que si $\mathfrak{A} \in I_K$ (idéal ordinaire vu dans $\mathcal{J}_K$), le symbole d'Artin de $\mathrm{N}_{K/k}(\mathfrak{A})$ dans $\mathcal{A}_k$ se décompose de façon unique sur $\Gamma_\infty^{p^n} \oplus \mathcal{T}_k$, et ainsi $\mathrm{N}_{K/k}(\mathfrak{A})$ peut s'écrire dans $\mathcal{J}_k$ sous la forme (où $(x_\infty) \in \mathcal{P}_{k,\infty}$) :

$$\mathrm{N}_{K/k}(\mathfrak{A}) = \mathfrak{a}^{p^n} \cdot \mathfrak{t} \cdot (x_\infty), \quad \mathfrak{a}, \mathfrak{t} \in \mathcal{J}_k, \left(\tfrac{H_k^{\rm pr}/k}{\mathfrak{a}}\right) \in \Gamma_\infty, \left(\tfrac{H_k^{\rm pr}/k}{\mathfrak{t}}\right) \in \mathcal{T}_k. \tag{1.3}$$

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

En conclusion, on verra que $\mathrm{N}_{K/k}(\mathfrak{A}) = (\alpha \cdot x_\infty) \cdot \mathfrak{t}$ dépend uniquement de $\mathfrak{t}$ sur le plan p-adique et p-groupe de classes, ce qui est un point fondamental car $\mathrm{N}_{K/k}(\mathfrak{A})$ ne dépend alors, numériquement, que des éléments de l'invariant fini $\mathcal{T}_k$ du corps de base, et ceci quel que soit $K = k_n$, $n \gg 0$.

1.2. **Algorithme de filtration des groupes de classes $\mathcal{C}\ell_{k_n}$.** Soit $K := k_n \subset k_\infty$ de degré p^n sur k et de groupe de Galois $G =: \langle \sigma \rangle$. Dans le cadre de l'algorithme général de calcul de $\mathcal{C}\ell_K$ 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 [4, § 6.1]) :

Définition 1.1. 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 $M_{i+1}^n = M_i^n$).

Remarques 1.2. (i) Pour $i = 0$, on obtient $M_1^n = (M^n)^G$ (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 donc que les groupes $\mathrm{N}_{K/k}(\mathcal{I}_i^n)$ ($n \gg 0$), qui représentent $\mathrm{N}_{K/k}(M_i^n) \subseteq \mathcal{C}\ell_k$, sont engendrés, modulo des (α) « quasi-infinitésimaux » (i.e., α très proche de 1 dans U_k), par des $\mathfrak{t} \in \mathcal{I}_k$ d'ordre fini modulo $\mathcal{P}_{k,\infty}$, et que les groupes :

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

qui contiennent E_k, sont obtenus via les idéaux principaux (x) de la forme $(\alpha \cdot x_\infty) \cdot \mathfrak{t}$, où $\mathfrak{t}$ est un idéal principal d'ordre fini modulo $\mathcal{P}_{k,\infty}$ (relation (1.3)). Rappelons enfin que, pour $n \geq 1$ fixé, une généralisation de la formule des classes ambiges de Chevalley, que nous avons redonnée dans [3], conduit à la i-suite d'entiers définie par :

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

(1.4) où :

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

seront appelés respectivement *le facteur clsses* 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 $\#\mathcal{R}_k$ (cf. [4, Théorème 4.2]).

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 puisque, d'après [4, Théorème 6.3], on a sur m_n les inégalités fondamentales suivantes (pour $\mathcal{T}_k \neq 1$) [1] :

$$\lambda \cdot n + \mu \cdot p^n + \nu \;\geq\; m_n \;\geq\; \frac{1}{v_p(\#\mathcal{T}_k)}\big(\lambda \cdot n + \mu \cdot p^n + \nu\big), \tag{1.5}$$

pour tout $n \gg 0$, où λ, μ, ν sont les invariants d'Iwasawa et v_p la valuation p-adique. Il est donc équivalent que m_n soit borné lorsque $n \to \infty$ pour que $\lambda = \mu = 0$.

Or m_n (pour n fixé) dépend de la progression des deux facteurs de (1.4), et on constate en pratique que, sous réserve de probabilités naturelles de répartition des éléments de $\mathcal{T}_k$ en relation avec la formule 1.3, chacun des deux facteurs est rapidement trivial.

On rappelle les résultats suivants [4, 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 notée $p^{c_i^\infty} \mid \#\mathcal{C}\ell_k$.

Ce facteur est rapidement égal à 1 (i.e., $p^{c_i^\infty} = 1$ pour $i \geq i_1$ convenable) sous réserve que les classes de la forme $\mathcal{C}\ell_k(\mathrm{N}_{k_n/k}(\mathfrak{A})) = \mathcal{C}\ell_k(\mathfrak{t})$ (où $\mathfrak{A}$ est un *idéal aléatoire de* k_n et $\mathfrak{t}$ la composante donnée par la relation (1.3)), se répartissent de façon uniforme dans le groupe des classes de k.

(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 notée $p^{\rho_i^\infty} \mid \#\mathcal{R}_k$.

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 de Hasse de suffisamment de $x \in \Lambda_i^n$ engendrent $\Omega(k_n/k)$ qui est le sous-groupe, de la somme directe $\bigoplus_{\mathfrak{p}|p} I_\mathfrak{p} = G_n^d$ des groupes d'inertie $I_\mathfrak{p}$, formé des familles $\Big(\Big(\frac{x, k_n/k}{\mathfrak{p}}\Big)\Big)_{\mathfrak{p}|p}$ vérifiant la formule

[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 [4, Théorème 4.7], on a $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{T}_k$ pour tout $n \gg 0$.

du produit ; or chaque symbole ne dépend que du $\mathfrak{p}$-quotient de Fermat $\mathfrak{p}^{\delta_\mathfrak{p}(x)}$ de x, où l'on a posé, pour x étranger à p :

$$\frac{x^{p-1}-1}{p} =: \prod_{\mathfrak{p}\mid p} \mathfrak{p}^{\delta_\mathfrak{p}(x)} \cdot \mathfrak{b}(x), \quad \delta_\mathfrak{p}(x) \geq 0,\ \mathfrak{b}(x) \text{ étranger à } p. \tag{1.6}$$

L'ordre de $\left(\frac{x,\, k_n/k}{\mathfrak{p}}\right)$ étant $p^{n-\delta_\mathfrak{p}(x)}$ pour $n \gg 0$ (cf. [4, Théorème 4.4]), ce symbole engendre G_n si et seulement si $\delta_\mathfrak{p}(x) = 0$, qui est a priori de probabilité $1 - \frac{1}{p}$, les $\delta_\mathfrak{p}(x) \geq r$ étant de probabilités $\frac{1}{p^r}$.

Pour le calcul des $\delta_\mathfrak{p}(x)$, pour $x \in k^\times$ de la forme $(x) = \mathrm{N}_{k_n/k}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}_i^n$ (i.e., $x \in \Lambda_i^n$), on aura, d'après la relation (1.3), pour $n \gg 0$:

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

où le nombre $\alpha \cdot x_\infty$ est négligeable quant aux $\delta_\mathfrak{p}(\alpha \cdot x_\infty) = \delta_\mathfrak{p}(\alpha)$; les $\delta_\mathfrak{p}(x)$ ne dépendent alors que de l'idéal principal $\mathfrak{t}$ noté encore (x) par abus. En effet, 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 ; donc $\mathrm{N}_{k/\mathbb{Q}}(x) = 1$ dans $U_\mathbb{Q}$, l'image de x dans U_k est définie dans $U_k^*/\overline{E}_k$ et $\delta_\mathfrak{p}(x) \pmod{\delta_\mathfrak{p}(E_k)}$ ne prend qu'un nombre fini de valeurs alors que $\delta_\mathfrak{p}(\alpha) \to \infty$ avec n.

Nous avons formulé dans [4, Hypothèse 7.1] les hypothèses suivantes, au sujet de la composante $\mathfrak{t}$, que nous nous proposons de tester numériquement :

Hypothèses 1.3. *On suppose que les idéaux $\mathfrak{A}$ (étrangers à p) de $K = k_n$, obtenus au cours de l'algorithme de calcul de $\#\mathcal{C}\ell_K$ (cf. § 1.2), définissent une variable aléatoire, et qu'il en est de même pour la composante $\mathfrak{t}$ de $\mathrm{N}_{K/k}(\mathfrak{A})$. Enfin on suppose que les symboles de Frobenius $\left(\frac{F/k}{\mathfrak{t}}\right)$ se répartissent uniformément dans $\mathrm{Gal}(F/k) \simeq \mathcal{T}_k$.*

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) Lorsque $\mathfrak{t} = (x)$, les $\delta_\mathfrak{p}(x) \pmod{\delta_\mathfrak{p}(E_k)}$ parcourent uniformément un ensemble fini. [2]

(iii) L'heuristique principale de [4] 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 $n \to \infty$.

On notera que les limites $p^{c_i^\infty + \rho_i^\infty}$ des n-suites $\#\left(M_{i+1}^n/M_i^n\right)$, $n \to \infty$, constituent une i-suite *décroissante stationnaire* de diviseurs de $\#\mathcal{T}_k$ (cf. [4, 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 sur un plan pratique que si $\lambda \geq 1$ ou $\mu \geq 1$ alors, pour n fixé *arbitrairement grand*, l'algorithme « bouclerait » $O(\lambda \cdot n + \mu \cdot p^n)$ fois de suite (cf. 1.5), ce qui constitue un non-sens numérique mais suggère l'immense difficulté pour établir une contradiction conduisant à une preuve de la conjecture de Greenberg.

[2] Pour k quadratique, $\delta_\mathfrak{p}(x)$ est indépendant du choix de $\mathfrak{p} \mid p$ et sera noté $\delta_p(x)$ (cf. [4, Définition 4.1 & § 5.1]).

2. Statistiques sur les idéaux $\mathrm{N}_{K/k}(\mathfrak{A})$

On se place dans le cas quadratique réel $k=\mathbb{Q}(\sqrt{m})$, $p>2$ totalement décomposé, et on utilise des programmes PARI [11] pour les calculs. On suppose que l'unité fondamentale ε est telle que $\delta_p(\varepsilon)$ est assez grand afin que, lorsque x (étranger à p et norme locale en dehors de p dans k_n/k) n'est défini que modulo E_k, le calcul des $\delta_p(x)$ soit indépendant de tout choix effectué par PARI, au moins pour les petites valeurs des $\delta_p(x)$. En effet, si $\delta_p(\varepsilon)=r$ et $\delta_p(x)<r$, alors $\delta_p(x\cdot\varepsilon')=\delta_p(x)$ quelle que soit $\varepsilon'\in E_k$, alors que si $\delta_p(x)\geq r$, $\delta_p(x\cdot\varepsilon')$ peut prendre toute valeur $\geq r$.
Rappelons que les $x\in\Lambda_i^n$, qui sont par nature des 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 pratique il n'est pas nécessaire de prendre n très grand car les $\delta_p(\varepsilon)$ sont limités puisque, dans le cas quadratique, le régulateur p-adique normalisé est $\mathcal{R}_k\sim\frac{1}{p}\log(\varepsilon)\sim p^{\delta_p(\varepsilon)}$; 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).
On suppose désormais que $p=3$ et on désigne par $\mathfrak{p}$ un idéal premier de k au-dessus de 3.

2.1. **Programme général de calcul de h, $\delta_{\mathfrak{p}}(\eta_3)$, $\delta_3(\varepsilon)$.** Il donne la liste des m pour lesquels $k=\mathbb{Q}(\sqrt{m})$ répond à certaines spécifications au niveau du nombre de classes h, et des valeurs de $\delta_3(\varepsilon)$ et $\delta_{\mathfrak{p}}(\eta_3)$, où η_3 est une S_k-unité fondamentale (donnée par $\mathfrak{p}^{h'}=(\eta_3)$ où h' est l'ordre de $\mathscr{cl}_k(\mathfrak{p})$).
On teste la condition suffisante (cf. [4, Théorème 3.4]) conduisant à $\lambda=\mu=0$ pour k quadratique (condition qui équivaut à la trivialité du groupe des classes logarithmiques $\widetilde{\mathcal{C}\ell}_k$ introduit dans [8]) :

(i) $\mathcal{C}\ell_k^{S_k}=1$ (i.e., $\mathfrak{p}$ engendre le 3-groupe des classes de k),

(ii) $\delta_3(\varepsilon)\geq 1$ & $\delta_{\mathfrak{p}}(\eta_3)\geq 1$.

Si (i) (resp. (ii)) n'a pas lieu, le programme indique PROBLEME-CLASSES (resp. PROBLEME-NORMIQUE). On impose par commodité h puissance de 3 et on fixe un ordre de grandeur à $\delta_3(\varepsilon)$ (zmax $=\frac{1}{3^\delta}$ pour $\delta_3(\varepsilon)>\delta$) :

```
{y=x;p=3;m=1;n=8;n0=n+1;zmax=1/p^2;while(m<2*10^4,m=m+1;
if(core(m)==m & kronecker(m,p)==1,Q=x^2-m;K=bnfinit(Q,1);
M=m;t=Mod(m,4);if(t!=1,M=4*m);h=qfbclassno(M);vh=valuation(h,p);
if(vh>=1 & h==p^vh,E=quadunit(M);
e1=component(E,2);e2=component(E,3);if(t==1,e2=e2/2;e1=e1+e2);
E=e1+e2*x;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(m,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);
hs=norm(Mod(pi1,Q));h0=valuation(hs,p);
delta=valuation(h,p)-valuation(h0,p);
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("PROBLEME-CLASSES"));
if(zpi+ze<1,print("PROBLEME-NORMIQUE"));print("m=",m," h=",h," E=",E);
print("p=",p," S=",pi1," ",pi2);print(zpi," ",ze);print(" "));x=y)))}
```

2.2. **Représentation des classes par des idéaux premiers.** On désire établir des statistiques sur l'influence numérique des $\mathrm{N}_{K/k}(\mathfrak{A}) \in \mathrm{N}_{K/k}(\mathcal{I}_i^n)$ de l'algorithme sur le facteur classes et sur le facteur normique de (1.4).

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 (1.4) ; en effet, le premier facteur est relatif aux *classes des* $\mathrm{N}_{K/k}(\mathfrak{A})$ et le second est relatif aux *indices normiques* $(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{K/k}(K^\times))$ qui ne dépendent pas du choix des $x \in \Lambda_i^n$, modulo $E_k \cdot \mathrm{N}_{K/k}(K^\times)$ (cf. [4, § 6.2]).

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 (ce qui sera précisé au § 3.1).

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 $\mathcal{C}l_k$ dont la croissance algorithmique, en fonction du nombre de pas, est censée atteindre $\mathcal{C}l_k$ 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 $\delta_3(\eta_\ell)$ (modulo $\delta_3(E_k)$) ont 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 $\delta_3(\varepsilon) = 4$ pour limiter les incertitudes sur le choix par PARI de x modulo E_k (la variable NPX compte le nombres de produits non principaux).

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=listcreate;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=1,1000,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 (par utilisation du programme général du § 2.1) :

```
m=7249, h=3, E=17052467702474466522 0*x+14518651659981320194199
p=3, S={131480821*x-11194416394,131480821*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 :

$$[937,\ 883,\ 811,\ 631,\ 487,\ 181,\ 163,\ 37].$$

Plusieurs passages du programme donnent par exemple : $N_n = 10720$, 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.

2.3. **Facteur classes et facteur normique 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.

2.3.1. *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 $\ell \equiv 1 \pmod{3^{8+1}}$, puis $-1 \pmod{3^{8+1}}$), 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).

La répartition des ordres des classe des $\mathfrak{l}$ constitue la première partie du programme et seulement en seconde partie, on fait choix d'une valeur de r.

Le nombre NL_r représente le nombre de premiers $\ell \leq B = 2{\cdot}10^{12}$ totalement décomposés dans K/k tels que la classe de $\mathfrak{l} = \mathrm{N}_{K/k}(\mathfrak{L})$ soit d'ordre r (ici $r \in \{1, 3, 9\}$). Les proportions correspondantes sont comparées aux probabilités naturelles $\frac{1}{9}$, $\frac{2}{9}$, $\frac{6}{9}$.

On a $NL = NL_1 + NL_3 + NL_9$ (nombre de ℓ considérés).

Pour chaque r, on désigne par $C_0, C_1, C_2, C_3, C_4, C_5$ les nombres de $\ell \leq B$ tels que $(\eta_\ell) = \mathfrak{l}^r$ et $\delta_3(\eta_\ell) = 0, 1, 2, 3, 4, \geq 5$ respectivement :

```
{p=3;m=72262;n=8;B=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<B,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);

r=3;if(vcl==r,NLr=NLr+1;
A=F;AA=(Mod(A,Q)^2-1)/3;v=valuation(AA,3);
if(v==0,C0=C0+1);if(v==1,C1=C1+1);if(v==2,C2=C2+1);
if(v==3,C3=C3+1);if(v==4,C4=C4+1);if(v>=5,C5=C5+1)))));
print("p=",p," m=",m," n=",n," B=",B);
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)}
```

2.3.2. *Répartition des ordres des classes pour $m = 72262$.* On obtient :

$$NL = 5584183,\ NL_1 = 620512,\ NL_3 = 1240284,\ NL_9 = 3723387,$$

et le tableau des proportions :

proportions	probabilités
$NL_1/NL = 0.1111195675$	$\frac{2}{3} = 0.1111111111$
$NL_3/NL = 0.2221066179$	$\frac{2}{3^2} = 0.2222222222$
$NL_9/NL = 0.6667738145$	$\frac{2}{3^3} = 0.6666666666$

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 § 3.2).

2.3.3. *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 $NL_1 = 620512$ avec :

$C_0 = 412997$, $C_1 = 137911$, $C_2 = 46166$, $C_3 = 15833$, $C_4 = 5090$, $C_5 = 2515$,
et le tableau :

proportions	probabilités
$C_0/NL_1 = 0.6655745577$	$\frac{2}{3} = 0.6666666666$
$C_1/NL_1 = 0.2222535583$	$\frac{2}{3^2} = 0.2222222222$
$C_2/NL_1 = 0.0743998504$	$\frac{2}{3^3} = 0.0740740740$
$C_3/NL_1 = 0.0255160254$	$\frac{2}{3^4} = 0.0246913580$
$C_4/NL_1 = 0.0082029034$	$\frac{2}{3^5} = 0.0082304526$
$C_5/NL_1 = 0.0040531045$	$\sum_{j\geq 6} \frac{2}{3^j} = 0.0041152264$

(ii) Dénombrement des $\mathscr{C}\ell_k(\mathfrak{l})$ d'ordre $r = 3$ et calcul des $\delta_3(\eta_\ell)$.
On obtient $NL_3 = C_0 = 1240284$, $C_1 = C_2 = C_3 = C_4 = C_5 = 0$.

(iii) Dénombrement des $\mathscr{C}\ell_k(\mathfrak{l})$ d'ordre $r = 9$ et calcul des $\delta_3(\eta_\ell)$.
On obtient aussi $NL_9 = C_0 = 3723387$, $C_1 = C_2 = C_3 = C_4 = C_5 = 0$.
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 réflexion, 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 particulières.

2.4. **Facteur classes et facteur normique 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.

2.4.1. *Programme.* Le programme est similaire au précédent avec $r \in \{1, 3\}$, les nombres NL_1, NL_3 représentent le nombre de premiers $\ell \leq B = 2 \cdot 10^{12}$, 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 C_0, C_1, C_2, C_3, C_4, C_5 sont les mêmes et sont les nombres de premiers ℓ tels que $\delta_3(\eta_\ell) = 0, 1, 2, 3, 4, \geq 5$ respectivement. On a $NL = NL_1 + NL_3$.

2.4.2. *Répartition des ordres des classe pour $m = 10942$.* Les données sur la répartition des classe sont les mêmes pour les valeurs de $r \in \{1, 3\}$:

$$NL = 5587470, NL_1 = 1862666, NL_3 = 3724804,$$

et pour les proportions :

proportions	probabilités
$NL_1/NL = 0.333364832$	$\frac{1}{3} = 0.3333333333$
$NL_3/NL = 0.6666351676$	$\frac{2}{3^2} = 0.6666666666$

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

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

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

On obtient $NL_1 = 1862666$, $C_0 = 1241224$, $C_1 = 414270$, $C_2 = 138044$, $C_3 = 45829$, $C_4 = 15475$, $C_5 = 7824$ et le tableau :

proportions	probabilités
$C_0/NL_1 = 0.6663696014$	$\frac{2}{3} = 0.6666666666$
$C_1/NL_1 = 0.2224070230$	$\frac{2}{3^2} = 0.2222222222$
$C_2/NL_1 = 0.0741109785$	$\frac{2}{3^3} = 0.0740740740$
$C_3/NL_1 = 0.0246039816$	$\frac{2}{3^4} = 0.0246913580$
$C_4/NL_1 = 0.0083079843$	$\frac{2}{3^5} = 0.0082304526$
$C_5/NL_1 = 0.0042004309$	$\sum_{j\geq 6} \frac{2}{3^j} = 0.0041152264$

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

On obtient $NL_3 = 3724804$, $C_0 = 0$, $C_1 = 2484070$, $C_2 = 827554$, $C_3 = 275264$, $C_4 = 91971$, $C_5 = 45945$ et le tableau :

proportions	probabilités
$C_0/NL_3 = 0.0000000000$	$\frac{2}{3} = 0.0000000000$
$C_1/NL_3 = 0.6668995200$	$\frac{2}{3^2} = 0.6666666666$
$C_2/NL_3 = 0.2221738378$	$\frac{2}{3^3} = 0.2222222222$
$C_3/NL_3 = 0.0739002642$	$\frac{2}{3^4} = 0.0740740740$
$C_4/NL_3 = 0.0246915005$	$\frac{2}{3^5} = 0.0246913580$
$C_5/NL_3 = 0.0123348772$	$\frac{2}{3^6} = 0.0123450517$

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 $\delta_3(x) = 0$ comme on l'a vu au § 2.2) :

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, on sait que le 3-rang de $\mathcal{T}_L$ est égal à :

$$\mathrm{rg}_3(\mathcal{C}\ell_L^{S_L}) + \#S_L - 1 = \mathrm{rg}_3(\mathcal{C}\ell_L^{S_L}) + 1 \quad [2, \text{Proposition III.4.2.2}],$$

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-places 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 $\mathrm{rg}_3(\mathcal{T}_k) = 1$ [2, 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 $C_0 = 0$.

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 $\frac{1}{3}$).

2.5. **Exemples de corps k avec $\mathcal{C}\ell_k^{S_k} \neq 1$, $\delta_3(\varepsilon)$ & $\delta_{\mathfrak{p}}(\eta_3) \geq 1$.** 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) $m = 94918, \varepsilon = 1881606172088175003974358115094 34 \cdot x$
$+5796996235321435886132945573590 8197,$

$\eta_3 = -8591 \cdot x - 2646781,$

$\delta_3(\varepsilon) = 3$ & $\delta_{\mathfrak{p}}(\eta_3) = 2$, 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]].

Remarque 2.1. Pour $m = 31069$ et $r = 3$, on trouve des résultats analogues à ceux du second exemple où $C_0 = 0$:

$NL_3 = 3721754$, $C_0 = 0$, $C_1 = 2480548$, $C_2 = 826613$, $C_3 = 276142$, $C_4 = 92283$, $C_5 = 46168$.

Pour $m \in \{26893, 92269, 94918, 171061\}$ et $r = 3$, on trouve les résultats suivants, analogues à ceux du premier exemple : $C_0 = NL_3$, $C_1 = C_2 = C_3 = C_4 = C_5 = 0$.

3. L'équation $(y) = \mathfrak{B} \cdot \mathfrak{A}^{1-\sigma}$, pour $\mathrm{N}_{K/k}(\mathfrak{B}) = \mathrm{N}_{K/k}(y)$

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 $\mathcal{I}_i^n$ et sur la question de savoir si ces idéaux et leurs normes sont « aléatoires » ou non par rapport aux précédents.

3.1. **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 $\delta_p(x)$ (cf. (1.6)). On pose alors en vertu du théorème des normes de Hasse :

$$x = \mathrm{N}_{K/k}(y), \quad y \in K^\times,$$

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 précédent (autrement dit, que $\mathfrak{A}$ n'a aucune relation *algébrique* avec $\mathfrak{B}$ et constitue un nouveau « tirage probabiliste »). Comme $\mathfrak{A}$ est défini modulo l'étendu d'un idéal $\mathfrak{a}$ de k, $\mathrm{N}_{K/k}(\mathfrak{A})$ est défini modulo $\mathfrak{a}^{p^n}$ de composante triviale sur $\mathcal{T}_k$ pour $n \gg 0$ (relation (1.3)), 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 à $\mathrm{N}_{K/k}(\mathfrak{A}) \in \mathrm{N}_{K/k}(\mathcal{I}_{i+1}^n)$ 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 de l'Hypothèse 1.3, 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.

Remarque 3.1. Le théorème des normes de Hasse pour les extensions cycliques est, au plan numérique, assez problématique et fortement lié à 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 $K = k_n$, il n'est pas possible d'en déduire une solution globale y.

Il faut signaler le cas trivial $x = 1$ et l'équation $\mathrm{N}_{k_1/k}(y) = 1$ qui conduit par le Théorème 90 de Hilbert, à $y = z^{1-\sigma}$, $z \in k_1^\times$, où une solution z_0 est donnée par une résolvante de Hilbert (qui existe en toute généralité pour une extension cyclique) et qui pour le niveau $n = 1$ du cas cubique s'écrit :

$$z_0 = 1 + y + y^{1+\sigma},$$

mais l'aspect additif suggère justement une part totalement aléatoire. Dans le cas de l'équation norme en idéaux, il n'y a pas de résolvante explicite, mais on peut penser qu'il y a une complexité du même ordre.

Lemme 3.2. *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 choisir tout $x \in \Lambda_i^n$ 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 composnte $\mathfrak{t}$ est inchangée. □

Remarque 3.3. 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 s'attache 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 :

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

(idéal premier principal de k en-dessous de $\mathfrak{L}$). L'aspect statistique devant 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 § 3.3.

3.2. **Remarques heuristiques fondamentales.**

(i) On pourrait 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 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.

Pour l'aspect statistique sur une donnée numérique $k = \mathbb{Q}(\sqrt{m})$, 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.

(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 $(y) = \mathfrak{B} \cdot \mathfrak{A}^{1-\sigma}$ et sur la détermination de quotients de Fermat $\delta_{\mathfrak{p}}(x)$ issus de la relation $\left(\frac{x^{p-1}-1}{p}\right) =: \prod_{\mathfrak{p}|p} \mathfrak{p}^{\delta_{\mathfrak{p}}(x)} \cdot \mathfrak{b}(x)$, $\mathfrak{b}(x)$ étranger à p.

A priori, il n'y a pas d'obstruction à une répartition uniforme de la composante $\mathfrak{t} \in \mathcal{T}_k$ associée à $\mathrm{N}_{K/k}(\mathfrak{A})$ en raison des propriétés du symbole d'Artin de $\mathrm{N}_{K/k}(\mathfrak{A})$ dans $\Gamma_\infty^{p^n} \oplus \mathcal{T}_k$ (suite exacte (1.2) et relation (1.3)). 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 prévisible.

(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 (i, 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^m $(m \geq n)$.

(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 tendant vers 0 en prenant par exemple des corps quadratiques $k = \mathbb{Q}(\sqrt{m})$ avec $m = a^2 \cdot p^{2n} \pm 1$ supposé sans facteur carré, auquel cas l'unité fondamentale de k est $\varepsilon = a \cdot p^n \pm \sqrt{m}$ dont le logarithme p-adique tend vers 0 si $n \to \infty$. Et cependant la conjecture de Leopoldt est ici trivialement vraie.

(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 [4, 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 [8], cette complexité est aussi mesurée par le comportement du *groupe des classes logarithmiques* de k par extension dans k_∞.

(iv) Il faut ajouter que, comme pour la conjecture de Leopoldt, les algorithmes 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, ainsi que la théorie du corps de classes qui indique par exemple que, pour $m \geq n$, $\mathrm{N}_{k_m/k_n}(\mathcal{C}\ell_{k_m}) = \mathcal{C}\ell_{k_n}$, etc.).

Ce lien est exprimé par le fait que, pour tout $h \geq 1$ et $i \geq 1$ fixé, modulo des normes globales convenables dans les extensions k_{n+j}/k, $j \in [1, h]$, ce qui ne modifie pas les indices $(\Lambda_i^{n+j} : \Lambda_i^{n+j} \cap \mathrm{N}_{k_{n+j}/k}(k_{n+j}^\times))$, on peut obtenir les relations d'inclusions suivantes [4, § 7.1, Schéma & Relation (7.1)] :

$$\mathrm{N}_{k_{n+h}/k}(\mathcal{I}_i^{n+h}) \subseteq \cdots \subseteq \mathrm{N}_{k_{n+1}/k}(\mathcal{I}_i^{n+1}) \subseteq \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)$$

$$E_k \subseteq \Lambda_i^{n+h} \subseteq \cdots \subseteq \Lambda_i^{n+1} \subseteq \Lambda_i^n.$$

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.

Signalons que ce résultat provient des flèches :

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

du schéma, qui ne sont a priori ni injectives ni surjectives, et que c'est à ce niveau que se trouve l'obstruction à une preuve *algébrique* de la conjecture de Greenberg.

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.

3.3. **Programme de recherche des idéaux $\mathfrak{A}$ tels que $(y) = \mathfrak{B}\cdot\mathfrak{A}^{1-\sigma}$.** Il est impossible de faire des statistiques en supposant K arbitrairement grand dans la tour. Nous allons cependant examiner, au moyen d'un programme, le principe général d'obtention de $\mathfrak{A} = \mathfrak{Q}^{\omega}$ et $\mathrm{N}_{K/k}(\mathfrak{A}) = \mathrm{N}_{K/k}(\mathfrak{Q}^{\omega}) = \mathfrak{q}^{\omega(1)}$ à partir de la relation précédente du § 3.1 :

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

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 puisque'il ne s'arrête que si les $\mathfrak{q}^{\omega(1)}$ finissent par engendrer $\mathcal{C}\ell_k$ et si suffisamment d'itérations finissent par donner un $\delta_3(x) = 0$; les statistiques examineront ces deux aspects qui correspondent aux deux facteurs de l'expression (1.4).

Le programme général, qui détermine la solution $y \in k_1^{\times}$ et la factorisation de $\mathfrak{A} = \mathfrak{Q}^{\omega}$ 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. On constatera que 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 $\mathfrak{A} = \mathfrak{Q}^{\omega}$ dont la norme $\mathfrak{q}^{\omega(1)}$ dans k_1/k contribue au pas suivant de l'algorithme.

3.3.1. *Programme principal : 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 (dans E), la S_k-unité fondamentale η_3 et sa conjuguée (dans S), $\delta_{\mathfrak{p}}(\eta_3)$, $\delta_3(\varepsilon) \geq 1$ 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 $\ell < B$, $\ell \equiv \pm 1 \pmod{M_p = 9}$ et $\mathfrak{l} = (\eta_\ell)$ dans k, où η_ℓ est calcué sous la forme $\mathrm{Mod}(a * z + b, z^2 - m)$, 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 $\delta_3(\varepsilon) = 2$:

```
PROBLEME-NORMIQUE
m=67,h=1,E=5967*z+48842
p=3,S={z+8,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 donne ci-après le programme complet :

```
{y=z;p=3;m=67;n=8;n0=n+1;B=10^4;Q=z^2-m;K=bnfinit(Q,1);
M=m;t=Mod(m,4);if(t!=1,M=4*m);h=qfbclassno(M);E=quadunit(M);
e1=component(E,2);e2=component(E,3);if(t==1,e2=e2/2;e1=e1+e2);
E=e1+e2*z;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);delta=valuation(h,p)-valuation(h0,p);
npi=norm(XPpi)^(p-1);ne=norm(XPe)^(p-1);
zpi=znorder(npi)/p^n;ze=znorder(ne)/p^n;
if(delta!=0,print("PROBLEME-CLASSES"));
if(zpi+ze<1,print("PROBLEME-NORMIQUE"));
print("m=",m," h=",h," E=",E);print("p=",p," S=",pi1," ",pi2);
print(zpi," ",ze);print(" ");

Mp=p^2;Nlist=0;list=listcreate;listL=listcreate;
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}
```

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

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 précédente :

```
991
Mat([[991,[145,0,0,0,1,0]~,1,1,[385,-256,182,-61,334,-466]~],1])
883
Mat([[883,[-395,0,0,0,1,0]~,1,1,[67,287,91,-236,-207,74]~],1])
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]
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]
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]
773
Mat([[773,[-145,0,0,0,1,0]~,1,1,[-14,277,39,-355,343,-149]~],1])
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]
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]
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.

3.3.2. *Programme recherchant des* $\mathfrak{A}$ *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;M=m;t=Mod(m,4);if(t!=1,M=4*m);E=quadunit(M);
e1=component(E,2);e2=component(E,3);
if(t==1,e2=e2/2;e1=e1+e2); E=Mod(e1+e2*y,y^2-m);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;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 $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/3\mathbb{Z}$).

4. Evolution de la i-suite $\#(M_{i+1}^1/M_i^1)$ 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 $\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

4.1. **Utilisation du programme principal 3.3.1.** 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 :

```
PROBLEME-NORMIQUE
m=6559,h=18,E=81*z+6560
p=3,S={379*z-30694,379*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)])
```

4.2. **Décomposition de (y) en idéaux, pour $k = \mathbb{Q}(\sqrt{6559})$.** Le programme 3.3.1 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
                873830482232719727293475639984052 9/418195493*y
-8390598661945059443075872989882636906451249
                973368798056889904121752787877 0/418195493,y^2-6559)*x^2
```

```
+Mod(-19471075694983430251815098361774199857 0
              941303601495212020463437158589931 0/418195493*y
+15769167293211778079551042284522907830683899
              947946906063185100186533603787 4/418195493,y^2-6559)*x
+Mod(55126233574835545800719913475586793 9
              764504856477125221099310399055725544/418195493*y
-44645442969040311582101175795304512633193 33
          45308698265081589912634047713604/418195493,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 les résultats suivants 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 § 4.1) :

```
92179
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],1;
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-1;
[92179, [16160,0,0,0,1,0]~,1,1,
      [-34250,-40280,3133,-29163,-3589,-27112]~],1]
86239
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],3;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],2;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-1;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],1;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-5;
[86239,[-15841,0,0,0,1,0]~,1,1,
      [42046,29382,41192,20964,27633,-12780]~], 1]
70327
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],2;
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-2;
[70327, [22052,0,0,0,1,0]~,1,1,
      [32411,11187,23443,18808,-289,-19643]~],1]
68743
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],2;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],4;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-2;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-6;
[68743,[23513,0,0,0,1,0]~,1,1,
      [24129,16740,26535,3717,11912,-12637]~],1]
58321
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],5;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],3;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-2;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-8;
[58321,[12524,0,0,0,1,0]~,1,1,
      [13509,16128,23244,-16488,-7523,-20417]~], 1]
48907
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],1;
```

```
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-1;
[48907,[-7471,0,0,0,1,0]~,1,1,
      [12062,22844,17998,-17401,-4054,-17679]~],1]
47143
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],3;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],4;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-2;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-7;
[47143,[3366,0,0,0,1,0]~,1,1,
      [12897,21052,-1667,-5566,12609,-21078]~],1]
40519
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],3;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],2;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-1;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],1;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-5;
[40519,[14026,0,0,0,1,0]~,1,1,
      [-16554,-9590,-5735,-1348,6288,-10697]~],1]
30781
[[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],1;
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-1;
[30781, [3151,0,0,0,1,0]~,1,1,
      [-5658,-3195,-12396,-5993,-3172,-11357]~],1]
28279
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],3;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],4;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-2;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-7;
[28279,[3506,0,0,0,1,0]~,1,1,
      [356,7859,1221,-1277,3345,8122]~],1]
25237
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],6;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],3;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-2;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-9;
[25237,[-5803,0,0,0,1,0]~,1,1,
      [-846,-3686,-10226,-7500,1330,-8604]~],1]
12547
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],1;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],2;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-1;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],1;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-3;
[12547,[-5707,0,0,0,1,0]~,1,1,
      [4280,-2107,-4165,-5825,-2717,-3182]~],1]
8011
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],4;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],3;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-2;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-7;
[8011,[-2063,0,0,0,1,0]~,1,1,
      [-2011,-1995,2900,979,-3590,1411]~],1]
1621
Mat([[1621,[-62,0,0,0,1,0]~,1,1,
```

```
      [119,-637,235,621,776,762]~],1])
96461
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],-1;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],1;
[96461,[-38381,0,0,0,1,0]~,1,1,
      [-3184,25989,35903,47120,-34637,-1125]~],1]
96263
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],2;
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-2;
[96263,[-28877,0,0,0,1,0]~,1,1,
      [-42114,34772,17252,-37514,44396,-9080]~],1]
89009
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],1;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],2;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-1;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],1;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-3;
[89009,[35383,0,0,0,1,0]~,1,1,
      [-42840,40957,-35093,31095,7577,29134]~],1]
88001
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],2;
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-2;
[88001, [37926,0,0,0,1,0]~,1,1,
      [24936,-21477,10233,-38146,-22686,-12008]~],1]
84653
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],1;
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-1;
[84653, [24445,0,0,0,1,0]~,1,1,
      [27778,-34833,11002,-38982,-15462,16757]~],1]
82457
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],2;
[53,[9,0,0,0,1,0]~,1,1,[-25,11,16,-3,-22,10]~],-2;
[82457,[-11462,0,0,0,1,0]~,1,1,
      [-12743,-34335,-22650,2405,35275,-22073]~],1]
77003
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],3;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],2;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-1;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],1;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-5;
[77003,[21128,0,0,0,1,0]~,1,1,
      [-19120,-16548,-9829,-16250,-24213,-24196]~],1]
37781
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],6;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],3;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-2;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],2;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-9;
[37781,[-6707,0,0,0,1,0]~,1,1,
      [9934,7768,-4682,-17248,18665,-12078]~],1]
27179
Mat([[27179,[-5996,0,0,0,1,0]~,1,1,
      [10104,8864,-2451,5717,-5400,-3876]~],1])
16361
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],2;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],2;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-1;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],1;
```

```
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-4;
[16361,[614,0,0,0,1,0]~,1,1,
     [-6183,-3018,-2610,5978,5744,7412]~],1]
2267
[[53,[-7,0,0,0,1,0]~,1,1,[-21,12,17,-11,-24,10]~],3;
[53,[-2,0,0,0,1,0]~,1,1,[-22,15,20,-9,23,10]~],1;
[53,[2,0, 0,0,1,0]~,1,1,[22,-15,-20,-9,23,10]~],-1;
[53,[7,0,0,0,1,0]~,1,1,[21,-12,-17,-11,-24,10]~],1;
[53,[9,0,0,0,1, 0]~,1,1,[-25,11,16,-3,-22,10]~],-4;
[2267,[855,0,0,0,1,0]~,1,1,[433,150,-991,-60,-759,-378]~],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 $\mathfrak{Q}$.

4.3. **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 $nfgaloisconj$:

τ défini par $x \mapsto -x$,

σ défini par $x \mapsto -1/43020481\,x^5 + 5/6559\,x^3 - 6\,x$,

$\tau \cdot \sigma^2$ défini par $x \mapsto -1/43020481 * x^5 + 5/6559 * x^3 - 5 * x$,

σ^2 défini par $x \mapsto 1/43020481 * x^5 - 5/6559 * x^3 + 5 * x$,

$\tau \cdot \sigma$ défini par $x \mapsto 1/43020481 * x^5 - 5/6559 * x^3 + 6 * x$.

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 :

```
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 :

```
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 :

```
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 (1.3) de $\mathrm{N}_{k_1/k}(\mathfrak{A})$.

4.4. **Evolution du facteur normique pour $\mathbb{Q}(\sqrt{6559})$.** Le 3-groupe des classes du corps miroir $k' = \mathbb{Q}(\sqrt{-3 \cdot 6559})$ est $\mathscr{Cl}_{k'} \simeq (\mathbb{Z}/3\,\mathbb{Z})^2$, 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 $\delta_3(\eta) \geq 1$ (cas analogue au cas de $m = 10942$ du § 2.4).

Considérons le groupe des classes ambigesM_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 $\varepsilon = \mathrm{N}_{k_1/k}(y)$, 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 $\mathscr{cl}_k(\mathfrak{p})$ engendre $\mathscr{Cl}_k$), de $\mathfrak{q}_{53}$ et $\mathfrak{q}_{163}$ (rajoutés par commodité). Or le nombre $y \in k_1$ suivant :

```
Mod(Mod(-718772867073155962663309950739304618254881458965242761610777
748022808885957117737704968186794105796351441782387003630640150141197
788431032978502591085009086578880724752156325579 4/319368996194651583
505768629775038129626414323*y+582117278174738949308664878774940722458
848826348261618137138107888426415201350606031728654287153305269415 2
218746873373546239632503827499737723455106867045611060092573830764 8
948394/319368996194651583505768629775038129626414323,y^2-6559)*x^2
+Mod(135085111841955056137422199655385619621111050141311363211546949
986093001291512487360593830764009509822712411875222525433358232800 7
742711074388814166978010414912867115203832816 36/319368996194651583 50
576862977503812962641432 3*y-109402262146556022102438398230262394707 0
116590967555241901293862411942000367395102671935978250261955354051 0
072960396567557374044772960830089358031078748245257703233303828987 0
73255/319368996194651583505768629775038129626414323,y^2-6559)*x
+Mod(-382451054299018003640087471562523868395359399795366619009943 51
600013480161056807590568709444476433465107850177611862777507305882 31
121562017272617752307656200327245919536166909 1/319368996194651583505
768629775038129626414323*y+309738134203867300907648136875882808215 66
274093760471247395436951307532608307139337982191786808831935731370 76
```

```
9108143702260180553511394963663651519378888792490729241654950722855
7
9/319368996194651583505768629775038129626414323,y^2-6559),
x^3-3*x+Mod(1,y^2-6559))
```

a pour norme relative le nombre entier $x \in k$ suivant :

```
Mod(68323557884764791769090883935119570 25*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).

Remarques 4.1. (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 [4, 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 groupe des 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 $m \geq n$, les normes $\mathrm{N}_{k_m/k_n} : \mathcal{C}\ell_{k_m} \longrightarrow \mathcal{C}\ell_{k_n}$ sont surjectives, $\#\mathcal{C}\ell_{k_n}$ est fonction croissante de n, mais avec la contrainte $M_1^n = \#\mathcal{C}\ell_{k_n}^{G_n} = 3^5$ 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 $\#\mathcal{T}_k$.

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

5. Conclusion

Le schéma du § 1.1 indique que $\mathcal{T}_k$ joue le rôle d'espace de probabilité dans le cadre de l'algorithme de dévissage des $M^n = \mathcal{C}\ell_{k_n}$; en effet, la partie $\mathcal{C}\ell_k$ contrôle le premier facteur de (1.4) (le « facteur classes »), et la partie régulateur $\mathcal{R}_k = U_k^*/\overline{E}_k$ contrôle le second (le « facteur normique »).

L'ordre du groupe M_1^n n'est probabiliste qu'au niveau des valeurs des invariants classes et unités du corps k (totalement réel et p-décomposé) car donné par la formule de Chevalley et de plus égal ici à $\#\mathcal{T}_k$ pour tout $n \geq e$, où p^e est l'exposant de $U_k^*/\overline{E}_k$ [4, Théorème 4.7]. Mais pour un tel corps k, pris « au hasard », $\mathcal{T}_k$ peut être égal à 1 (cas des corps p-rationnels) ou non, et il serait intéressant de savoir si $\#\mathcal{T}_k$ (pour p fixé) peut être borné ou non en fonction du discriminant par exemple (les exemples donnés au

§ 3.2 (iii) donnant des discriminants tendant vers l'infini). Des informations probabilistes à ce sujet pourraient indiquer que les ordres des M_i^n ont un comportement analogue.

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 $i > 1$, *tendent rapidement vers* 1, *indépendamment de* n, selon des lois binomiales sur les pas successifs, $1 < i \leq m_n$, tout en étant fonction de plusieurs paramètres de type corps de classes comme certains exemples l'ont montré en faisant intervenir le corps miroir.

Ceci rend crédible l'hypothèse et les heuristiques que nous avions données [4, Hypothèse 7.1, Heuristiques 7.5, 7.6] dont nous rappelons l'essentiel pour un corps k p-décomposé totalement réel de degré d :

(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* $\frac{1}{\#\mathcal{C}\ell_k}$.

(ii) *La probabilité que, pour un* $x \in \Lambda_i^n$*, on ait* $\delta_{\mathfrak{p}}(x) \geq r$*, pour tout* $\mathfrak{p} \mid p$*, est* $\frac{1}{p^{\,r\,(d-1)}}$.

(iii) *Il existe* $i_0 \gg 0$*, indépendant de* n*, tel que* $\mathrm{N}_{k_n/k}(M_{i_0}^n) = \mathcal{C}\ell_k$ *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 :

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* $n \gg 0$.

Remarque 5.1. L'existence de $i_0 \gg 0$, *indépendant de* $n \to \infty$, stopant les algorithmes, peut paraître arbitraire à première vue car les liens numériques entre les étages n et $m \geq n$ semblent difficilement analysables (à l'exeption du (iv) du § 3.2), mais au contraire, cette existence est notablement renforcée par le résultat théorique (mais non effectif) de Jaulent [8, Théorème 7, § 1.4], d'après les techniques de classes logarithmiques de [7], disant, sous la seule conjecture de Leopoldt, que :

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_∞.

Or si $\widetilde{\mathcal{C}\ell}_k$ capitule dans k_n, il capitule dans k_m pour tout $m \geq n$. Il y a probablement un lien concret entre le k_{n_0} de capitulation 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'algorithmes de dévissages des M_i^n.

On pourrait également traiter le cas où il n'existe qu'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 mixte d'une décomposition partielle, mis à part l'aspect technique, il est clair que les mêmes heuristiques s'appliquent ; en outre le résultat de Jaulent ne fait aucune hypothèse de décomposition.

Le comportement des $\mathcal{C}\ell_{k_n}$ dans la tour ne dépend donc pas uniquement de *circonstances algébriques à la Iwasawa*, mais de phénomènes arithmétiques

p-adiques subtils qui semblent pouvoir se lire de façon probabiliste au moyen des invariants habituels du corps de base 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 totalement réels*.

Références

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

[2] G. Gras – *Class Field Theory: from theory to practice*, SMM, Springer-Verlag, 2003; second corrected printing 2005.https://www.researchgate.net/publication/268005797

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

[4] G. Gras – Approche p-adique de la conjecture de Greenberg pour les corps totalement réels, *Annales Mathématiques Blaise Pascal* 2017 (à paraître).

[5] G. Gras – The p-adic Kummer–Leopoldt Constant – Normalized p-adic Regulator, *International Journal of Number Theory* 2018 (to appear).

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

[7] J-F. Jaulent – Théorie ℓ-adique globale du corps de classes, *J. Théorie des Nombres de Bordeaux* **10** (1998), no. 2, p. 355–397.http://www.numdam.org/article/JTNB_1998__10_2_355_0.pdf

[8] J-F. Jaulent – Note sur la conjecture de Greenberg, *J. Ramanujan Math. Soc.* (2017) (to appear).https://arxiv.org/abs/1612.00718

[9] T. Nguyen Quang Do – Formules de genres et conjecture de Greenberg, *Ann. Math. Québec* 2018 (à paraître).https://www.researchgate.net/publication/311846783

[10] M. Ozaki – The class group of $\mathbb{Z}_p$-extensions over totally real number fields, *Tohoku Math. J.* 49 (1997), p. 431-435.https://projecteuclid.org/download/pdf_1/euclid.tmj/1178225114

[11] The PARI Group – PARI/GP version `2.9.0`, *Université de Bordeaux* (2016).http://pari.math.u-bordeaux.fr/.

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

[13] H. Taya – On cyclotomic $\mathbb{Z}_p$-extensions of real quadratic fields, *Acta Arithmetica*, 74 (1996), no. 2, p. 107–119.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`