



**HAL**  
open science

# CONJECTURE DE GREENBERG

Georges Gras

► **To cite this version:**

Georges Gras. CONJECTURE DE GREENBERG : hypothèses p-adiques sur les normes d'idéaux. 2017. hal-01546656v1

**HAL Id: hal-01546656**

**<https://hal.science/hal-01546656v1>**

Preprint submitted on 25 Jun 2017 (v1), 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.

# CONJECTURE DE GREENBERG

## HYPOTHÈSES $p$ -ADIQUES SUR LES NORMES D'IDÉAUX

GEORGES GRAS

ABSTRACT. Soit  $k$  un corps de nombres totalement réel et soit  $k_\infty$  sa  $\mathbb{Z}_p$ -extension cyclotomique pour  $p$  totalement décomposé dans  $k$ . Ce texte complète notre article intitulé : “Approche  $p$ -adique de la conjecture de Greenberg pour les corps totalement réels” (Annales Mathématiques Blaise Pascal 2017), au moyen d’heuristiques sur le comportement  $p$ -adique des normes, dans  $k_n/k$ , des idéaux de  $k_n$  ( $n$ -ième étage de  $k_\infty$ ) : une hypothèse de répartition de ces normes 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  $k_\infty$  be its cyclotomic  $\mathbb{Z}_p$ -extension for  $p$  totally split in  $k$ . This text completes our article entitled: “Approche  $p$ -adique de la conjecture de Greenberg pour les corps totalement réels” (Annales Mathématiques Blaise Pascal 2017), by means of heuristics on the  $p$ -adic behavior of the norms, in  $k_n/k$ , of the ideals of  $k_n$  ( $n$ th stage of  $k_\infty$ ): an assumption of distribution of these norms 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 [3], nous avons posé une hypothèse de répartition  $p$ -adique des normes d'idéaux,  $N_{k_n/k}(\mathfrak{A})$ , dans la tour cyclotomique  $k_\infty = \bigcup_{n \geq 0} k_n$  d'un corps de nombres totalement réel  $k$ ,  $p$ -décomposé, pour justifier les obstructions  $p$ -adiques à une preuve, dans le seul cadre de la théorie d'Iwasawa algébrique, de la conjecture de Greenberg [6] : il s'agit de l'Hypothèse 1.3 rappelée à la fin du § 1.2 (pour un historique sur la conjecture de Greenberg, se reporter à la bibliographie de [3] ainsi qu'aux récents points de vue de [8] et [9]).

---

*Date:* 24 Juin 2017.

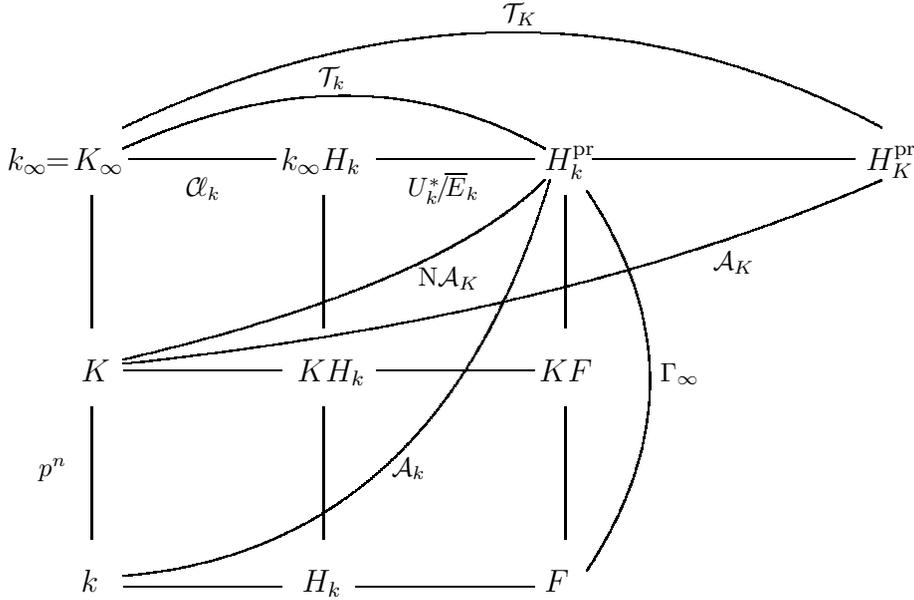
*1991 Mathematics Subject Classification.* 11R23, 11R29, 11R37; 11Y40.

*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 vérifiant la conjecture de Leopoldt et totalement décomposé dans  $k$ .

On désigne par  $\mathcal{C}_k$  le  $p$ -groupe des classes de  $k$  et par  $E_k$  son groupe des unités. Soit  $U_k^*$  le  $\mathbb{Z}_p$ -module libre de rang  $d - 1$  formé des unités locales principales de  $k$  en  $p$ , de norme 1 sur  $\mathbb{Q}$  ; 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  $U_k^*$ .

Soit  $K := k_n$ , de degré  $p^n$  sur  $k$ , le  $n$ -ième étage de la  $\mathbb{Z}_p$ -extension cyclotomique  $k_\infty$  de  $k$  ; c'est une extension Galoisienne réelle de  $\mathbb{Q}$ . On considère (sous la conjecture de Leopoldt pour  $p$  dans  $k_\infty$ ) le schéma ci-après (dit de la  *$p$ -ramification Abélienne sur  $k$* ), où  $H_k^{\text{pr}}$  et  $H_K^{\text{pr}}$  sont les pro- $p$ -extensions Abéliennes  $p$ -ramifiées (i.e., non ramifiées en dehors de  $p$ ) maximales, de  $k$  et  $K$ . On a fixé une extension  $F$  de  $k$ , contenant le  $p$ -corps de classes de Hilbert  $H_k$  de  $k$ , telle que  $H_k^{\text{pr}}$  soit le composé direct de  $F$  et  $k_\infty$  sur  $k$ , et on pose  $\Gamma_\infty = \text{Gal}(H_k^{\text{pr}}/F)$  :



Introduisons les symboles d'Artin  $(\frac{H_k^{\text{pr}}/k}{\cdot})$  et  $(\frac{H_K^{\text{pr}}/K}{\cdot})$  sur  $\mathcal{J}_k := I_k \otimes \mathbb{Z}_p$  et  $\mathcal{J}_K := I_K \otimes \mathbb{Z}_p$ , où  $I_k$  et  $I_K$  sont les groupes des idéaux étrangers à  $p$  de  $k$  et  $K$ . Leurs images sont les groupes de Galois  $\mathcal{A}_k$  et  $\mathcal{A}_K$  qui sont des  $\mathbb{Z}_p$ -modules de type fini ; les noyaux de ces symboles d'Artin 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  $(x_\infty)$  où  $x_\infty \in k^\times \otimes \mathbb{Z}_p$  est étranger à  $p$  et d'image diagonale triviale dans le groupe  $U_k$  des unités locales principales de  $k$  en  $p$ , et de même avec  $K$  (cf. [2, Theorem III.2.4, Proposition III.2.4.1], [7, § 2]).

Les groupes  $\mathcal{T}_k$  et  $\mathcal{T}_K$  sont les groupes de torsion de  $\mathcal{A}_k$  et  $\mathcal{A}_K$ . Pour un corps  $k$  totalement réel,  $\#\mathcal{T}_k$  est donné par la formule de Coates [1], en relation avec le résidu de la fonction  $\zeta$   $p$ -adique de  $k$  (cf. [11]).

L'application norme arithmétique  $N_{K/k} : \mathcal{J}_K \rightarrow \mathcal{J}_k$  induit, via les symboles d'Artin, la restriction  $\mathcal{A}_K \rightarrow \mathcal{A}_k$  (notée encore  $N_{K/k}$ ) qui s'exprime par la suite exacte suivante, où  $N_{K/k}(\mathcal{A}_K)$  est d'indice  $p^n$  dans  $\mathcal{A}_k$  :

$$1 \rightarrow \text{Gal}(H_K^{\text{pr}}/H_k^{\text{pr}}) \longrightarrow \mathcal{A}_K \longrightarrow N_{K/k}(\mathcal{A}_K) = \Gamma_\infty^{p^n} \oplus \mathcal{T}_k \longrightarrow 1.$$

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

$$(1.1) \quad N_{K/k}(\mathfrak{A}) = \mathfrak{a}^{p^n} \cdot \mathfrak{t} \cdot (x_\infty), \quad \mathfrak{a}, \mathfrak{t} \in \mathcal{J}_k, \quad \left(\frac{H_k^{\text{pr}}/k}{\mathfrak{a}}\right) \in \Gamma_\infty, \quad \left(\frac{H_k^{\text{pr}}/k}{\mathfrak{t}}\right) \in \mathcal{T}_k.$$

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

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

**1.2. Algorithme de filtration des groupes de classes  $\mathcal{C}_{k_n}$ .** 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  $\mathcal{C}_K$  par dévissage, on dispose d'une filtration, au moyen de sous-groupes :

$$M_i^n = \mathcal{C}_K(\mathcal{I}_i^n), \quad 0 \leq i \leq m_n, \quad \mathcal{I}_i^n \subset I_K,$$

ainsi définie avec  $M^n := \mathcal{C}_K$  (d'après [3, § 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 (avec  $M_0^n := 1$ ) 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  $K/k$  dont l'ordre est donné par la formule de Chevalley).

(ii) On a  $M_{i+1}^n = \{c \in M^n, c^{1-\sigma} \in M_i^n\}$  ; ainsi, pour tout  $i$ ,

$$M_i^n = \{c \in M^n, c^{(1-\sigma)^i} = 1\}.$$

(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  $N_{K/k}(\mathcal{I}_i^n)$  ( $n \gg 0$ ), qui représentent  $N_{K/k}(M_i^n) \subseteq \mathcal{C}_k$ , sont engendrés, modulo des  $(\alpha)$  “quasi-infinitésimaux” (i.e.,  $\alpha$  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 :

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

qui contiennent  $E_k$ , sont obtenus via les idéaux principaux  $(x)$  qui se déduisent du sous-module engendré par les composantes  $\mathfrak{t}$  des  $N_{K/k}(\mathfrak{B})$ ,  $\mathfrak{B} \in \mathcal{I}_i^n$  (cf. (1.1)). Rappelons enfin que, pour  $n \geq 1$  fixé, une généralisation de la formule des classes ambiguës de Chevalley, que nous avons redonnée dans [4], conduit à la  $i$ -suite d’entiers définie par :

$$(1.2) \quad \#(M_{i+1}^n/M_i^n) = \frac{\#\mathcal{C}_k}{\#N_{K/k}(M_i^n)} \cdot \frac{p^{n \cdot (d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap N_{K/k}(K^\times))},$$

où

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

seront appelés respectivement *le facteur classes* et *le facteur normique*.

Comme  $\#\mathcal{C}_K = \prod_{i=0}^{m_n-1} \#(M_{i+1}^n/M_i^n)$ , la conjecture de Greenberg revient à estimer le nombre de pas  $m_n$  de l’algorithme puisque, d’après [3, Théorème 6.3], on a sur  $m_n$  les inégalités fondamentales suivantes (lorsque  $\mathcal{T}_k \neq 1$ ) :

$$(1.3) \quad \lambda \cdot n + \mu \cdot p^n + \nu \geq m_n \geq \frac{1}{v_p(\#\mathcal{T}_k)} (\lambda \cdot n + \mu \cdot p^n + \nu),$$

pour tout  $n \gg 0$ , où  $\lambda, \mu, \nu$  sont les invariants d’Iwasawa et  $v_p$  la valuation  $p$ -adique. Il est donc équivalent que  $m_n$  soit borné lorsque  $n \rightarrow \infty$  pour que  $\lambda = \mu = 0$  (rappelons que  $\mathcal{T}_k = 1$  implique trivialement  $\lambda = \mu = \nu = 0$  ; c’est même équivalent dans le cas  $p$ -décomposé).

Or  $m_n$  (pour  $n$  fixé) dépend de la progression des deux facteurs de l’expression (1.2), et on constate en pratique que, sous réserve de probabilités naturelles de répartition des éléments de  $\mathcal{T}_k$  en relation avec la formule 1.1, chacun des deux facteurs est rapidement trivial.

On rappelle les résultats suivants [3, Lemme 7.1], où  $i$  est ici fixé :

(i) La  $n$ -suite  $\frac{\#\mathcal{C}_k}{\#N_{k_n/k}(M_i^n)} =: p^{c_i^n}$  est *croissante* stationnaire à une valeur maximale notée  $p^{c_i^\infty} \mid \#\mathcal{C}_k$ .

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  $\mathcal{C}_k(N_{k_n/k}(\mathfrak{A})) = \mathcal{C}_k(\mathfrak{t})$  (où  $\mathfrak{A}$  est un “idéal aléatoire de  $k_n$ ” et  $\mathfrak{t}$  la composante donnée par (1.1)), se répartissent de façon uniforme dans le groupe des classes de  $k$ .

(ii) La  $n$ -suite  $\frac{p^{n \cdot (d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap N_{k_n/k}(k_n^\times))} =: p^{\rho_i^n}$  est *croissante* stationnaire à une valeur maximale notée  $p^{\rho_i^\infty} \mid R_k := U_k^*/\overline{E}_k$ , le “régulateur  $p$ -adique normalisé” de  $k$ , défini en toute généralité dans [5]).

On a  $(\Lambda_i^n : \Lambda_i^n \cap N_{k_n/k}(k_n^\times)) = p^{n \cdot (d-1)}$  (i.e.,  $p^{\rho_i^n} = 1$  pour tout  $i \geq i_2$  convenable) dès que les symboles de Hasse de suffisamment de nombres  $x \in \Lambda_i^n$  engendrent  $\Omega(k_n/k)$  qui est le sous-groupe, de la somme directe  $\bigoplus_{\mathfrak{p} \mid p} I_{\mathfrak{p}} = G_n^{d-1}$  des groupes d’inertie  $I_{\mathfrak{p}}$ , formé des familles  $\left(\left(\frac{x, k_n/k}{\mathfrak{p}}\right)\right)_{\mathfrak{p} \mid p}$  vérifiant la formule 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  $p$  :

$$(1.4) \quad \frac{x^{p-1} - 1}{p} =: \prod_{\mathfrak{p} \mid p} \mathfrak{p}^{\delta_{\mathfrak{p}}(x)} \cdot \mathfrak{b}(x), \quad \delta_{\mathfrak{p}}(x) \geq 0, \mathfrak{b}(x) \text{ étranger à } p.$$

L’ordre de  $\left(\frac{x, k_n/k}{\mathfrak{p}}\right)$  étant  $p^{n - \delta_{\mathfrak{p}}(x)}$  pour  $n$  assez grand (cf. [3, 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  $(x) = N_{k_n/k}(\mathfrak{A})$ ,  $\mathfrak{A} \in \mathcal{I}_i^n$  (i.e.,  $x \in \Lambda_i^n$ ), on aura, d’après la relation (1.1),

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

où, pour  $n \gg 0$ , le nombre  $\alpha$  est “négligeable” quant à ses  $\delta_{\mathfrak{p}}(\alpha)$  ; les  $\delta_{\mathfrak{p}}(x)$ ,  $\mathfrak{p} \mid p$ , ne dépendent alors que de l’idéal principal  $\mathfrak{t}$  que nous notons encore  $(x)$  par abus.

Nous avons formulé dans [3, Hypothèse 7.1] les hypothèses suivantes 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  $\#\mathcal{C}_K$ , définissent une variable aléatoire, et qu’il en est de même pour la composante  $\mathfrak{t}$  de  $N_{K/k}(\mathfrak{A})$ . Enfin on suppose que les symboles de Frobenius  $\left(\frac{F/k}{\mathfrak{t}}\right)$  se répartissent uniformément dans  $\text{Gal}(F/k) \simeq \mathcal{T}_k$ .*

Si ces hypothèses sont vérifiées, ceci a les conséquences suivantes :

- (i) Les classes des idéaux  $\mathfrak{t}$  sont réparties uniformément dans  $\mathcal{C}_k$ .
- (ii) Lorsque  $\mathfrak{t} = (x)$ , puisque  $\text{Gal}(F/H_k) \simeq \text{Gal}(H_k^{\text{pr}}/k_\infty H_k) \simeq U_k^*/\overline{E}_k$  est d’exposant fini (noté  $p^e$ ), on a  $x^{p^e} = x_\infty \cdot \varepsilon$ , avec  $\varepsilon \in E_k \otimes \mathbb{Z}_p$  et  $x_\infty$  infinitésimal (donc  $N_{k/\mathbb{Q}}(x) = 1$  dans  $U_{\mathbb{Q}}$  et l’image de  $x$  est définie dans  $U_k^*/\overline{E}_k$ ) ; par conséquent,  $x$  modulo  $\overline{E}_k$  parcourt uniformément un ensemble fini, ainsi que les  $\delta_{\mathfrak{p}}(x)$  modulo  $\delta_{\mathfrak{p}}(E_k)$ .

Pour  $k$  quadratique,  $\delta_{\mathfrak{p}}(x)$  est indépendant de  $\mathfrak{p} \mid p$  pour  $x$  étranger à  $p$  et nous écrirons  $\delta_p(x)$  ; sinon on doit préciser  $\mathfrak{p}$  pour les  $S_k$ -unités où  $S_k$  est l’ensemble des  $p$ -places de  $k$  (cf. [3, Définition 4.1 & §5.1]).

(iii) En résumé, l’heuristique principale utilisée dans [3] 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*. Ceci est conforté par le fait que si  $\mathcal{T}_k = 1$  (i.e.,  $p$ -rationalité de  $k$ ), alors *pour des raisons triviales* la conjecture est vérifiée sous la forme forte de nullité des invariants  $\lambda, \mu, \nu$  d’Iwasawa (de fait, d’après [3, Théorème 4.7], on a  $\#\mathcal{C}_{k_n}^{G_n} = \#\mathcal{T}_k$  pour tout  $n \gg 0$ ).

On notera que les limites  $p^{c_i^\infty + \rho_i^\infty}$  des  $n$ -suites  $\#(M_{i+1}^n/M_i^n)$ ,  $n \rightarrow \infty$ , constituent une  $i$ -suite *décroissante stationnaire* de diviseurs de  $\#\mathcal{T}_k$  (cf. [3, Lemme 7.2]) et que 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 “boucle”  $O(\lambda \cdot n + \mu \cdot p^n)$  fois de suite (cf. 1.3), ce qui constitue un non-sens numérique mais suggère l’immense difficulté pour établir une contradiction.

## 2. STATISTIQUES SUR LES IDÉAUX $N_{K/k}(\mathfrak{A})$

On se place dans le cas quadratique réel  $k = \mathbb{Q}(\sqrt{m})$ ,  $p > 2$  totalement décomposé, et on utilise des programmes PARI [10] pour les calculs. On suppose que l’unité fondamentale  $\varepsilon$  est telle que  $\delta_p(\varepsilon)$  (cf. (1.4)) est assez grand afin que, lorsque  $x$  (étranger à  $p$  et norme locale en dehors de  $p$  dans  $k_n/k$ )<sup>1</sup> 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  $\delta_p(\varepsilon) = r \ll n$  et  $\delta_p(x) < r$ , alors  $\delta_p(x \cdot \varepsilon') = \delta_p(x)$  quelle que soit  $\varepsilon' \in E_k$ , alors que si  $\delta_p(x) = r$ ,  $\delta_p(x \cdot \varepsilon^a)$ ,  $a \in \mathbb{Z}$ , peut prendre toute valeur entre  $r$  et  $n$ .

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  $R_k \sim \frac{1}{p} \log(\varepsilon) \sim p^{\delta_p(\varepsilon)}$  ; 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  $p = 3$ .

**2.1. Programme général calculant  $h, \delta_{\mathfrak{p}}(\eta_3), \delta_3(\varepsilon)$ .** 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  $\delta_{\mathfrak{p}}(\eta_3)$ ,  $\mathfrak{p} \mid 3$ ,

---

<sup>1</sup>Ceci a toujours lieu pour les  $x \in \Lambda_i^n$  qui sont par nature des normes d’idéaux dans  $k_n/k$ , auquel cas,  $N_{k/\mathbb{Q}}(x) \equiv 1 \pmod{p^n}$  lorsque  $x$  est étranger à  $p$ . Lorsque  $x$  est une  $S_k$ -unité, la condition normique en dehors de  $p$  est toujours vérifiée.

où  $\eta_3$  est une  $S_k$ -unité fondamentale (qui est donnée par  $\mathfrak{p}^{h'} = (\eta_3)$  où  $h'$  est l'ordre de  $\mathcal{C}_k(\mathfrak{p})$ ).

On teste la condition suffisante (cf. [3, Théorème 3.4]) conduisant à  $\lambda = \mu = 0$  pour  $k$  quadratique (condition qui équivaut à la trivialité du groupe des classes logarithmiques  $\tilde{\mathcal{C}}_k$  introduit dans [8]) :

- (i)  $\mathcal{C}_k^{S_k} = 1$  (i.e.,  $\mathfrak{p} \mid 3$  engendre le 3-groupe des classes de  $k$ ),
- (ii)  $\delta_3(\varepsilon) \geq 1$  &  $\delta_{\mathfrak{p}}(\eta_3) \geq 1$ .

On impose par commodité que  $h$  soit puissance de 3 et on fixe un ordre de grandeur à  $\delta_3(\varepsilon)$  (bd =  $3^{-k}$  signifiant  $\delta_3(\varepsilon) > k$ ) :

```
{p=3;m=1;n=8;n0=n+1;bd=1/p^2;while(m<2*10^5,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);E=quadunit(M);
h=qfbcassno(M);vh=valuation(h,p);if(vh>=1 & h==p^vh,y=x;
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<bd,print(" ");
if(zpi+ze<1,print("PROBLEME-NORMIQUE"));
if(delta!=0,print("PROBLEME-CLASSES"));
print("m=",m," h=",h," E=",E);
print("p=",p," S=",pi1," ",pi2);print(zpi," ",ze));x=y)}}}
```

**2.2. Méthode générale à partir d'idéaux premiers.** On souhaite établir des statistiques sur l'influence des  $N_{K/k}(\mathfrak{A}) \in N_{K/k}(\mathcal{I}_i^n)$  de l'algorithme sur le facteur classes et sur le facteur normique de (1.2).

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  $H_k/\mathbb{Q}$ ). Il en résulte que, comme une relation de la forme  $\mathfrak{A} = \mathfrak{L} \cdot (\alpha)$  dans  $K$  implique, dans  $k$  :

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

le fait de supposer les idéaux  $\mathfrak{A}$  premiers est sans conséquences sur l'étude statistique des deux facteurs de l'expression (1.2) ; en effet, le premier facteur est relatif aux *classes des*  $N_{K/k}(\mathfrak{A})$  et le second aux *indices normiques* ( $\Lambda_i^n : \Lambda_i^n \cap N_{K/k}(K^\times)$ ) qui ne dépendent pas du choix des  $x \in \Lambda_i^n$ , modulo  $E_k \cdot N_{K/k}(K^\times)$  (cf. [3, § 6.2]).

On considère donc un grand nombre de premiers  $\ell$  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  $\mathfrak{l} := N_{K/k}(\mathfrak{L})$  sont les variables aléatoires qui “conduisent l’algorithme” à chaque étape (cf. § 3.1).

On peut donc supposer  $N_{K/k}(\mathcal{I}_i^n)$  engendré par des  $\mathfrak{l}_j = N_{K/k}(\mathfrak{L}_j)$  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  $\langle \mathcal{C}_k(\mathfrak{l}_j) \rangle_j$  de  $\mathcal{C}_k$  dont la croissance algorithmique, en fonction du nombre de pas, est censée atteindre  $\mathcal{C}_k$  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  $r_\ell$  est l’ordre de la classe de  $\mathfrak{l}$ , on posera  $\mathfrak{l}^{r_\ell} = (\eta_\ell)$ , où  $\eta_\ell$  est une  $\ell$ -unité (définie modulo  $E_k$ ), puis on calculera  $\delta_3(\eta_\ell)$ . Comme  $N_{k/\mathbb{Q}}(\eta_\ell) = \pm \ell^{r_\ell} \equiv \pm 1 \pmod{3^{n+1+r_\ell}}$ , on pourra négliger la conjugaison dans  $k/\mathbb{Q}$  et travailler avec un unique idéal premier  $\mathfrak{l} \mid \ell$  et une unique  $\eta_\ell$ .

Ensuite, si l’on constate que les entiers  $\delta_3(\eta_\ell)$  (modulo  $\delta_3(\varepsilon)\mathbb{Z}$ ) 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”  $\mathfrak{l}^{r_\ell} = (\eta_\ell)$  ne donnent qu’une partie des  $x \in \Lambda_i^n$  susceptibles d’être normes dans  $K/k$ .

On peut cependant donner un aperçu de la question et faire des statistiques sur les relations en considérant un petit nombre de  $\ell_j$ , 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 “VIDE” 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  $\ell_j$  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;vide=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,vide=vide+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," ",vide," ",vide/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 précédent) :

```

m=7249, h=3, E=170524677024744665220*x+14518651659981320194199
p=3, S={131480821*x-11194416394,131480821*x+11194416394}
1 1/81

```

pour lesquelles  $\delta_p(\eta_3) = 0$  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 :  $N_n = 10720$ ,  $\text{VIDE} = 454$ , 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.

**2.3. Etude des facteurs de la relation (1.2) ( $m = 72262$ ).** On a :

$$\varepsilon = 632566365854478210 \cdot \sqrt{m} + 170043910956651732101,$$

et la 3-unité fondamentale  $\eta_3 = -1037963 \cdot \sqrt{m} + 279020981$ .

On a  $\delta_p(\eta_3) = 0$ ,  $\delta_3(\varepsilon) = 4$ ,  $\mathcal{C}_k \simeq \mathbb{Z}/9\mathbb{Z}$  est engendré par  $\mathfrak{p} \mid 3$  (on a aussi  $\mathcal{C}_{k_1} \simeq \mathbb{Z}/27\mathbb{Z}$  et  $\mathcal{C}_{k_2} \simeq \mathbb{Z}/81\mathbb{Z}$ ). 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  $\ell$  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  $\ell$  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  $\eta_\ell$ , où  $\mathfrak{l}$  est un idéal premier de  $k$  au-dessus de  $\ell$ , 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  $r$  (on peut éviter cette répétition en faisant deux programmes si nécessaire, notamment si  $r$  peut prendre beaucoup de valeurs).

Les nombres  $NL_1, NL_3, NL_9$  représentent respectivement le nombre de premiers  $\ell \leq B = 2 \cdot 10^{12}$  totalement décomposés dans  $K/k$  tels que la classe de  $\mathfrak{l} = N_{K/k}(\mathfrak{L})$  soit d'ordre  $r = 1, 3, 9$ . Les proportions correspondantes sont comparées aux probabilités naturelles  $\frac{1}{9}, \frac{2}{9}, \frac{6}{9}$ .

On a  $N_L = NL_1 + NL_3 + NL_9$  (nombre de  $\ell$  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 classe pour  $m = 72262$ .* On obtient :

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

et le tableau des proportions :

proportions	probabilités
$NL_1/NL = 0.1111195675$	$\frac{2}{9} = 0.1111111111$
$NL_3/NL = 0.2221066179$	$\frac{3}{9} = 0.2222222222$
$NL_9/NL = 0.6667738145$	$\frac{6}{9} = 0.6666666666$

Il est clair que l'heuristique de répartition uniforme est vérifiée.

Ceci traduit le comportement du facteur classes de l'expression (1.2) 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  $\mathcal{C}_k(\mathfrak{l})$  principales et calcul des  $\delta_3(\eta_\ell)$ .

On obtient  $NL_1 = 620512$ ,  $C_0 = 412997$ ,  $C_1 = 137911$ ,  $C_2 = 46166$ ,  $C_3 = 15833$ ,  $C_4 = 5090$ ,  $C_5 = 2515$ , et le tableau :

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

(ii) Dénombrement des  $\mathcal{C}_k(\mathfrak{l})$  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  $\mathcal{C}_k(\mathfrak{l})$  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  $\varepsilon$  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, ce qui justifie de façon radicale l'heuristique sur le comportement du second facteur de l'expression (1.2) qui se trivialisent plus facilement puisque  $\delta_3(\eta_\ell) = 0$  équivaut à un symbole de Hasse d'ordre  $3^n$ . Mais ceci dépend de l'arithmétique de  $k$ .

2.4. **Etude des facteurs de la relation (1.2) ( $m = 10942$ ).** On a :

$$\varepsilon = 110617476121372232880 \cdot \sqrt{m} + 11571032155720815417599,$$

et une 3-unité fondamentale  $\eta_3 = -890711 \cdot \sqrt{m} + 93171947$ .

On a  $\delta_p(\eta_3) = 1$ ,  $\delta_3(\varepsilon) = 6$ ,  $h = 3$ ,  $\mathcal{C}_k \simeq \mathbb{Z}/3\mathbb{Z}$  et  $\mathcal{C}_{k_1} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .

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, sauf que ici  $r \in \{1, 3\}$ . Les nombres  $NL_1$ ,  $NL_3$  représentent respectivement le nombre de premiers  $\ell \leq B = 2 \cdot 10^{12}$  totalement décomposés dans  $K/k$  tels que la classe de  $\mathfrak{l} = N_{K/k}(\mathfrak{L})$  soit d'ordre  $r = 1, 3$ . Les proportions correspondantes sont comparées aux probabilités naturelles  $\frac{1}{3}, \frac{2}{3}$ .

On désigne encore par  $C_0, C_1, C_2, C_3, C_4, C_5$  les nombres de  $\ell$  tels que  $\delta_3(\eta_\ell) = 0, 1, 2, 3, 4, \geq 5$  respectivement.

On a  $NL = NL_1 + NL_3$ .

```
{p=3;m=10942;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;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);

r=1;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);
print(CL1/NL+0.0," ",CL3/NL+0.0);print(1./3," ",2./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  $r \in \{1, 3\}$  : on a  $NL = 5587470$ ,  $NL_1 = 1862666$ ,  $NL_3 = 3724804$ , et pour les proportions :

proportions	probabilités
$NL_1/NL = 0.333364832$	$\frac{2}{3} = 0.333333333$
$NL_3/NL = 0.6666351676$	$\frac{1}{3} = 0.666666666$

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
$C_0/NL_1 = 0.6663696014$	$\frac{1}{3^2} = 0.6666666666$
$C_1/NL_1 = 0.2224070230$	$\frac{2}{3^3} = 0.2222222222$
$C_2/NL_1 = 0.0741109785$	$\frac{4}{3^4} = 0.0740740740$
$C_3/NL_1 = 0.0246039816$	$\frac{8}{3^5} = 0.0246913580$
$C_4/NL_1 = 0.0083079843$	$\frac{16}{3^6} = 0.0082304526$
$C_5/NL_1 = 0.0042004309$	$\sum_{j \geq 6} \frac{1}{3^j} = 0.0041152264$

(ii) Dénombrement des  $\mathcal{C}_k(\mathfrak{l})$  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
$C_0/NL_3 = 0.0000000000$	$\frac{1}{3^2} = 0.0000000000$
$C_1/NL_3 = 0.6668995200$	$\frac{2}{3^3} = 0.6666666666$
$C_2/NL_3 = 0.2221738378$	$\frac{4}{3^4} = 0.2222222222$
$C_3/NL_3 = 0.0739002642$	$\frac{8}{3^5} = 0.0740740740$
$C_4/NL_3 = 0.0246915005$	$\frac{16}{3^6} = 0.0246913580$
$C_5/NL_3 = 0.0123348772$	$\frac{32}{3^7} = 0.0123450517$

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 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  $\mathfrak{l}^3 = (b)$ ,  $\delta_3(b) \geq 1$ .<sup>2</sup> 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 du groupe  $\mathcal{T}_L$  est égal à :

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

où  $S_L$  est l'ensemble des 3-places de  $L$ . Or  $\mathcal{C}_L^{S_L}$  est la somme directe de  $\mathcal{C}_k^{S_k} = 1$  (car  $S_k$  engendre  $\mathcal{C}_k$ ) et de  $\mathcal{C}_{k'}$  (car  $S_{k'}$  est réduit à une unique 3-places de carré (3)).

<sup>2</sup>On peut même vérifier que la  $S_k$ -unité fondamentale conduit à une extension non ramifiée sur le corps miroir en considérant  $(-890711 \cdot \sqrt{10942} + 93171947) \cdot (\sqrt{10942} - 1)^{-3} = \frac{36686207034}{48507321023} \cdot \sqrt{10942} - \frac{3837524558923}{48507321023} \equiv 1 \pmod{9}$ .

Donc  $\text{rg}_3(\mathcal{T}_L) = 3$  puis, comme  $\mathcal{T}_L = \mathcal{T}_k \oplus \mathcal{T}_{k'}$  et comme  $\text{rg}_3(\mathcal{T}_k) = 1$  [2, Corollary III.4.2.3], on a

$$\text{rg}_3(\mathcal{T}_{k'}) = 2 = \text{rg}_3(\mathcal{C}_{k'}),$$

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 très 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  $\mathcal{C}_k^{S_k} \neq 1$ ,  $\delta_3(\varepsilon)$  &  $\delta_p(\eta_3) \geq 1$ .** On a trouvé les cas suivants (avec  $h = 3$ ), pour lesquels aucun des deux points de la condition suffisante de nullité de  $\lambda$  et  $\mu$  n'est vérifié ; on donne en outre la structure du groupe des classes de  $k_1$  :

(i)  $m = 26893, \varepsilon = 142445225/2 \cdot x + 23359714011/2,$

$$\eta_3 = -x - 164,$$

$$\delta_3(\varepsilon) = 3 \text{ \& } \delta_p(\eta_3) = 3, \text{ structure}=[36, [18, 2]].$$

(ii)  $m = 31069, \varepsilon = 933602804601721/2 \cdot x + 164560570852019805/2,$

$$\eta_3 = -23257 \cdot x + 4099372,$$

$$\delta_3(\varepsilon) = 3 \text{ \& } \delta_p(\eta_3) = 1, \text{ structure}=[27, [3, 3, 3]].$$

(iii)  $m = 92269, \varepsilon = 182039966136652680262184737485085/2 \cdot x$

$$+ 55296119237149041291682191243785961/2,$$

$$\eta_3 = -3397805798209/2 \cdot x - 1032111126747851/2,$$

$$\delta_3(\varepsilon) = 3 \text{ \& } \delta_p(\eta_3) = 1, \text{ structure}=[9, [9]]$$

(iv)  $m = 94918, \varepsilon = 188160617208817500397435811509434 \cdot x$

$$+ 57969962353214358861329455735908197,$$

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

$$\delta_3(\varepsilon) = 3 \text{ \& } \delta_p(\eta_3) = 2, \text{ structure}=[27, [9, 3]]$$

(v)  $m = 171061, \varepsilon = 900555961068792369443990032360047045/2 \cdot x$

$$+ 372465634300948242809059190380968649273/2,$$

$$\eta_3 = 902353/2 \cdot x - 373208881/2,$$

$$\delta_3(\varepsilon) = 4 \text{ \& } \delta_p(\eta_3) = 4, \text{ structure}=[9, [9]].$$

**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  $N_{K/k}(\mathfrak{B}) = N_{K/k}(y)$

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 sont "aléatoires" ou non par rapport aux précédents.

**3.1. Rappels sur l'algorithme de calcul des  $\#\mathcal{C}_K$ .** Une fois le groupe  $\Lambda_i^n$  déterminé, l'étape suivante de l'algorithme consiste à trouver les  $x \in \Lambda_i^n$  normes locales en  $\mathfrak{z}$ , ce qui résulte des valeurs des  $\delta_{\mathfrak{z}}(x)$  (cf. (1.4)) selon le fait que l'ordre de  $\left(\frac{x, K/k}{\mathfrak{p}}\right)$  est  $3^{n-\delta_{\mathfrak{z}}(x)}$  et que ce symbole engendre  $G_n$  si et seulement si  $\delta_{\mathfrak{z}}(x) = 0$ , auquel cas l'algorithme ne dépend plus que du premier facteur (facteur classes).

On pose :

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

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  $\mathfrak{A}$ , 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"). 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  $N_{K/k}(\mathfrak{A}) \in N_{K/k}(\mathcal{I}_{i+1}^n)$  et  $\Lambda_{i+1}^n$ , afin de prendre les  $x' \in \Lambda_{i+1}^n$  tels que  $x'$  soit la norme d'un  $y' \in K^\times$ , etc.

Le problème posé au sujet du théorème des normes de Hasse est très général et peut s'aborder pour une extension  $K/k$ , cyclique, quelconque, de groupe de Galois  $G$  engendré par  $\sigma$ .

**Lemme 3.1.** *Sans modifier l'algorithme ni les statistiques, on peut supposer que  $\mathfrak{B}$  est un idéal premier  $\mathfrak{L}$  totalement décomposé dans  $K/\mathbb{Q}$ . Dans la relation  $(y) = \mathfrak{L} \cdot \mathfrak{A}^{1-\sigma}$  qui s'en déduit, on peut supposer que  $\mathfrak{A}$  est un idéal premier  $\mathfrak{Q}$ , totalement décomposé dans  $K/\mathbb{Q}$ .*

*Démonstration.* On sait que l'on peut choisir  $x \in \Lambda_i^n$  modulo  $N_{K/k}(K^\times)$  pour l'algorithme, 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  $N_{K/k}(\mathfrak{A})$  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  $N_{K/k}(\mathfrak{Q}) =: \mathfrak{q}$  est un idéal premier au-dessus de  $q \equiv \pm 1 \pmod{p^n}$ .

La composante du symbole d'Artin de  $N_{K/k}(\mathfrak{A})$  dans  $\text{Gal}(F/k) \simeq \mathcal{T}_k$  ne dépend pas des choix effectués.  $\square$

**Remarque 3.2.** Il est nécessaire de remarquer que dans les calculs, PARI ne donne pas directement  $\mathfrak{A} = \mathfrak{Q}$ , mais le plus souvent un idéal  $\mathfrak{A}$  de la forme  $\mathfrak{Q}^\omega$ ,  $\omega \in \mathbb{Z}[\text{Gal}(K/\mathbb{Q})]$  non nécessairement égal à 1, ce qui conduit à la relation :

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

où  $\mathfrak{q}$  est l'idéal premier de  $k$  au-dessous de  $\mathfrak{Q}$  et  $\omega(1) \in \mathbb{Z}$  l'image de  $\omega$  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 :

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

(idéal premier principal de  $k$  en-dessous de  $\mathfrak{L}$ ). L'aspect statistique devant vérifier que  $\mathfrak{l} = N_{K/k}(\mathfrak{L})$  et  $\mathfrak{q}^{\omega(1)} = N_{K/k}(\mathfrak{Q}^\omega)$  sont "indépendants" du point de vue classes d'idéaux et propriétés  $p$ -adiques (au sens des sections précédentes). Ces calculs font l'objet du § 3.3.

### 3.2. Remarques heuristiques fondamentales.

(i) On pourrait objecter que notre démarche pose un problème de logique en ce sens que l'on peut concevoir les deux "implications" suivantes :

(a) C'est l'ensemble des groupes de classes des  $k_n$  (donc les valeurs de  $\lambda$  et  $\mu$ ) qui "préexistent" et qui "imposent", pour chaque  $n$ , les algorithmes numériques qui les déterminent et en particulier le nombre de pas  $m_n = O(1) \cdot (\lambda \cdot n + \mu \cdot p^n)$ . Ceci compromet pour une part notre étude statistique dans la mesure où il est impossible (pour une donnée numérique de  $k = \mathbb{Q}(\sqrt{m})$ ) de s'affranchir du fait que la structure arithmétique de  $K/k$  influe directement sur les étapes de l'algorithme.

(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  $\delta_p(x)$  issus de la relation  $\left(\frac{x^{p-1}-1}{p}\right) =: \prod_{\mathfrak{p}|p} \mathfrak{p}^{\delta_p(x)} \cdot \mathfrak{b}(x)$ ,  $\mathfrak{b}(x)$  étranger à  $p$ .

(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 la même nature que le point de vue (b) ci-dessus sur la conjecture de Greenberg :

En effet, pour la conjecture de Leopoldt, la complexité repose sur les calculs, modulo  $p^n$ , des déterminants des développements  $p$ -adiques des logarithmes d'une unité de Minkowski du corps  $k$  et de ses conjuguées. Ici, les algorithmes sont liés par la condition (triviale) de réduction modulo  $p^n$  du calcul modulo  $p^m$  ( $m \geq n$ ).

(iii) Par ailleurs, l'influence du corps de base  $k$  (quant à sa complexité arithmétique) 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 son unité fondamentale est  $\varepsilon = a \cdot p^n \pm \sqrt{m}$  dont le logarithme  $p$ -adique tend vers 0 si  $n \rightarrow \infty$ . Et cependant la conjecture de Leopoldt est ici trivialement vraie puisque  $\log(\varepsilon) = 0$  équivaut à  $\varepsilon$  racine de l'unité dans  $k$ .

(b) Le cas de la conjecture de Greenberg est plus délicat, mais les aspects numériques dépendent fortement du groupe de torsion  $\mathcal{T}_k$  (qui conjugue  $p$ -groupe des classes  $\mathcal{C}_k$  et régulateur  $p$ -adique normalisé  $R_k := U_k^*/\overline{E}_k$ ) ; en particulier, on sait [3, 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  $k$  dans  $k_\infty$ .

(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  $m \geq n$ ,  $N_{k_m/k_n}(\mathcal{C}_{k_m}) = \mathcal{C}_{k_n}$ , etc.). Ce lien est exprimé par la relation (7.1) de [3, §7.1] et le schéma qui précède sur les flèches  $N_{k_{n+1}/k_n} : M_i^{n+1} \rightarrow M_i^n$ , permettant de dire que, modulo des normes dans les extensions correspondantes, on peut faire en sorte que pour tout  $h \geq 1$ , on ait les inclusions :

$$(3.1) \quad E_k \subseteq \Lambda_i^{n+h} \subseteq \dots \subseteq \Lambda_i^{n+1} \subseteq \Lambda_i^n.$$

Noter que  $h$  est nécessairement fini, non borné, car la suite ci-dessus dépend de  $n$  et  $h$ . Il y a donc un lien entre la complexité des algorithmes pour chaque  $n$  et les valeurs de  $\lambda$  et  $\mu$  ; 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. Programmes PARI résolvant l'équation**  $(y) = \mathfrak{L} \cdot \mathfrak{A}^{1-\sigma}$ . 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  $N_{K/k}(\mathfrak{A}) = N_{K/k}(\mathfrak{Q}^\omega) = \mathfrak{q}^{\omega(1)}$  à partir de la relation précédente du §3.1 :

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

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  $\eta_\ell$  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  $\mathcal{C}_{k_1}$  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  $\mathcal{C}_k$  et si suffisamment de  $x$  finissent par donner  $\delta_3(x) = 0$  ; les statistiques examineront ces deux aspects qui correspondent aux deux facteurs de l'expression (1.2).

Le programme général, qui détermine la solution  $y \in k_1^\times$  et la factorisation correspondante 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  $\eta_\ell$  est norme globale dans l'extension  $k_1/k$  ; on supposera  $\ell$  totalement décomposé dans  $k_n/k$ ,  $n \geq 1$  (ici  $n = 8$ ), donc, a fortiori, de la forme  $N_{k_1/k}(\mathfrak{L})$  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  $\eta_\ell$  précédents pour calculer (au moyen de la fonction *rnfnorminit* 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.

**Remarque 3.3.** A ce sujet, 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  $k_{1,w}$  au-dessus de  $v$  à l'équation normique  $\eta_v = N_{k_{1,w}/k_v}(y_w)$ , soient connues pour toute place  $v$  de  $k$  et  $w \mid v$  de  $K$ , il n'est pas possible d'en déduire une solution globale  $y$ .

Il faut signaler le cas "trivial"  $\eta = 1$  et l'équation  $N_{k_1/k}(y) = 1$  qui conduit, par le Théorème 90 de Hilbert pour le degré 3, à  $y = z^{1-\sigma}$ ,  $z \in k_1^\times$ , où une solution  $z_0$  est donnée par la résolvante de Hilbert

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

mais l'aspect additif suggère justement une part totalement aléatoire.

3.3.1. *Programme I – Recherche des idéaux  $\mathfrak{l} = (\eta_\ell)$  de  $k$ .* On rappelle que  $k = \mathbb{Q}(\sqrt{m})$ , pour  $m \equiv 1 \pmod{3}$ . Le programme, semblable à celui du § 2.1, redonne les caractéristiques du corps  $k$  (nombre de classes,  $\delta_p(\eta_3)$  pour la  $S_k$ -unité fondamentale, l'unité fondamentale  $\varepsilon$  étant supposée en général telle que  $\delta_3(\varepsilon) \geq 1$ ) et calcule une liste de nombres premiers  $\ell$  totalement décomposés dans  $k_n/\mathbb{Q}$  tels que les idéaux premiers  $\mathfrak{l} \mid \ell$  soient principaux de la forme  $(\eta_\ell)$  où  $\delta_3(\eta_\ell) \geq 1$  afin que  $\eta_\ell$  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  $\eta_\ell$  est calculé sous la forme  $\text{Mod}(a * x + b, x^2 - m)$ , mais les  $\delta_p(\eta_3)$  et  $\delta_3(\varepsilon)$  nécessitent des calculs modulo une grande puissance de 3 :

```
{p=3;m=67;n=8;n0=n+1;
y=x;Q=x^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*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);
Pk=y^2-Mod(m,p^n0);Y=Mod(y,Pk);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,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(zpi+ze<1,print("PROBLEME-NORMIQUE"));
if(delta!=0,print("PROBLEME-CLASSES"));
print("m=",m," h=",h," E=",E);
print("p=",p," S=",pi1," ",pi2);print(zpi," ",ze);x=y;
```

```
B=5*10^4;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)}
```

Il fournit les résultats sous la forme suivante indiquant (pour  $m = 67$ ) que  $\delta_p(\eta_3) = 1$  et  $\delta_3(\varepsilon) = 2$  (on a limité la borne à  $B = 10^4$ ) :

PROBLEME-NORMIQUE

m=67,h=1,E=5967\*x+48842

p=3,S={x+8,x-8}

1/3 1/9

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

La liste obtenue contient dans l'ordre,  $m$ , le nombre de  $\ell$  trouvés, et enfin la liste des  $\eta_\ell$  qui sera exploitée par le second programme.

3.3.2. *Programme II – Recherche des idéaux  $\mathfrak{A}$  tels que  $(y) = \mathfrak{L} \cdot \mathfrak{A}^{1-\sigma}$ .*

Pour des raisons de priorités des variables PARI, on doit changer  $x$  en  $y$  dans la liste précédente et la reproduire dans la liste nommée *list* ; ensuite 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  $\zeta_9$  est une racine primitive 9-ième de l'unité ( $R = x^6 - 6m x^4 + 9m^2 x^2 - m^3$ ).

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

m=component(list,1);p=3;
Nlist=component(list,2);listL=component(list,3);
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);
Eta=X^2/m-2;racm=m^2/(3*m*X-X^3);z=X^2/m-2;
for(j=1,Nlist,Z=component(list,j+3);
N=rnfisnorm(T,Z);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);L=component(listL,j);
print(L);print(F))}
```

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

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.

3.3.3. *Programme III – Idéaux  $\mathfrak{A}$  tels que  $(y) = \mathfrak{A}^{1-\sigma}$  &  $N_{k_1/k}(y) = \varepsilon$ .*  
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 résout l'équation  $N_{k_1/k}(y) = \varepsilon$  qui a toujours une solution dans la mesure où l'on suppose  $\delta_3(\varepsilon) \geq 1$ ; on donne aussi la structure de  $\mathcal{C}_{k_1}$  :

```
{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); epsilon=Mod(e1+e2*y,y^2-m);
bnf=bnfinit(y^2-m);PK=polsubcyclo(9,3)+Mod(0,bnf.pol);
T=rnfnorminit(bnf,PK,1);R=x^6-6*m*x^4+9*m^2*x^2-m^3;
K=nfinit(R);X=Mod(x,R);
Eta=X^2/m-2;racm=m^2/(3*m*X-X^3);z=X^2/m-2;
N=rnfnorm(T,epsilon);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  $m = 67$  ( $h = 1$ ,  $\delta_p(\eta_3) = 1$ ,  $\delta_3(\varepsilon) = 2$ ,  $\mathcal{C}_{k_1} = [3]$ ),  $y$  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  $181 = N_{k/\mathbb{Q}}(3\sqrt{67} + 28)$  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  $N_{k_1/k}(M_1^1) = 1$  et  $\Lambda_1^1 = \langle \varepsilon, \eta_3, 3\sqrt{67} + 28 \rangle$  qui stoppe l'algorithme.

(ii) Pour  $m = 6559$  ( $h = 18$ ,  $\delta_p(\eta_3) = 1$ ,  $\delta_3(\varepsilon) = 3$ ,  $\mathcal{C}_{k_1} = [54, 3]$ ),  $y$  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  $\omega$ .

(iii) Pour  $m = 3259$  ( $h = 1, \delta_p(\eta_3) = 0, \delta_3(\varepsilon) = 4, \mathcal{C}_{k_1} = [3, [3]]$ ), on trouve  $\mathfrak{A} = (1)$  qui montre que  $\varepsilon$  est norme de l'unité de  $k_1$  :

Mod(Mod(-495452848877794109154272\*y-28284239771961302173706384,  
y^2-3259)\*x^2  
 +Mod(931133218427718936425952\*y+53156209050568241456130896,  
y^2-3259)\*x  
 +Mod(-263604189149463218625499\*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  $\delta_p(\eta_3) = 0$ , l'algorithme stope, ce qui est cohérent avec  $\#\mathcal{C}_{k_1} = 3$ .

(iv) Pour  $m = 1867$  ( $h = 1, \delta_p(\eta_3) = 1, \delta_3(\varepsilon) = 5, \mathcal{C}_{k_1} = [3, [3]]$ ), 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  $N_{k/\mathbb{Q}}(34086\sqrt{m} + 1472815) = -107$  et  $\delta_3(34086\sqrt{m} + 1472815) = 0$ .

Certains de ces exemples donnent au premier stade  $\Lambda_1^1$  des  $\delta_3(x)$  qui stopent l'algorithme ( $m = 67, 3259, 1867$  pour lesquels  $\mathcal{C}_{k_1} \simeq \mathbb{Z}/3\mathbb{Z}$ ). Pour  $m = 6559$ , qui reste à examiner, on a  $\mathcal{C}_{k_1} \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .

#### 4. EVOLUTION DE L'EXPRESSION (1.2) 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  $\frac{1}{27}$ , ce qui donne un groupe  $\mathcal{T}_k$  d'ordre  $3^5$ , donc une grande variété de décompositions.

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

PROBLEME-NORMIQUE  
 m=6559, h=18, E=81\*x+6560  
 p=3, S={379\*x-30694, 379\*x+30694}  
 1/3 1/27

qui indiquent que  $\delta_{\mathfrak{p}}(\eta_3) = 1$  et  $\delta_3(\varepsilon) = 3$ . On notera que  $\mathcal{A}_k$  est engendré par  $\mathfrak{p} \mid 3$ .

On obtient la liste suivante des  $\eta_\ell$  dans la variable *list*, après avoir substitué la variable *y* :

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

**4.2. Décomposition de  $(y)$  en idéaux, pour  $k = \mathbb{Q}(\sqrt{6559})$ .** Le second programme donne la solution  $y \in k_1^\times$  telle que  $N_{k_1/k}(y) = \eta_\ell$  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  $x^3 - 3x + 1$  pour l'extension relative  $k_1/k$ ).

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

```
Y=Mod(Mod(103603429803986698500793761812835866687
8738304822327197272934756399840529/418195493*y
-8390598661945059443075872989882636906451249
9733687980568899041217527878770/418195493,y^2-6559)*x^2
+Mod(-194710756949834302518150983617741998570
9413036014952120204634371585899310/418195493*y
+15769167293211778079551042284522907830683899
9479469060631851001865336037874/418195493,y^2-6559)*x
+Mod(551262335748355458007199134755867939
764504856477125221099310399055725544/418195493*y
-4464544296904031158210117579530451263319333
4530869826508158991263404771360/418195493,y^2-6559),
x^3-3*x+Mod(1,y^2-6559))
```

On aura en général :

$$(y) = \mathfrak{L} \cdot \Omega^{\omega \cdot (1-\sigma)}, \quad \omega \in \mathbb{Z}[\text{Gal}(k_1/\mathbb{Q})],$$

où  $\text{Gal}(k_1/\mathbb{Q})$  est engendré par  $\sigma$  d'ordre 3 et  $\tau$  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  $\Omega$ , dont les coefficients sont dans l'intervalle  $[-9, +9]$  et où l'idéal  $\mathfrak{A} = \Omega^\Omega$  est tel que  $\Omega \mid 53$  où  $N_{k_1/k}(\Omega) = \mathfrak{q}$  dont la classe est d'ordre 9.

Le tableau complet des décompositions est le suivant (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  $\eta_\ell$  sont données au § 4.1) :

92179

$[[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 1;$   
 $[53, [9, 0, 0, 0, 1, 0]^\sim, 1, 1, [-25, 11, 16, -3, -22, 10]^\sim], -1;$   
 $[92179, [16160, 0, 0, 0, 1, 0]^\sim, 1, 1,$   
 $[-34250, -40280, 3133, -29163, -3589, -27112]^\sim], 1]$

86239

$[[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 3;$   
 $[53, [-2, 0, 0, 0, 1, 0]^\sim, 1, 1, [-22, 15, 20, -9, 23, 10]^\sim], 2;$   
 $[53, [2, 0, 0, 0, 1, 0]^\sim, 1, 1, [22, -15, -20, -9, 23, 10]^\sim], -1;$   
 $[53, [7, 0, 0, 0, 1, 0]^\sim, 1, 1, [21, -12, -17, -11, -24, 10]^\sim], 1;$   
 $[53, [9, 0, 0, 0, 1, 0]^\sim, 1, 1, [-25, 11, 16, -3, -22, 10]^\sim], -5;$   
 $[86239, [-15841, 0, 0, 0, 1, 0]^\sim, 1, 1,$   
 $[42046, 29382, 41192, 20964, 27633, -12780]^\sim], 1]$

70327

$[[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 2;$   
 $[53, [9, 0, 0, 0, 1, 0]^\sim, 1, 1, [-25, 11, 16, -3, -22, 10]^\sim], -2;$   
 $[70327, [22052, 0, 0, 0, 1, 0]^\sim, 1, 1,$   
 $[32411, 11187, 23443, 18808, -289, -19643]^\sim], 1]$

68743

$[[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 2;$   
 $[53, [-2, 0, 0, 0, 1, 0]^\sim, 1, 1, [-22, 15, 20, -9, 23, 10]^\sim], 4;$   
 $[53, [2, 0, 0, 0, 1, 0]^\sim, 1, 1, [22, -15, -20, -9, 23, 10]^\sim], -2;$   
 $[53, [7, 0, 0, 0, 1, 0]^\sim, 1, 1, [21, -12, -17, -11, -24, 10]^\sim], 2;$   
 $[53, [9, 0, 0, 0, 1, 0]^\sim, 1, 1, [-25, 11, 16, -3, -22, 10]^\sim], -6;$   
 $[68743, [23513, 0, 0, 0, 1, 0]^\sim, 1, 1,$   
 $[24129, 16740, 26535, 3717, 11912, -12637]^\sim], 1]$

58321

$[[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 5;$   
 $[53, [-2, 0, 0, 0, 1, 0]^\sim, 1, 1, [-22, 15, 20, -9, 23, 10]^\sim], 3;$   
 $[53, [2, 0, 0, 0, 1, 0]^\sim, 1, 1, [22, -15, -20, -9, 23, 10]^\sim], -2;$   
 $[53, [7, 0, 0, 0, 1, 0]^\sim, 1, 1, [21, -12, -17, -11, -24, 10]^\sim], 2;$   
 $[53, [9, 0, 0, 0, 1, 0]^\sim, 1, 1, [-25, 11, 16, -3, -22, 10]^\sim], -8;$   
 $[58321, [12524, 0, 0, 0, 1, 0]^\sim, 1, 1,$   
 $[13509, 16128, 23244, -16488, -7523, -20417]^\sim], 1]$

48907

$[[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 1;$   
 $[53, [9, 0, 0, 0, 1, 0]^\sim, 1, 1, [-25, 11, 16, -3, -22, 10]^\sim], -1;$   
 $[48907, [-7471, 0, 0, 0, 1, 0]^\sim, 1, 1,$   
 $[12062, 22844, 17998, -17401, -4054, -17679]^\sim], 1]$

47143

$[[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 3;$   
 $[53, [-2, 0, 0, 0, 1, 0]^\sim, 1, 1, [-22, 15, 20, -9, 23, 10]^\sim], 4;$   
 $[53, [2, 0, 0, 0, 1, 0]^\sim, 1, 1, [22, -15, -20, -9, 23, 10]^\sim], -2;$

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

[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  $\Omega^\omega$  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  $\omega$  nécessite d'identifier numériquement les conjugués de  $\Omega$ .

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

$\tau$  défini par  $x \mapsto -x$ ,  
 $\sigma$  défini par  $x \mapsto -1/43020481x^5 + 5/6559x^3 - 6x$ ,  
 $\tau \cdot \sigma^2$  défini par  $x \mapsto -1/43020481 * x^5 + 5/6559 * x^3 - 5 * x$ ,  
 $\sigma^2$  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  $\Omega$  ; 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  $\Omega_1$  :

$$\Omega_1, \quad \Omega_1^\sigma = \Omega_2, \quad \Omega_1^{\sigma^2} = \Omega_3.$$

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  $N_{k_1/k}(\mathfrak{A}) = (53)^2 \cdot \mathfrak{q}^8$  ; 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

$$\begin{aligned} & [[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 2; & \text{Q1} \\ & [53, [9, 0, 0, 0, 1, 0]^\sim, 1, 1, [-25, 11, 16, -3, -22, 10]^\sim], -2; & \text{Q3} \\ & [82457, [-11462, 0, 0, 0, 1, 0]^\sim, 1, 1, \\ & \quad [-12743, -34335, -22650, 2405, 35275, -22073]^\sim], 1] \end{aligned}$$

qui conduit à  $\omega(1) = 4$ .

Pour  $\ell = 2267$ , il vient :

2267

$$\begin{aligned} & [[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 3; & \text{Q1} \\ & [53, [-2, 0, 0, 0, 1, 0]^\sim, 1, 1, [-22, 15, 20, -9, 23, 10]^\sim], 1; & \text{Q2} \\ & [53, [2, 0, 0, 0, 1, 0]^\sim, 1, 1, [22, -15, -20, -9, 23, 10]^\sim], -1; & \text{tau(Q2)} \\ & [53, [7, 0, 0, 0, 1, 0]^\sim, 1, 1, [21, -12, -17, -11, -24, 10]^\sim], 1; & \text{tau(Q1)} \\ & [53, [9, 0, 0, 0, 1, 0]^\sim, 1, 1, [-25, 11, 16, -3, -22, 10]^\sim], -4; & \text{Q3} \\ & [2267, [855, 0, 0, 0, 1, 0]^\sim, 1, 1, \\ & \quad [433, 150, -991, -60, -759, -378]^\sim], 1] \end{aligned}$$

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

Pour  $\ell = 8011$  on obtient :

8011

$$\begin{aligned} & [[53, [-7, 0, 0, 0, 1, 0]^\sim, 1, 1, [-21, 12, 17, -11, -24, 10]^\sim], 4; & \text{Q1} \\ & [53, [-2, 0, 0, 0, 1, 0]^\sim, 1, 1, [-22, 15, 20, -9, 23, 10]^\sim], 3; & \text{Q2} \\ & [53, [2, 0, 0, 0, 1, 0]^\sim, 1, 1, [22, -15, -20, -9, 23, 10]^\sim], -2; & \text{tau(Q2)} \\ & [53, [7, 0, 0, 0, 1, 0]^\sim, 1, 1, [21, -12, -17, -11, -24, 10]^\sim], 2; & \text{tau(Q1)} \\ & [53, [9, 0, 0, 0, 1, 0]^\sim, 1, 1, [-25, 11, 16, -3, -22, 10]^\sim], -7; & \text{Q3} \\ & [8011, [-2063, 0, 0, 0, 1, 0]^\sim, 1, 1, \\ & \quad [-2011, -1995, 2900, 979, -3590, 1411]^\sim], 1] \end{aligned}$$

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

Par conséquent, tous les cas intéressants de  $\omega$  sont obtenus, ce qui suggère la répartition uniforme de la composante  $\mathcal{d}_k(\mathfrak{t})$  dans  $\mathcal{C}_k$  relativement à la décomposition (1.1) de  $N_{k_1/k}(\mathfrak{A})$ .

**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  $\mathcal{C}_{k'} \simeq (\mathbb{Z}/3\mathbb{Z})^2$ , 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  $\delta_3(\eta) \geq 1$ .

Considérons le groupe des classes ambiges  $M_1^1$  d'ordre 27 ; il est engendré par les classes de  $\mathfrak{P} \mid 3$  dans  $k_1$  et de  $\mathfrak{A} = \Omega_{53}^{-2} \cdot \Omega_{163}^{-2+(\tau-2)\cdot\sigma}$

provenant de la résolution de  $\varepsilon = N_{k_1/k}(y)$ , 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  $N_{k_1/k}(M_1^1)$  est engendré par les classes dans  $k$  de  $\mathfrak{p} \mid 3$  (car  $\mathcal{C}_k(\mathfrak{p})$  engendre  $\mathcal{C}_k$ ), de  $\mathfrak{q}_{53}$  et  $\mathfrak{q}_{163}$  (rajoutés par commodité). Or le nombre  $y$  :

```
Mod(Mod(-7187728670731559626633099507393046182548814589652
4276161077748022808885957117737704968186794105796351441782
3870036306401501411978843103297850259108500908657888072475
21563255794/319368996194651583505768629775038129626414323*y
+582117278174738949308664878774940722458488263482616181371
3810788842641520135060603172865428715330526941522187468733
7354623963250382749973772345510686704561106009257383076489
48394/319368996194651583505768629775038129626414323, y^2-6559)*x^2
+Mod(13508511184195505613742219965538561962111105014131136
3211546949986093001291512487360593830764009509822712411875
2225254333582328007742711074388814166978010414912867115203
83281636/319368996194651583505768629775038129626414323*y
-1094022621465560221024383982302623947070116590967555241901
2938624119420003673951026719359782502619553540510072960396
5675573740447729608300893580310787482452577032333038289870
73255/319368996194651583505768629775038129626414323, y^2-6559)*x
+Mod(-38245105429901800364008747156252386839535939979536661
9009943516000134801610568075905687094444764334651078501776
11862777507305882311215620172726177523076562003272459195361
669091/319368996194651583505768629775038129626414323*y
+309738134203867300907648136875882808215662740937604712473
9543695130753260830713933798219178680883193573137076910814
3702260180553511394963663651519378888792490729241654950722
85579/319368996194651583505768629775038129626414323, y^2-6559),
x^3-3*x+Mod(1, y^2-6559))
```

a pour norme relative le nombre  $x$  :

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

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

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

et qui fournit un élément de  $\Lambda_1^1$  norme dans  $k_1/k$  (le symbole de Hasse de  $x$  peut se calculer, mais comme  $x$  n'est pas étranger à 3, son calcul est plus complexe ;  $y$  pourrait permettre le pas suivant de l'algorithme).

Par conséquent,  $\#(M_2^1/M_1^1) = 3$  car le facteur classes a été trivialisé puisque  $N_{k_1/k}(M_1^1) = \mathcal{C}_k$ . D'où  $\#M_2^1 = 81$ , et comme PARI donne  $\mathcal{C}_{k_1} \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ , on a fin de l'algorithme (normalement on devrait déterminer  $M_3^1/M_2^1$  à partir du calcul de  $\Lambda_2^1$  pour constater la fin).

**Remarques 4.1.** (i) On vérifie avec PARI 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 (cf. [3, 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  $N_{k_m/k_n} : \mathcal{C}_{k_m} \rightarrow \mathcal{C}_{k_n}$  sont surjectives,  $\#\mathcal{C}_{k_n}$  est fonction croissante de  $n$ , mais avec la contrainte  $M_1^n = \#\mathcal{C}_{k_n}^{G_n} = 3^5$  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  $N_{k_n/k}(S_{k_n}) = S_k$  qui engendre  $\mathcal{C}_k$ , le facteur classes est toujours trivialisé et tout dépend de la  $i$ -suite décroissante  $3^{\rho_i^n} \mid (U_k^*/\overline{E}_k) = 3^3$ .

**Remarque 4.2.** 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.

## 5. CONCLUSION

Le schéma du § 1.1 indique que  $\mathcal{T}_k$  joue le rôle d'espace de probabilité dans ce cadre ; en effet, la partie  $\mathcal{C}_k$  contrôle le premier facteur de (1.2) ("facteur classes"), et la partie régulateur  $U_k^*/\overline{E}_k$  contrôle le second ("facteur normique").

Le facteur  $\#M_1^n$  n'est pas probabiliste 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  $U_k^*/\overline{E}_k$  (cf. [3, Théorème 4.7]).

Les expérimentations algorithmiques suggèrent que, pour tout  $n$  fixé assez grand, 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 [3, Hypothèse 7.1] et les heuristiques [3, Heuristiques 7.5, 7.6] dont nous rappelons l’essentiel :

- (i) Soit  $c \in \mathcal{C}_k$  ; la probabilité que, pour un idéal  $\mathfrak{A}$  de  $k_n$  étranger à  $p$ , la  $p$ -classe de  $N_{k_n/k}(\mathfrak{A})$  soit égale à  $c$ , est  $\frac{1}{\#\mathcal{C}_k}$ .
- (ii) La probabilité que, pour un  $x \in \Lambda_i^n$ , on ait  $\delta_p(x) \geq r$  (cf. (1.4)), 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  $N_{k_n/k}(M_{i_0}^n) = \mathcal{C}_k$  et  $\frac{1}{p^{n \cdot (d-1)} (\Lambda_{i_0}^n : \Lambda_{i_0}^n \cap N_{k_n/k}(k_n^\times))} = 1$ , pour  $n \rightarrow \infty$ .

Ce que l’on peut résumer de la façon approximative suivante :

Pour  $\lambda$  ou  $\mu$  non nuls, la probabilité de  $\#\mathcal{C}_{k_n} = p^{\lambda \cdot n + \mu \cdot p^n + \nu}$  est au plus en  $\frac{1}{p^{O(1) \cdot (\lambda \cdot n + \mu \cdot p^n)}}$ , lorsque  $n \rightarrow \infty$ .

**Remarque 5.1.** L’existence de  $i_0$  assez grand, *indépendant de  $n \rightarrow \infty$* , stopant les algorithmes, peut paraître arbitraire car les liens numériques entre les étages  $n$  et  $m \geq n$  semblent difficilement analysables (à l’exception de la relation fondamentale (3.1) du § 3.2). Cependant, cette existence est 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  $\tilde{\mathcal{C}}_k$  capitule dans  $k_\infty$ .*

Or si  $\tilde{\mathcal{C}}_k$  capitule dans  $k_n$ , il capitule dans  $k_m$ . 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.

Le comportement des  $\mathcal{C}_{k_n}$  dans la tour ne dépend donc pas uniquement de *circonstances algébriques à la Iwasawa*, c’est-à-dire d’un théorème de structure de certaines limites projectives, 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  $\#\mathcal{C}_{k_n}$ , lorsque  $n \rightarrow \infty$ , 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.
- [3] G. GRAS – Approche  $p$ -adique de la conjecture de Greenberg pour les corps totalement réels, *Annales Mathématiques Blaise Pascal* 2017 (à paraître).
- [4] 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>
- [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](http://www.jstor.org/stable/2373625?seq=1#page_scan_tab_contents)
- [7] J-F. JAULENT – Théorie  $\ell$ -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](http://www.numdam.org/article/JTNB_1998_10_2_355_0.pdf)
- [8] J-F. JAULENT – Note sur la conjecture de Greenberg (preprint 2016). <https://arxiv.org/abs/1612.00718>
- [9] T. NGUYEN QUANG DO – Formules de genres et conjecture de Greenberg (preprint 2017). <https://www.researchgate.net/publication/311846783>
- [10] THE PARI GROUP – PARI/GP version 2.9.0, *Université de Bordeaux* (2016). <http://pari.math.u-bordeaux.fr/>.
- [11] 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.

VILLA LA GARDETTE, CHEMIN CHÂTEAU GAGNIÈRE, 38520 LE BOURG D’OISANS.,  
[http://www.researchgate.net/profile/Georges\\_Gras](http://www.researchgate.net/profile/Georges_Gras)  
*E-mail address:* g.mn.gras@wanadoo.fr