Approche p-adique de la conjecture de Greenberg pour les corps totalement réels

Georges Gras

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

par

Georges Gras

Résumé. — Soit k un corps de nombres totalement réel et soit k_∞ sa $\mathbb{Z}_p$-extension cyclotomique pour un premier $p > 2$. Nous donnons (Théorème 3.2) une condition suffisante de nullité des invariants d'Iwasawa λ, μ, lorsque p est totalement décomposé dans k, et nous obtenons d'importantes tables de corps quadratiques et p pour lesquels on peut conclure que $\lambda = \mu = 0$. Nous montrons que le nombre de p-classes ambiges de k_n (n-ième étage dans k_∞) est égal à l'ordre du groupe de torsion $\mathcal{T}_k$ du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale de k (Théorème 4.2), pour tout $n \geq e$, où p^e est l'exposant de $U_k^*/\overline{E}_k$ (en termes d'unités locales et globales). Puis nous établissons des analogues de la formule de Chevalley en utilisant une famille $(\Lambda_i^n)_{0\leq i\leq m_n}$ de sous-groupes de $k^\times$ contenant E_k, dans lesquels tout x est norme d'un idéal de k_n. Cette famille est attachée à la filtration classique du p-groupe des classes de k_n définissant l'algorithme de calcul de son ordre en m_n pas. A partir de cela, nous montrons (Theorem 6.1) que $m_n \geq (\lambda \cdot n + \mu \cdot p^n + \nu)/v_p(\#\mathcal{T}_k)$ et que la condition $m_n = O(1)$ (i.e., $\lambda = \mu = 0$) dépend essentiellement des valuations $\mathfrak{p}$-adiques des $\frac{x^{p-1}-1}{p}$, $x \in \Lambda_i^n$, pour $\mathfrak{p} \mid p$, de sorte que la conjecture de Greenberg est fortement dépendante de "quotients de Fermat" dans $k^\times$. Des heuristiques et statistiques sur ces quotients de Fermat (Sections 6, 7, 8) montrent qu'ils suivent des lois de probabilités naturelles, liées à $\mathcal{T}_k$ quel que soit n, suggérant que $\lambda = \mu = 0$ (Heuristiques 7.1, 7.2, 7.3).
Ceci impliquerait que, pour une preuve de la conjecture de Greenberg, certains résultats p-adiques profonds (probablement inaccessibles actuellement), ayant une certaine analogie avec la conjecture de Leopoldt, sont nécessaires avant toute référence à la seule théorie d'Iwasawa algébrique.

***Classification mathématique par sujets* (2000).** — 11R23, 11R29, 11R37; 11Y40.
Mots clefs. — Greenberg's conjecture, Iwasawa's theory, p-class groups, class field theory, Fermat quotients, p-adic regulators, Leopoldt's conjecture.

Abstract. — Let k be a totally real number field ant let k_∞ be its cyclotomic $\mathbb{Z}_p$-extension for a prime $p > 2$. We give (Theorem 3.2) a sufficient condition of nullity of the Iwasawa invariants λ, μ, when p totally splits in k, and we obtain important tables of quadratic fields and p for which we can conclude that $\lambda = \mu = 0$. We show that the number of ambiguous p-classes of k_n (nth stage in k_∞) is equal to the order of the torsion group $\mathcal{T}_k$, of the Galois group of the maximal Abelian p-ramified pro-p-extension of k (Theorem 4.2), for all $n \geq e$, where p^e is the exponent of $U_k^*/\overline{E}_k$ (in terms of local and global units). Then we establish analogs of Chevalley's formula using a family $(\Lambda_i^n)_{0 \leq i \leq m_n}$ of subgroups of $k^\times$ containing E_k, in which any x is norm of an ideal of k_n. This family is attached to the classical filtration of the p-class group of k_n defining the algorithm of computation of its order in m_n steps. From this, we prove (Theorem 6.1) that $m_n \geq (\lambda \cdot n + \mu \cdot p^n + \nu)/v_p(\#\mathcal{T}_k)$ and that the condition $m_n = O(1)$ (i.e., $\lambda = \mu = 0$) essentially depends on the $\mathfrak{p}$-adic valuations of the $\frac{x^{p-1}-1}{p}$, $x \in \Lambda_i^n$, for $\mathfrak{p} \mid p$, so that Greenberg's conjecture is strongly related to "Fermat quotients" in $k^\times$. Heuristics and statistical analysis of these Fermat quotients (Sections 6, 7, 8) show that they follow natural probabilities, linked to $\mathcal{T}_k$ whatever n, suggesting that $\lambda = \mu = 0$ (Heuristics 7.1, 7.2, 7.3).
This would imply that, for a proof of Greenberg's conjecture, some deep p-adic results (probably out of reach now), having some analogy with Leopoldt's conjecture, are necessary before referring to the sole algebraic Iwasawa theory.

1. Introduction

Nous appelons *Conjecture de Greenberg pour les corps de nombres totalement réels* k, le fait que les invariants d'Iwasawa $\lambda_p(k)$ et $\mu_p(k)$, associés à la limite projective des p-groupes de classes d'idéaux dans la p-tour cyclotomique k_∞, sont nuls (quel que soit le nombre premier p). Comme la nullité de $\lambda_p(k)$ et $\mu_p(k)$ implique celle relative aux sous-corps de k, nous supposerons $k/\mathbb{Q}$ Galoisienne réelle.

Le corps k et le nombre premier p étant fixés, on désigne par λ, μ, ν les invariants d'Iwasawa pour k et p.

Dans l'approche classique, la décomposition de p dans $k/\mathbb{Q}$ joue un rôle important. En effet, soient $d := [k : \mathbb{Q}]$ et $t \mid d$ le nombre d'idéaux premiers au-dessus de p dans k ; par exemple, si dans un premier temps on ne s'intéresse qu'à la trivialité du p-groupe des classes $\mathcal{C}\ell_{k_n}$ du n-ième étage k_n de k_∞, celle-ci est, en supposant implicitement p *totalement ramifié dans* k_∞/k, équivalente à la trivialité de chacun des deux facteurs de la formule des classes ambiges de Chevalley qui s'écrit dans ce cas :

$$\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{C}\ell_k \cdot \frac{p^{n\cdot(t-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}, \tag{1.1}$$

où $G_n = \mathrm{Gal}(k_n/k)$, $\mathcal{C}\ell_k$ est le p-groupe des classes de k, et E_k son groupe des unités. Chaque facteur joue alors un rôle spécifique pour la conjecture ; en ce qui concerne le facteur normique, on a les faits suivants :

(i) Le cas $t = 1$ implique $E_k \subset \mathrm{N}_{k_n/k}(k_n^\times)$ (formule du produit des symboles de restes normiques) et les invariants λ et μ dépendent essentiellement du comportement du p-groupe des classes de k par extension des idéaux dans la tour [**21**, Theorem 1, § 4 (1976)].

(ii) Le cas $t = d$ montrera que, sous la conjecture de Leopoldt, le facteur $\dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ a, pour tout $n \gg 0$, même valuation p-adique que le régulateur p-adique normalisé R_k de k (Théorème 4.2).

(iii) Si $1 < t < d$, l'étude se ramène grosso modo aux cas précédents, ce que l'on peut illustrer au moyen du cas Abélien réel de degré d étranger à p, par découpage semi-simple (selon les caractères p-adiques de $\mathrm{Gal}(k/\mathbb{Q})$, comme dans **[18]**, **[23]**, **[27]**, **[28]**). Si k' est le corps de décomposition de p dans k, alors $\#\mathcal{C}\ell_k \cdot \dfrac{p^{n\cdot(t-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ s'écrit comme produit de

$$\#\mathcal{C}\ell_{k'} \cdot \frac{p^{n\cdot(t-1)}}{(E_{k'} : E_{k'} \cap \mathrm{N}_{k'_n/k'}(k_n'^\times))} \quad \text{par} \quad \#\mathcal{C}\ell_k^* \cdot \frac{1}{(E_k^* : E_k^* \cap \mathrm{N}_{k_n/k}(k_n^\times))} = \#\mathcal{C}\ell_k^*,$$

où l'on a posé $E_k = E_{k'} \bigoplus E_k^*$ (à un indice près étranger à p), où E_k^* est le sous-groupe des unités de norme 1 sur k'. Autrement dit, pour tout n on a $E_k^* \subset \mathrm{N}_{k_n/k}(k_n^\times)$ et on est ramené au cas totalement décomposé pour k'. Cependant, s'il existe un p-groupe de classes relatives $\mathcal{C}\ell_k^*$ dans k/k', la question est analogue, en relatif, au cas non décomposé $t = 1$.

2. Conjecture de Greenberg (p décomposé)

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

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

Théorème 2.1. — [**21**, Theorem 2, § 4 (1976)]. *Sous les hypothèses et notations précédentes, et sous la conjecture de Leopoldt pour p dans k, les invariants $\lambda_p(k)$ et $\mu_p(k)$ d'Iwasawa sont nuls si et seulement si pour tout $n \gg 0$, on a $\mathcal{C}\ell_K^G = c\ell_K(S_K)$ (i.e., le sous-groupe de $\mathcal{C}\ell_K$ formé des p-classes ambiges est égal au sous-groupe engendré par les p-classes des idéaux premiers de K au-dessus de p).*

Dans cet énoncé interviennent le p-groupe des classes ambiges $\mathcal{C}\ell_K^G$ et le groupe $c\ell_K(S_K)$ qui est un sous-groupe du p-groupe des classes du groupe des idéaux invariants I_K^G ; on a l'isomorphisme classique :

$$\mathcal{C}\ell_K^G/c\ell_K(I_K^G) \simeq E_k \cap \mathrm{N}_{K/k}(K^\times)/\mathrm{N}_{K/k}(E_K), \tag{2.1}$$

où E_k et E_K sont les groupes des unités de k et K. Or seul $E_k \cap \mathrm{N}_{K/k}(K^\times)$, donné par le corps de classes local, est accessible en pratique, $\mathrm{N}_{K/k}(E_K)$ étant un invariant arithmétique non trivial associé à l'extension K/k, en relation avec les problèmes de capitulation de classes d'idéaux, ce qui explique la difficulté du calcul de λ et μ en termes d'unités globales (éventuellement comparées aux unités cyclotomiques du cadre Abélien comme dans [**37**, (1995)] pour le cas

non décomposé). On a par ailleurs $\mathcal{cl}_K(I_K^G) = \mathcal{cl}_K(S_K) \cdot j_{K/k}(\mathcal{C}\ell_k)$, où $j_{K/k}$ est l'extension des classes de k à K, et la relation $\mathcal{C}\ell_K^G = \mathcal{cl}_K(S_K)$ implique de plus $j_{K/k}(\mathcal{C}\ell_k) \subseteq \mathcal{cl}_K(S_K)$.

Remarque 2.1. — *Si $\mathcal{C}\ell_{k_n}^{G_n} = 1\ \forall n \gg 0$, la conjecture de Greenberg est vraie sous la forme $\lambda = \mu = \nu = 0$ et réciproquement ; or $\mathcal{C}\ell_{k_n}^{G_n} = 1\ \forall n \gg 0$ équivaut à $\#\mathcal{C}\ell_k = 1\ \&\ (E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)}\ \forall n \gg 0$ (cf. (1.1)).*
La Proposition 4.1 montrera que $(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)}$ pour un $n \geq 1$ équivaut à $(E_k : E_k \cap \mathrm{N}_{k_1/k}(k_1^\times)) = p^{d-1}$, et ainsi $\mathcal{C}\ell_{k_n}^{G_n} = 1\ \forall n \gg 0$ équivaut à $\mathcal{C}\ell_{k_1}^{G_1} = 1$ qui est effectif en pratique. Or la condition normique sur les unités a lieu si et seulement si le régulateur p-adique normalisé R_k de k (au sens de [**20**, Section 5]*) est une unité p-adique (Théorème 4.2 (ii)). Il en résulte que la condition $\lambda = \mu = \nu = 0$ équivaut (sous la conjecture de Leopoldt pour p dans k) à la nullité du groupe de torsion $\mathcal{T}_k$ de $\mathrm{Gal}(H_k^{\mathrm{pr}}/k)$, où H_k^{pr} est la pro-p-extension Abélienne p-ramifiée maximale de k (en effet, dans ce cas, $\#\mathcal{T}_k = \#\mathcal{C}\ell_k \cdot R_k$), ce qui équivaut à la p-rationalité de k (notion définie dans* [**14**, § IV.3], [**13**], [**36**], [**39**]*).*

3. Condition suffisante de nullité de λ et μ

Nous avons démontré dans [**15**, (1973)], [**16**, (1994)], et repris récemment dans [**17**, Theorem 3.6 (2016)], le résultat suivant valable en toute généralité, ici énoncé dans le cas "$T = \emptyset$" qui correspond aux groupes de classes au sens classique (l'énoncé n'utilisant que la ramification des places finies et l'éventuelle complexification des places à l'infini on doit utiliser le sens restreint) ; on désigne par I_K et P_K le groupe des idéaux de K et son sous-groupe des idéaux principaux (au sens restreint) :

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

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

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

Corollaire 3.1. — *Si $\mathcal{H} = \mathcal{cl}_K(S_K)$, où S_K est un ensemble fini quelconque d'idéaux premiers de K, on obtient :*

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

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

Jaulent a obtenu dans [**30**, p. 177 (1986)] l'autre écriture :

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

Utiliser la relation $E_k^{S_k} \cap \mathrm{N}_{K/k}(K^\times) = E_k^{\mathrm{N}S_K} \cap \mathrm{N}_{K/k}(K^\times)$ et la suite exacte $1 \to E_k^{S_k}/E_k^{\mathrm{N}S_K} \longrightarrow \langle S_k\rangle_{\mathbb{Z}}/\langle \mathrm{N}_{K/k}S_K\rangle_{\mathbb{Z}} \longrightarrow \mathcal{A}_k(S_k)/\mathcal{A}_k(\mathrm{N}_{K/k}S_K) \to 1$ pour comparer les deux expressions.

Remarques 3.1. — *(i) La relation du Théorème 3.1 (et ses analogues) se met sous la forme du produit de deux entiers :*

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

où H_k est le corps de classes de Hilbert de k ; si $K \cap H_k = k$, alors le premier facteur est égal à $\dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{K/k}(\mathcal{H})}$ et le second à $\dfrac{[K : k]^{-1} \cdot \prod_{\mathfrak{q}} e_{\mathfrak{q}}}{(\Lambda : \Lambda \cap \mathrm{N}_{K/k}(K^\times))}$.

(ii) Pour $K = k_n \subset k_\infty$, $G = G_n = \mathrm{Gal}(k_n/k)$, on obtient les formules :

$$\#\big(\mathcal{C}\ell_K/\mathcal{H}\big)^G = \frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{K/k}(\mathcal{H})} \cdot \frac{p^{n\cdot(d-1)}}{(\Lambda : \Lambda \cap \mathrm{N}_{K/k}(K^\times))},$$

$$\#\mathcal{C}\ell_K^{S_K G} = \#\mathcal{C}\ell_k^{S_k} \cdot \frac{p^{n\cdot(d-1)}}{(E_k^{S_k} : E_k^{S_k} \cap \mathrm{N}_{K/k}(K^\times))}.$$

On peut énoncer, en désignant maintenant par $\mathcal{C}\ell$ les *p-groupes de classes*, la condition seulement suffisante suivante, en rapport avec les résultats évoqués dans la Remarque 2.1 :

Théorème 3.2. — *Soit k Galoisien réel et soit $p > 2$ totalement décomposé dans k ; on suppose que p vérifie la conjecture de Leopoldt dans k. Soit k_1, de degré p sur k, le premier étage de la $\mathbb{Z}_p$-extension cyclotomique de k.*
Alors une condition suffisante pour que $\lambda = \mu = 0$ est que les deux conditions suivantes soient réalisées, où S_k est l'ensemble des idéaux premiers de k au-dessus de p et $E_k^{S_k}$ le groupe des S_k-unités de k :

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

(ii) $(E_k^{S_k} : E_k^{S_k} \cap \mathrm{N}_{k_1/k}(k_1^\times)) = p^{d-1}$, où $d = [k : \mathbb{Q}]$.

Démonstration. — Soit $n \geq 1$ et considérons $K := k_n$, $G := G_n$. On a la suite exacte de G-modules $1 \longrightarrow \mathcal{A}_K(S_K) \longrightarrow \mathcal{C}\ell_K \longrightarrow \mathcal{C}\ell_K^{S_K} \longrightarrow 1$, qui conduit à :

$$1 \longrightarrow \mathcal{A}_K(S_K)^G \longrightarrow \mathcal{C}\ell_K^G \longrightarrow \mathcal{C}\ell_K^{S_K G} \longrightarrow \mathrm{H}^1(G, \mathcal{A}_K(S_K)).$$

Comme p est totalement ramifié dans k_∞/k, $\mathcal{A}_K(S_K)^G = \mathcal{A}_K(S_K)$ et finalement on obtient :

$$1 \to \mathcal{C}\ell_K^G/\mathcal{A}_K(S_K) \to \mathcal{C}\ell_K^{S_K G} = (\mathcal{C}\ell_K/\mathcal{A}_K(S_K))^G \to \mathrm{H}^1(G, \mathcal{A}_K(S_K)),$$

qui fait que la condition $\mathcal{C}\ell_K^{S_K G} = 1$ pour tout $n \gg 0$ implique la conjecture de Greenberg (Théorème 2.1) ; cette condition est équivalente (cf. Remarque 3.1 (ii)) à la réunion de la condition (i) et de la condition $(E_k^{S_k} : E_k^{S_k} \cap \mathrm{N}_{K/k}(K^\times)) = p^{n\cdot(d-1)}$. D'après la Proposition 4.1, il suffira qu'elle soit satisfaite pour $K = k_1$ pour qu'elle le soit pour tout $n \geq 1$. □

Remarques 3.2. — *(i) On a $\mathrm{H}^1(G, \mathcal{A}_K(S_K)) = {}_\nu\mathcal{A}_K(S_K)$ où $\nu := \nu_n$ est la norme algébrique pour G ; par conséquent, si $\mathrm{N}_{K/k}$ est la norme arithmétique (ici surjective) et $j_{K/k}$ l'extension des classes, on a $\nu = j_{K/k} \circ \mathrm{N}_{K/k}$. On a $\mathrm{H}^1(G, \mathcal{A}_K(S_K)) = 0$ si et seulement si ν est injective sur $\mathcal{A}_K(S_K)$, donc (comme $\nu(\mathcal{C}\ell_K(S_K)) = j_{K/k}(\mathcal{A}_k(S_k))$ car $\mathrm{N}_{K/k}(S_K) = S_k$) si et seulement si*

on a l'isomorphisme $\nu : cl_K(S_K) \xrightarrow{\simeq} j_{K/k}(cl_k(S_k)) \subseteq cl_K(S_K)$ *qui indique que* $cl_K(S_K) = j_{K/k}(cl_k(S_k))$ *; or* $j_{K/k}(cl_k(S_k)) = cl_K(S_K)^{p^n}$ *puisque si* $\mathfrak{p} \in S_k$*, on a* $j_{K/k}(\mathfrak{p}) = \mathfrak{P}^{p^n}$, $\mathfrak{P} \mid \mathfrak{p}$ *dans* K*, d'où* $cl_K(S_K) = cl_K(S_K)^{p^n}$ *et* $cl_K(S_K) = 1$*. On a donc* $\mathrm{H}^1(G, cl_K(S_K)) = 0$ *si et seulement si* $cl_K(S_K) = 1$*.*
(ii) Si $\lambda = \mu = 0$*,* $cl_K(S_K)$ *est borné dans la tour et on a* $j_{K/k}(cl_k(S_k)) = cl_K(S_K)^{p^n} = 1$ *pour* $n \gg 0$ *(capitulation de* $cl_k(S_k)$ *dans* k_∞*). De même il y a, pour tout* n*, capitulation de* $cl_K(S_K)$ *dans* k_∞*.*

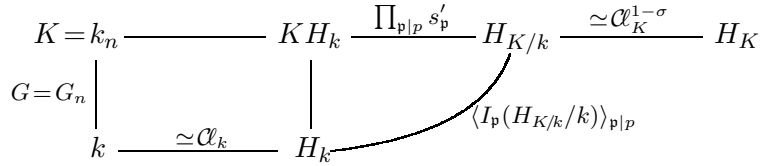
4. Symboles de restes normiques

Par commodité, rappelons (cf. [**14**, § II.4.4.3]) une méthode de calcul des symboles de restes normiques de Hasse $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right) \in G_n := \mathrm{Gal}(k_n/k)$, dans le cas particulier d'un corps de nombres Galoisien k avec $k_n \subset k_\infty$ de degré p^n sur k, et relativement à un idéal premier $\mathfrak{p} \mid p$ de k pour $p > 2$ totalement décomposé dans $k/\mathbb{Q}$. Dans ce cas, le conducteur de k_n/k divise (p^{n+1}) car on a, localement, $1 + p^{n+1}\,\alpha_0 = (1 + p\,\alpha_0')^{p^n} = \mathrm{N}_{k_n/k}(1 + p\,\alpha_0')$, où α_0, α_0' sont des p-entiers du produit des p-complétés de k. Le conducteur de $\mathbb{Q}_n$ est p^{n+1} $(n \geq 1)$.
Les calculs en question sont liés à la théorie des genres dont nous rappelons d'abord l'essentiel.

4.1. Suite exacte des genres pour les sous-corps de k_∞/k. — On désigne par H_k et H_K les p-corps de classes de Hilbert de k et $K := k_n$. Les groupes d'inertie $I_\mathfrak{p}(K/k)$ des $\mathfrak{p} \mid p$ dans K/k sont égaux à $G := G_n$.
On considère l'application $\omega := \omega_n$ qui associe à $x \in E_k$ la famille des symboles de Hasse $\left(\frac{x\,,K/k}{\mathfrak{p}}\right) \in G$, $\mathfrak{p} \mid p$.
On obtient alors la suite exacte des genres interprètant la formule du produit des symboles de Hasse d'une unité (voir, e.g., [**14**, Proposition IV.4.5.1] pour $T = S = \emptyset$) :

$$\begin{aligned} 1 \to E_k/E_k \cap \mathrm{N}_{K/k}(K^\times) \xrightarrow{\omega} \Omega(K/k) \subseteq \bigoplus_{\mathfrak{p}\mid p} I_\mathfrak{p}(K/k) \\ \xrightarrow{\pi} \mathrm{Gal}(H_{K/k}/KH_k) \to 1, \end{aligned} \tag{4.1}$$

où $\Omega(K/k) := \left\{(s_\mathfrak{p})_\mathfrak{p} \in \bigoplus_{\mathfrak{p}\mid p} I_\mathfrak{p}(K/k),\ \prod_{\mathfrak{p}\mid p} s_\mathfrak{p} = 1\right\} \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d-1}$ et où $H_{K/k}$ est *le p-corps des genres* de K défini comme la sous-extension maximale de H_K, Abélienne sur k, selon le schéma suivant, $H_{K/k}$ étant fixé par l'image, par l'application d'Artin, de $\mathcal{C}\ell_K^{1-\sigma}$, où $\sigma := \sigma_n$ est un générateur de G (en effet, le groupe des commutateurs $[\Gamma, \Gamma]$ de $\Gamma = \mathrm{Gal}(H_K/k)$ est $\mathrm{Gal}(H_K/K)^{1-\sigma}$, $\Gamma/\mathrm{Gal}(H_K/K)$ étant cyclique) :



L'image de ω est contenue dans $\Omega(K/k)$ et l'application $\pi := \pi_n$ est ainsi définie : à $(s_\mathfrak{p})_\mathfrak{p} \in \bigoplus_{\mathfrak{p}|p} I_\mathfrak{p}(K/k)$, π associe le produit $\prod_{\mathfrak{p}|p} s_\mathfrak{p}'$ des relèvements

$s'_{\mathfrak{p}}$ des $s_{\mathfrak{p}}$ dans les groupes d'inertie $I_{\mathfrak{p}}(H_{K/k}/k)$ qui engendrent $\mathrm{Gal}(H_{K/k}/H_k)$; il résulte de la formule du produit que si $(s_{\mathfrak{p}})_{\mathfrak{p}}$ est dans $\Omega(K/k)$, $\prod_{\mathfrak{p}|p} s'_{\mathfrak{p}}$ fixe à la fois H_k et K, donc KH_k.

On a ainsi $\pi\big(\Omega(K/k)\big) = \mathrm{Gal}(H_{K/k}/KH_k)$ et $\mathrm{Ker}(\pi) = \omega(E_k)$.

On a, comme attendu, $[H_{K/k} : K] = \frac{\#\mathcal{C}\ell_K}{\#\mathcal{C}\ell_K^{1-\sigma}} = \#\mathcal{C}\ell_K^G$. On montrera que ce degré $[H_{K/k} : K]$ (et donc $\#\mathcal{C}\ell_K^G$) est constant à partir du rang $n = e$ (i.e., $[K : \mathbb{Q}] \geq p^e$) donné par l'exposant p^e du groupe de torsion de $\mathrm{Gal}(H_k^{\mathrm{pr}}/H_k)$, où H_k^{pr} est la pro-p-extension Abélienne p-ramifiée maximale de k, et que ce degré est égal à $\#\mathcal{T}_k$, où $\mathcal{T}_k$ est le groupe de torsion de $\mathrm{Gal}(H_k^{\mathrm{pr}}/k)$ (cf. Théorèmes 4.2 et 4.3).

4.2. Calcul effectif des symboles $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right)$, $n \geq 1$. — Soit $x \in k^\times$ et soit $\mathfrak{p} \mid p$ un idéal premier de k au-dessus de p (x n'est pas supposé étranger à $\mathfrak{p}$). Soit $x'_{\mathfrak{p}} \in k^\times$ (appelé un $\mathfrak{p}$-associé de x relativement à k_n/k; on ne fait provisoirement aucune hypothèse sur la décomposition de p et si $\mathfrak{p} \mid p$ est unique, x est son propre associé) tel que (théorème des restes chinois) :

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

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

Par la formule du produit, on a $\left(\frac{x'_{\mathfrak{p}}\,,k_n/k}{\mathfrak{p}}\right) = \prod\limits_{\mathfrak{q}\,,\,\mathfrak{q}\neq\mathfrak{p}} \left(\frac{x'_{\mathfrak{p}}\,,k_n/k}{\mathfrak{q}}\right)^{-1}$, et comme $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right) = \left(\frac{x'_{\mathfrak{p}}\,,k_n/k}{\mathfrak{p}}\right)$ d'après (i) et la définition du $\mathfrak{p}$-conducteur de k_n/k, $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right) = \prod_{\mathfrak{q}\,,\,\mathfrak{q}\neq\mathfrak{p}} \left(\frac{x'_{\mathfrak{p}}\,,k_n/k}{\mathfrak{q}}\right)^{-1}$. Calculons les symboles de ce produit :

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

Finalement, $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right) = \prod_{\mathfrak{q}\,|\not{p}} \left(\frac{k_n/k}{\mathfrak{q}}\right)^{-v_{\mathfrak{q}}(x'_{\mathfrak{p}})}$. Posons $\mathfrak{a}_{\mathfrak{p}}(x) = \prod_{\mathfrak{q}\,|\not{p}} \mathfrak{q}^{v_{\mathfrak{q}}(x'_{\mathfrak{p}})}$ ($\mathfrak{a}_{\mathfrak{p}}(x)$ est étranger à p), alors on a $(x'_{\mathfrak{p}}) =: \mathfrak{p}^{v_{\mathfrak{p}}(x'_{\mathfrak{p}})}\mathfrak{a}_{\mathfrak{p}}(x) = \mathfrak{p}^{v_{\mathfrak{p}}(x)}\mathfrak{a}_{\mathfrak{p}}(x)$, et on a obtenu $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right) = \left(\frac{k_n/k}{\mathfrak{a}_{\mathfrak{p}}(x)}\right)^{-1}$ (inverse du symbole d'Artin de $\mathfrak{a}_{\mathfrak{p}}(x)$). On vérifie que $\left(\frac{k_n/k}{\mathfrak{a}_{\mathfrak{p}}(x)}\right)$ ne dépend pas du choix de $x'_{\mathfrak{p}}$. Si $v_{\mathfrak{p}}(x) = 0$, alors $\mathfrak{a}_{\mathfrak{p}}(x) = (x'_{\mathfrak{p}})$. En dépit des notations, $(x'_{\mathfrak{p}})$ et $\mathfrak{a}_{\mathfrak{p}}(x)$ dépendent de $n \geq 1$.

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

Définition 4.1. — *(i) Si $x \in k^\times$ est étranger à p, on définit les coefficients $\delta_{\mathfrak{p}}(x)$, $\mathfrak{p} \mid p$, par la relation :* $(x^{p-1} - 1) = p \cdot \prod\limits_{\mathfrak{p}|p} \mathfrak{p}^{\delta_{\mathfrak{p}}(x)} \cdot \mathfrak{b}_p$, *$\mathfrak{b}_p$ étranger à p.*

(ii) Si $x \in k^\times$ n'est pas étranger à p, on définit les coefficients $\delta_{\mathfrak{p}}(x)$ par les relations : $\big((x \cdot p^{-v_{\mathfrak{p}}(x)})^{p-1} - 1\big) = \mathfrak{p} \cdot \mathfrak{p}^{\delta_{\mathfrak{p}}(x)} \cdot \mathfrak{b}_{\mathfrak{p}}$, $\mathfrak{b}_{\mathfrak{p}}$ *étranger à $\mathfrak{p}$, $\mathfrak{p} \mid p$.*

Ces définitions peuvent s'exprimer en termes de valuations logarithmiques conduisant aux groupes de classes logarithmiques introduits par Jaulent (cf. **[33]** ainsi que **[2]** pour les aspects numériques, et **[14**, § III.5] pour des généralités logarithmiques et cyclotomiques liées à la conjecture de Gross). Jaulent ([**35**, Théorème 7]) montre que la conjecture de Greenberg équivaut à la capitulation du p-groupe des classes logarithmiques de k dans k_∞.

On suppose désormais p totalement décomposé dans k.

Lemme 4.1. — *Soit $x \in k^\times$ étranger à p et soit $\mathfrak{p} \mid p$ fixé. Soit $\mathfrak{a}_\mathfrak{p}(x) = (x'_\mathfrak{p})$, où $x'_\mathfrak{p}$ est un $\mathfrak{p}$-associé de x relativement à k_n/k. Alors $\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x)) \equiv x \pmod{\mathfrak{p}^{n+1}}$ et, pour tout $n \geq \delta_\mathfrak{p}(x)$, $\frac{1}{p} \cdot \log(\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x))) \equiv \alpha_\mathfrak{p}(x) \cdot p^{\delta_\mathfrak{p}(x)} \pmod{p^n}$, $\alpha_\mathfrak{p}(x) \in \mathbb{Z}_p^\times$.*

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

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

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

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

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

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

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

mais comme $\mathrm{N}_{k/\mathbb{Q}}(x'_\mathfrak{p})$ est rationnel, on a $v_p(\mathrm{N}_{k/\mathbb{Q}}(x'_\mathfrak{p})^{p-1} - 1) = \delta_\mathfrak{p}(x) + 1$, d'où le lemme en prenant le "logarithme normalisé" $\frac{1}{p} \cdot \log$ (ce qui donne 0 modulo p^n si $n \leq \delta_\mathfrak{p}(x)$). □

Le cas $v_\mathfrak{p}(x) \neq 0$ se traite comme suit et couvre tous les cas :

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

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

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

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

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

$$\tfrac{1}{p} \cdot \log(\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a}_\mathfrak{p}(x))) =: \alpha_\mathfrak{p}(x) \cdot p^{\delta_\mathfrak{p}(x)} \pmod{p^n}, \quad \alpha_\mathfrak{p}(x) \in \mathbb{Z}_p^\times.$$

On peut énoncer en résumé :

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

Soit $\mathcal{N}_k^n$ le sous-groupe des $x \in k^\times$ partout normes locales dans k_n/k en dehors de p. D'après l'étude et le calcul effectif des symboles de Hasse vus précédemment, on peut identifier ω_n (cf. § 4.1), qui à $x \in \mathcal{N}_k^n$ associe la famille des symboles de Hasse $\left(\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right)\right)_{\mathfrak{p}|p}$ dans $\Omega(k_n/k)$, à l'application :

$$\begin{array}{rccc} \omega'_n : & \mathcal{N}_k^n & \longrightarrow & \prod\limits_{\mathfrak{p}|p} \mathbb{Z}/p^n\,\mathbb{Z}. \\ & x & \longmapsto & \left(\alpha_\mathfrak{p}(x) \cdot p^{\delta_\mathfrak{p}(x)} \pmod{p^n}\right)_{\mathfrak{p}|p} \end{array}$$

dont l'image est dans l'ensemble des $(\alpha_\mathfrak{p} \cdot p^{\delta_\mathfrak{p}})_{\mathfrak{p}|p} \in \prod\limits_{\mathfrak{p}|p} \mathbb{Z}/p^n\,\mathbb{Z}$ vérifiant la relation $\sum\limits_{\mathfrak{p}|p} \alpha_\mathfrak{p} \cdot p^{\delta_\mathfrak{p}} \equiv 0 \pmod{p^n}$ (formule du produit sur les p-places).

Corollaire 4.1. — *Si $x \in k^\times$ est partout norme locale en dehors de p dans k_n/k (i.e., (x) norme d'un idéal de k_n), il est alors partout norme locale (donc norme globale dans k_n/k) si et seulement si $\delta_\mathfrak{p}(x) \geq n$ pour tout $\mathfrak{p} \mid p$ (sauf un en raison de la formule du produit).*

D'un point de vue heuristique on a, a priori, $\delta_\mathfrak{p}(x) \geq r$ avec la probabilité $\frac{1}{p^r}$, de sorte qu'en général $\left(\frac{x\,,k_n/k}{\mathfrak{p}}\right) = \left(\frac{k_n/k}{\mathfrak{a}_\mathfrak{p}(x)}\right)^{-1}$ est un générateur de G_n, ce qui est très favorable pour la conjecture de Greenberg comme le montre, par exemple, le Théorème 3.2 où le point (ii) est satisfait dès que l'on a suffisamment de S_k-unités dont les symboles engendrent G_1. Cependant, le cas de $x \in k^\times$ partout norme locale en dehors de p dans k_n/k montre que les $\delta_\mathfrak{p}(x)$ ne sont pas indépendants en raison de la formule du produit (considérée comme unique) ; pour x étranger à p, ceci implique $\mathrm{N}_{k/\mathbb{Q}}(x)^{p-1} \equiv 1 \pmod{p^{n+1}}$, car le symbole d'Artin de $\mathrm{N}_{k/\mathbb{Q}}(x)$ dans $\mathbb{Q}_n/\mathbb{Q}$ est égal à 1.

Proposition 4.1. — *(i) Soit Λ un sous-groupe de $k^\times$ tel que tout $x \in \Lambda$ soit partout norme locale en dehors de p dans k_n/k, pour $n \geq 1$ donné (i.e., (x) norme d'un idéal de k_n). On suppose que $(\Lambda : \Lambda \cap \mathrm{N}_{k_1/k}(k_1^\times)) = p^{d-1}$; alors on a $(\Lambda : \Lambda \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)}$.*
(ii) Si Λ est un sous-groupe de $E_k^{S_k}$, on a $(\Lambda : \Lambda \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)}$ pour tout $n \geq 1$ dès que ceci est vrai pour $n = 1$.

Démonstration. — L'hypothèse signifie $\omega_1(\Lambda) = \Omega(k_1/k)$ (cf. § 4.1). Il existe donc des éléments $x_j \in \Lambda$, $1 \leq j \leq d-1$, tels que:

$$\Omega(k_1/k) = \bigoplus_{j=1}^{d-1} \langle \omega_1(x_j) \rangle \ ;$$

les $\omega_1(x_j)$ sont les images canoniques des $\omega_\infty(x_j) := \big(\big(\frac{x_j\,,\,k_\infty/k}{\mathfrak{p}}\big)\big)_{\mathfrak{p}|p}$ (par restriction des symboles de Hasse) qui constituent une $\mathbb{Z}_p$-base topologique d'un sous-$\mathbb{Z}_p$-module (de dimension $d-1$) de $\mathrm{Gal}(k_\infty/k)^d \simeq \mathbb{Z}_p^d$ car toute relation $\prod_{j=1}^{d-1}\omega_\infty(x_j)^{a_j}=1$, $a_j\in\mathbb{Z}_p$ non tous divisibles par p, conduit par restriction à une relation non triviale au niveau $n=1$.

Au niveau n, $\omega_n(\Lambda)=\bigoplus_{j=1}^{d-1}\langle\omega_n(x_j)\rangle$ d'ordre $p^{n\cdot(d-1)}$. Mais pour $m>n$, les $x\in\Lambda$ ne sont plus nécessairement normes locales en dehors de p dans k_m/k et donc $\omega_m(x)$ n'est plus nécessairement dans $\Omega(k_m/k)$.

Pour $\Lambda\subseteq E_k^{S_k}$, la condition de normes locales en dehors de p dans k_n/k est satisfaite pour tout n et dans ce cas, les $\omega_\infty(x_j)$ engendrent $\Omega(k_\infty/k)$. □

4.3. Groupe de torsion de la p-ramification Abélienne. — Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale H_k^{pr} de k.

On a, en désignant par $U_k:=\prod_{\mathfrak{p}|p}U_\mathfrak{p}$ (où $U_\mathfrak{p}=1+\mathfrak{p}$) le groupe des unités locales principales de k, et par $\overline{E}_k$ l'adhérence de E_k dans U_k ou plus précisément l'image dans U_k de $E_k\otimes\mathbb{Z}_p$, la suite exacte classique :

$$1\longrightarrow \mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k)\longrightarrow \mathcal{T}_k\longrightarrow \mathcal{C}\ell_k\longrightarrow 1,$$

puisqu'ici $H_k\cap k_\infty=k$. En appliquant la formule analytique donnant $\#\mathcal{T}_k$ dans le cas réel sous la conjecture de Leopoldt (cf. [**6**, Appendix (1975)], [**47**, (1978)], [**14**, Remark III.2.6.5 (i)]), en tenant compte du fait que p est totalement décomposé dans k, que $\frac{1}{p}\prod_{\mathfrak{p}|p}\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{p})=p^{d-1}$, et que le régulateur p-adique normalisé R_k est le régulateur p-adique classique divisé par p^{d-1}, on a $\#\mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k)\sim R_k$ (voir aussi [**20**]).

Par abus, nous écrirons que ce régulateur R_k est égal à $p^{v_p(R_k)}$ bien qu'il soit (sous la conjecture de Leopoldt) un élément non nul de $\mathbb{Z}_p$ défini à une unité p-adique près. Posons $U_k^*:=\{u\in U_k,\ \mathrm{N}_{k/\mathbb{Q}}(u)=1\}$. De fait, on a

$$\mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k)=U_k^*/\overline{E}_k,$$

car si $u^{p^r}\in\overline{E}_k$, alors $\mathrm{N}_{k/\mathbb{Q}}(u)=1$ puisque $\mathrm{N}_{k/\mathbb{Q}}(\overline{E}_k)=\{1\}$ et que U_k est sans p-torsion ; enfin, U_k^* est un $\mathbb{Z}_p$-module libre de rang $d-1$ dans lequel $\overline{E}_k$ est d'indice fini (conjecture de Leopoldt). D'où finalement :

$$\#\mathcal{T}_k=\#\mathcal{C}\ell_k\cdot\#(U_k^*/\overline{E}_k)\quad\&\quad\#(U_k^*/\overline{E}_k)=R_k. \tag{4.2}$$

Théorème 4.2. — *Soit k Galoisien réel de degré d dans lequel $p>2$ est totalement décomposé. On suppose que la conjecture de Leopoldt est vraie pour p dans k. Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale H_k^{pr} de k et soit p^e l'exposant de $U_k^*/\overline{E}_k$.*

(i) Pour tout n, il existe une injection ψ_n de $E_k\cap\mathrm{N}_{k_n/k}(k_n^\times)/E_k^{p^n}$ dans $U_k^*/\overline{E}_k$; par conséquent $\dfrac{p^{n\cdot(d-1)}}{(E_k:E_k\cap\mathrm{N}_{k_n/k}(k_n^\times))}$ divise R_k et il en résulte que $\#\mathcal{C}\ell_{k_n}^{G_n}=\#\mathcal{C}\ell_k\cdot\dfrac{p^{n\cdot(d-1)}}{(E_k:E_k\cap\mathrm{N}_{k_n/k}(k_n^\times))}$ divise $\#\mathcal{T}_k$ (cf. Relation (4.2)).

(ii) Pour tout $n\geq e$, l'application ψ_n est surjective, et alors les divisibilités précédentes sont des égalités. En particulier on a $\#\mathcal{C}\ell_{k_n}^{G_n}=\#\mathcal{T}_k$ et la suite exacte $1\to E_k^{p^n}\longrightarrow E_k\cap\mathrm{N}_{k_n/k}(k_n^\times)\xrightarrow{\psi_n}U_k^*/\overline{E}_k\to 1$.

(iii) Si l'on peut trouver $n_0 \geq e$ tel que le critère de Greenberg soit vérifié en n_0 (i.e., $\mathcal{C}\ell_{k_{n_0}}^{G_{n_0}} = cl_{k_{n_0}}(S_{k_{n_0}})$), alors il est vérifié pour tout $n \geq n_0$ et il en résulte que $\lambda = \mu = 0$.

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

Soit $\varepsilon \in E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)$; par conséquent on a $\delta_{\mathfrak{p}}(\varepsilon) \geq n$ pour tout $\mathfrak{p} \mid p$ (Corollaire 4.1). Donc $\varepsilon = u^{p^n}$, où $u \in U_k^*$ est unique.

(α) (définition de ψ_n). Soit ψ_n l'application qui à $\varepsilon \in E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)$ associe la classe de u dans $U_k^*/\overline{E}_k$. L'application ψ_n est bien définie.

(β) (calcul de $\mathrm{Ker}(\psi_n)$). Si $u_0 \in \overline{E}_k$, alors $\varepsilon \in (\overline{E}_k)^{p^n}$ est arbitrairement proche d'un élément de $E_k^{p^n}$; en effet, $\varepsilon = \varepsilon_N'^{p^n} \cdot u_N$, $\varepsilon_N' \in E_k$, $u_N \to 1$ dans E_k pour $N \to \infty$ (e.g., $u_N \equiv 1 \pmod{p^{N+1}}$), d'où $u_N \in E_k^{p^n}$ (conjecture de Leopoldt [**14**, Théorème III.3.6.2 (iv)] en lien avec la constante de Kummer–Leopoldt [**1**], [**20**]) ; d'où $\varepsilon \in E_k^{p^n}$ et $\mathrm{Ker}(\psi_n) = E_k^{p^n}$. A ce stade, puisque $(E_k : E_k^{p^n}) = p^{n\cdot(d-1)}$, on obtient pour tout n les divisibilités du (i).

(γ) (surjectivité pour $n \geq e$). Soit $u \in U_k^*$ et écrivons que $u^{p^e} \in \overline{E}_k$; pour tout $N \gg 0$, il existe $\varepsilon_N' \in E_k$ tel que $u^{p^e} = \varepsilon_N' \cdot u_N$, $u_N \to 1$. D'où $u_N = u_1^{p^N} = (u_1^{p^e})^{p^{N-e}}$, $u_1 \in U_k^*$ et $u_1^{p^e} =: \overline{\varepsilon} \in \overline{E}_k$ par définition de e. Donc $u_N = \overline{\varepsilon}'^{p^e}$ pour $N \gg 0$, auquel cas $u^{p^e} = \varepsilon_N' \cdot \overline{\varepsilon}'^{p^e}$; par conséquent il existe $u' = u \cdot \overline{\varepsilon}'^{-1}$ dans la classe de u' donc de u modulo $\overline{E}_k$ tel que $u'^{p^e} = \varepsilon_N'$. Posons $\varepsilon := \varepsilon_N'^{p^{n-e}} = u'^{p^n}$ (car $n \geq e$) ; étant partout norme locale, $\varepsilon \in \mathrm{N}_{k_n/k}(k_n^\times)$ et $\psi_n(\varepsilon)$ est la classe de u modulo $\overline{E}_k$.

D'où la surjectivité de ψ_n, puis $\dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} = \#(U_k^*/\overline{E}_k) = R_k$, et finalement $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{T}_k$.

(δ) (calcul direct de l'ordre pour $n \geq e$). Puisque p^e annule $U_k^*/\overline{E}_k$, on a pour $n \geq e$, $U_k^*/\overline{E}_k = U_k^*/U_k^{*p^n}\overline{E}_k$ et la suite exacte :

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

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

(ε) (effectivité du critère de Greenberg). Posons $M_1^n := \mathcal{C}\ell_{k_n}^{G_n}$ pour tout $n \geq 0$; alors $\#M_1^n = \#\mathcal{T}_k$ pour tout $n \geq e$. Soit $n \geq n_0$ et posons $M_1' := cl_{k_n}(S_{k_n}) \subseteq M_1^n$; par la norme $\mathrm{N}' := \mathrm{N}_{k_n/k_{n_0}}$ il vient $\mathrm{N}'(M_1') = M_1^{n_0}$, car $\mathrm{N}'(S_{k_n}) = S_{k_{n_0}}$. En raison des ordres, il en résulte que N' induit un isomorphisme $M_1' \simeq M_1^{n_0}$, d'où $M_1' = M_1^n = cl_{k_n}(S_{k_n})$ pour tout $n \geq n_0$, d'où $\lambda = \mu = 0$ (Théorème 2.1). □

Théorème 4.3. — *Soit k Galoisien réel de degré d dans lequel $p > 2$ est totalement décomposé. On suppose que la conjecture de Leopoldt est vraie pour p dans k. Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale H_k^{pr} de k et soit p^e l'exposant de $U_k^*/\overline{E}_k$. Soit $H_{k_n/k}$ le p-corps des genres de k_n (cf. § 4.1).*

(i) On a $[H_{k_n/k} : k_n] = \#\mathcal{T}_k$, pour tout $n \geq e$.

(ii) On a $k_\infty H_{k_e/k} = H_k^{\rm pr}$ *et l'extension* $H_k^{\rm pr}/k_\infty$ *est non ramifiée.*[(1)]
(iii) Soit $\Lambda \supseteq E_k$ *un sous-groupe de* $k^\times$ *tel que tout* $x \in \Lambda$ *soit norme locale dans* k_n/k *en dehors de* p*, pour un entier* $n \geq 0$ *donné (i.e.,* (x) *norme d'un idéal de* k_n*). Alors* $\dfrac{p^{n\cdot(d-1)}}{(\Lambda : \Lambda \cap {\rm N}_{k_n/k}(k_n^\times))}$ *divise* R_k*.*
Pour $E_k \subseteq \Lambda \subseteq E_k^{S_k}$*, cette divisibilité a lieu pour tout* n*.*

Démonstration. — (i) Considérons les p-corps des genres $H_{k_e/k}$ et $H_{k_n/k}$; on a $H_{k_e/k}k_n \subseteq H_{k_n/k}$ en raison de la totale ramification de p dans k_∞/k et de l'Abélianité de $H_{k_e/k}k_n/k$. D'où la valeur stationnaire du degré $[H_{k_n/k} : k_n]$ puisque $[H_{k_n/k} : k_n] = \#\mathcal{C}\ell_{k_n}^{G_n}$ et que $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{T}_k$ pour tout $n \geq e$ d'après le Théorème 4.2 (ii). D'où (i) et par conséquent (ii).
(iii) On a les injections canoniques

$$E_k/E_k \cap {\rm N}_{k_n/k}(k_n^\times) \hookrightarrow \Lambda/\Lambda \cap {\rm N}_{k_n/k}(k_n^\times) \hookrightarrow \Omega(k_n/k) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d-1},$$

car les symboles de Hasse en p (pour k_n/k) des $x \in \Lambda$ vérifient la formule du produit par hypothèse.
Donc $\dfrac{p^{n\cdot(d-1)}}{(\Lambda : \Lambda \cap {\rm N}_{k_n/k}(k_n^\times))}$ divise $\dfrac{p^{n\cdot(d-1)}}{(E_k : E_k \cap {\rm N}_{k_n/k}(k_n^\times))}$, lequel divise R_k (Théorème 4.2 (i)). □

Remarque 4.1. — *La théorie des genres dit que l'image par* π_n *de* $\Omega(k_n/k)$ *est* ${\rm Gal}(H_{k_n/k}/k_nH_k)$ *et que le noyau de* π_n *est* $\omega_n(E_k) \subseteq \Omega(k_n/k)$*, où* $\omega_n(\varepsilon) = \left(\left(\frac{\varepsilon\,,k_n/k}{\mathfrak{p}}\right)\right)_{\mathfrak{p}|p}$ *pour tout* $\varepsilon \in E_k$ *et* $\#\omega_n(E_k) = (E_k : E_k \cap {\rm N}_{k_n/k}(k_n^\times))$ *; en introduisant le sous-groupe* $\mathcal{N}_k^n$ *des* $x \in k^\times$ *partout norme locale dans* k_n/k *en dehors de* p*, on a* $\Omega(k_n/k) = \omega_n(\mathcal{N}_k^n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d-1}$*, et* $\pi_n(\Omega(k_n/k)) = \pi_n \circ \omega_n(\mathcal{N}_k^n) = {\rm Gal}(H_{k_n/k}/k_nH_k)$*. Ainsi, pour tout* $n \geq 0$ *fixé, l'application :*

$$\theta_n := \pi_n \circ \omega_n \ : \ \mathcal{N}_k^n \xrightarrow{\omega_n} \Omega(k_n/k) \xrightarrow{\pi_n} {\rm Gal}(H_{k_n/k}/k_nH_k)$$

est surjective de $\mathcal{N}_k^n$ *sur* ${\rm Gal}(H_{k_n/k}/k_nH_k)$ *et de noyau* $E_k \cdot {\rm N}_{k_n/k}(k_n^\times)$*.*
Par conséquent, l'image par θ_n *d'un sous-groupe* Λ *de* $\mathcal{N}_k^n$ *contenant* E_k *est un sous-groupe de* ${\rm Gal}(H_{k_n/k}/k_nH_k)$ *isomorphe à* $\omega_n(\Lambda)/\omega_n(E_k)$*, où* $\#\omega_n(\Lambda) = (\Lambda : \Lambda \cap {\rm N}_{k_n/k}(k_n^\times))$*. Autrement dit, on a la suite exacte :*

$$1 \to E_k/E_k \cap {\rm N}_{k_n/k}(k_n^\times) \longrightarrow \Lambda/\Lambda \cap {\rm N}_{k_n/k}(k_n^\times) \xrightarrow{\theta_n} \theta_n(\Lambda) \subseteq {\rm Gal}(H_{k_n/k}/k_nH_k) \to 1.$$

L'image par π_n *d'un sous-groupe de* $\bigoplus_{\mathfrak{p}|p} I_{\mathfrak{p}}(k_n/k)$*, non contenu dans* $\Omega(k_n/k)$*, n'est pas nécessairement dans* ${\rm Gal}(H_{k_n/k}/k_nH_k)$ *par absence de la formule du produit sur les p-places.*

Théorème 4.4. — *Soit* $\mathcal{N}_k^n$*, pour* $n \geq 0$ *fixé, le sous-groupe des* $x \in k^\times$ *partout norme locale en dehors de* p *dans* k_n/k *(i.e.,* (x) *norme d'un idéal de* k_n*) et soit* $\theta_n := \pi_n \circ \omega_n$ *(cf. § 4.1 et Remarque 4.1).*
(i) Pour tout sous-groupe Λ *de* $\mathcal{N}_k^n$ *contenant* E_k*,* $\theta_n(\Lambda)$ *est isomorphe à un sous-groupe de* ${\rm Gal}(H_{k_n/k}/k_nH_k)$*, lequel est isomorphe à un quotient de* ${\rm Gal}(H_k^{\rm pr}/k_\infty H_k) \simeq U_k^*/\overline{E}_k \subseteq \mathcal{T}_k$ *et* $\#\theta_n(\Lambda)$ *divise* R_k*.*

(1) Ce résultat est démontré dans [**52**, Theorem 1.1, Lemma 2.3] par introduction du corps des genres. Voir aussi les approches de [**35**] et [**42**].

Pour $r \leq n$, $\#\theta_r(\Lambda)$ divise $\#\theta_n(\Lambda)$.

(ii) Si $n \geq e$, où p^e est l'exposant de $U_k^*/\overline{E}_k$, alors $\theta_n(\Lambda) \simeq \theta_e(\Lambda)$.

(iii) Si $E_k \subseteq \Lambda \subseteq E_k^{S_k}$, alors les $\#\theta_n(\Lambda)$ forment une n-suite croissante (stationnaire à partir de $n = e$) de diviseurs de R_k.

Démonstration. — Soit $r \leq n$. Comme $H_{k_r/k} \subseteq H_{k_n/k}$, pour $\mathfrak{p} \mid p$, les symboles $\left(\frac{x\,,\, H_{k_r/k}/H_k}{\mathfrak{p}}\right)$ sont les restrictions des $\left(\frac{x\,,\, H_{k_n/k}/H_k}{\mathfrak{p}}\right)$, et l'image de $\theta_n(x) = \prod_{\mathfrak{p}\mid p} \left(\frac{x\,,\, H_{k_n/k}/H_k}{\mathfrak{p}}\right)$ dans la surjection canonique :

$$\mathrm{Gal}(H_{k_n/k}/k_nH_k) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(H_{k_r/k}/k_rH_k)$$

est $\theta_r(x)$, et par conséquent on a une surjection $\theta_n(\Lambda) \longrightarrow\!\!\!\!\!\rightarrow \theta_r(\Lambda)$, d'où la relation entre les ordres. Si $n \geq e$, la surjection devient l'isomorphisme :

$$\mathrm{Gal}(H_{k_n/k}/k_nH_k) \simeq \mathrm{Gal}(H_{k_e/k}/k_eH_k)$$

du Théorème 4.3 (i), et $\theta_n(\Lambda)$ est isomorphe à $\theta_e(\Lambda)$ d'où le résultat.

Si $E_k \subseteq \Lambda \subseteq E_k^{S_k}$, ce qui précède est valable quel que soit n □

Remarques 4.1. — *(i) Certains résultats de théorie d'Iwasawa donnent des isomorphismes au niveau infini mettant en jeu le groupe $\mathcal{T}_k$ (cf.* [**38**, Lemma 4.7], [**51**], [**52**], [**44**], [**3**, Lemme 3.1]*), mais en réalité, il y a régularisation à un niveau fini explicite ne dépendant que du régulateur p-adique de k.*

(ii) Si $\mathcal{T}_k = 1$ (i.e., k est p-rationnel, [**14**, § IV.3], [**13**], [**36**], [**39**]*), on a évidemment $\lambda = \mu = \nu = 0$; ceci s'applique par exemple au corps cubique étudié dans* [**53**] *pour $p = 5$.*

On trouvera dans [**19**] *une étude détaillée des régulateurs p-adiques qui représentent le facteur crucial puisque $\mathcal{C}\ell_k$ est non trivial uniquement pour un nombre fini de p tandis que c'est seulement conjecturé pour R_k.*

(iii) On a $\mathcal{T}_k = 1$ si et seulement si $\mathcal{C}\ell_k = R_k = 1$, et alors (sous la conjecture de Leopoldt dans la tour), la formule de points fixes donnant $\#\mathcal{T}_{k_n}^{G_n}$ ([**14**, Théorème IV.3.3, § IV (b)], [**39**]*) conduit à $\mathcal{T}_{k_n} = 1$ car k_n/k est "p-primitivement ramifiée" (p-rationalité dans la tour). D'où $\mathcal{C}\ell_{k_n} = 1$ et $R_{k_n} = 1$ pour tout $n \geq 0$.*

(iv) Soit $p^{\widetilde{e}}$ l'exposant de $\mathcal{T}_k$. Soit I_k le groupe des idéaux de k étrangers à p et, pour $n \geq \widetilde{e}$, soit :

$$\widetilde{E}_k^n := \{x \in k^\times,\, (x) \in I_k^{p^n}\}.$$

Alors on peut établir (en utilisant les techniques du § 7.4.2) une suite exacte de la forme :

$$1 \longrightarrow \{x \in k^\times,\, x \text{ étranger à } p\}^{p^n} \longrightarrow \widetilde{E}_k^n \cap \mathrm{N}_{k_n/k}(k_n^\times) \xrightarrow{\widetilde{\psi}_n} \mathcal{T}_k \longrightarrow 1.$$

Remarques 4.2. — *(i) Une S_k-unité est norme locale en dehors de p dans k_n/k pour tout $n \geq 0$, tandis que pour $x \notin E_k^{S_k}$ ceci n'est pas possible ; en effet, supposons (x) norme d'un idéal $\mathfrak{A}$ de k_n, pour tout n, et posons :*

$$(x) = \mathrm{N}_{k_n/k}(\mathfrak{A}) = \mathfrak{a} \cdot \prod_{\mathfrak{p}\mid p} \mathfrak{p}^{c_\mathfrak{p}},$$

$\mathfrak{a}$ étranger à p, $c_\mathfrak{p} \geq 0$; si $\mathfrak{l}^{c_\mathfrak{l}}$ est la composante $\mathfrak{l}$-primaire de $\mathfrak{a}$ pour l'idéal premier $\mathfrak{l}$, pour un idéal premier $\mathfrak{L} \mid \mathfrak{l}$ de k_n, il existe $\tau_n \in \mathbb{Z}[G_n]$ tel que :

$$\mathfrak{l}^{c_\mathfrak{l}} = \mathrm{N}_{k_n/k}(\mathfrak{L}^{\tau_n}) = \mathfrak{l}^{f_\mathfrak{l}^n \cdot \tau_n(1)},$$

où $f_\mathfrak{l}^n$ est le degré résiduel de $\mathfrak{l}$ dans k_n/k et $\tau_n(1) \in \mathbb{Z}$ est l'image de τ_n par l'application d'augmentation. Les $f_\mathfrak{l}^n$ étant strictement croissants pour $n \gg 0$, ceci est impossible sauf si $\tau_n(1) = 0$, auquel cas $c_\mathfrak{l} = 0$ et x est une S_k-unité.

Par conséquent, si $x \notin E_k^{S_k}$, il n'y a pas de formule du produit portant uniquement sur les p-places dans k_n/k pour n au-delà d'une certaine valeur dépendant des degrés résiduels des $\mathfrak{l} \mid (x)$ dans k_∞/k.

(ii) Le cadre de la conjecture de Greenberg et l'introduction de la filtration des groupes de classes $\mathcal{C}\ell_{k_n}$ par les $c\ell_{k_n}(\mathcal{I}_i^n)$ ($\mathcal{I}_i^n$ étrangers à p) qui sont les sous-groupes des classes annulées par $(1-\sigma_n)^i$, $0 \leq i \leq m_n - 1$, mettra en jeu les groupes $\Lambda_i^n = \{x \in k^\times,\ \ (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)\}$ et le calcul des $(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))$. Ceci fait l'objet de la Section 6.

Donc Λ_i^n ne contiendra pas de S_k-unités autres que les unités et l'aspect algorithmique se ramènera à l'étude des $x \in \Lambda_i^n$ et de leurs symboles normiques donnés par leurs quotients de Fermat en les $\mathfrak{p} \mid p$, ce qui constitue une approche différente de la conjecture de Greenberg.

5. Aspects numériques – Corps quadratiques réels

Soient $\mathfrak{p}_1$ et $\mathfrak{p}_2$ les deux idéaux premiers de $k = \mathbb{Q}(\sqrt{m})$ au-dessus de p et S_k leur ensemble. Les S_k-unités génératrices modulo les unités sont données par π_1 et sa $\mathbb{Q}$-conjuguée π_2, et sont telles que $(\pi_j) = \mathfrak{p}_j^{h_0}$ où h_0 est l'ordre de la classe des $\mathfrak{p}_j$, $j = 1, 2$.

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

Démonstration. — Soient $\omega_j \in k^\times$, $j = 1, 2$, deux nombres conjugués tels que $v_{\mathfrak{p}_j}(\omega_j) = 1$ et $\omega_1 \cdot \omega_2 = p\,\beta'$, avec β' étranger à p, et posons $\alpha^{p-1} =: \alpha_1^{p-1} = 1 + p \cdot \omega_1^{\delta_{\mathfrak{p}_1}(\alpha)} \omega_2^{\delta_{\mathfrak{p}_2}(\alpha)} \cdot \beta_1$, β_1 étranger à p, et soit α_2 le conjugué de α_1. On a $\mathrm{N}_{k/\mathbb{Q}}(\alpha)^{p-1} = (\alpha_1 \cdot \alpha_2)^{p-1} \equiv 1 \pmod{p^{n+1}}$; donc on obtient :

$$\omega_1^{\delta_{\mathfrak{p}_1}(\alpha)} \cdot \omega_2^{\delta_{\mathfrak{p}_2}(\alpha)} \cdot \beta_1 + \omega_2^{\delta_{\mathfrak{p}_1}(\alpha)} \cdot \omega_1^{\delta_{\mathfrak{p}_2}(\alpha)} \cdot \beta_2 + p^{1+\delta_{\mathfrak{p}_1}(\alpha)+\delta_{\mathfrak{p}_2}(\alpha)} \cdot \beta_1\,\beta_2\,\beta'' \equiv 0 \pmod{p^n};$$

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

Remarque 5.1. — *Dans cette situation, pour les corps quadratiques, les $\delta_\mathfrak{p}(\alpha)$ seront notés $\delta_p(\alpha)$. Ceci vaut pour un $\alpha \in k^\times$ étranger à p et partout norme locale en dehors de p dans k_n/k (i.e., norme d'un idéal de k_n) ; en effet, le conducteur de $\mathbb{Q}_n/\mathbb{Q}$ étant p^{n+1}, on a $\mathrm{N}_{k/\mathbb{Q}}(\alpha)^{p-1} \equiv 1 \pmod{p^{n+1}}$.*

Pour une unité ε de k, on a (indépendamment de n) $\varepsilon^{p-1} = 1 + p \cdot p^{\delta_p(\varepsilon)} \cdot \beta$, $\delta_p(\varepsilon) \geq 0$, avec β étranger à p.

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

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

$$\begin{aligned} x' &\equiv \pi_2 \pmod{\pi_1^{n+1}},\\ x' &\equiv 1 \pmod{\pi_2^{n+1}}, \end{aligned} \tag{5.1}$$

On détermine une "relation de Bézout" $U_1\cdot\pi_1^{n+1}+U_2\cdot\pi_2^{n+1}=1$, où $U_1,U_2\in Z_{k,(p)}$ (anneau des p-entiers de k), ce qui conduit à la solution $x'=U_1\cdot\pi_1^{n+1}+U_2\cdot\pi_2^{n+1}\cdot\pi_2 \pmod{p^{n+1}}$. On a $\mathfrak{a}_{\mathfrak{p}_1}(x)=(x')$ dont on prend la norme dans $k/\mathbb{Q}$ pour caractériser le symbole d'Artin pour k_n/k ; son ordre, dans $(\mathbb{Z}/p^{n+1}\,\mathbb{Z})^\times$, est de la forme $p^{n-\delta_{\mathfrak{p}_1}(\pi_2)}$.

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

5.2. Programmes PARI. — Le programme ci-dessous (d'après [**45**]) fournit les informations suivantes :

m, $h=$ nombre de classes de k, $\varepsilon=u+v\sqrt{m}=$ unité fondamentale de k, $u,v\in\mathbb{Z}$ ou $\frac{1}{2}\,\mathbb{Z}$, $S_k=:\{\pi_1,\,\pi_2\}$, $z_\pi=p^{-\delta_{\mathfrak{p}_1}(\pi_2)}$ et $z_\varepsilon=p^{-\delta_p(\varepsilon)}$, et aussi n_π et n_ε qui figurent les symboles de Hasse de π_2 et ε dans $\Omega(k_n/k)$.

D'après le Théorème 3.2, la conjecture de Greenberg est vérifiée dès que $\mathcal{cl}_k(S_k)=\mathcal{C}\ell_k$ et que l'un au moins des nombres z_π ou z_ε est égal à 1 (i.e., $\delta_{\mathfrak{p}_1}(\pi_2)=0$ ou $\delta_p(\varepsilon)=0$) car le symbole de Hasse correspondant engendre G_n pour tout n et de fait on a $\Omega(k_n/k)\simeq G_n$ (si $z_\varepsilon=1$, c'est que le régulateur normalisé $R_k\sim\frac{1}{p}\log(\varepsilon)$ est égal à 1). En pratique le programme utilise un n de l'ordre de 8 qui suffit largement dans tous les résultats numériques obtenus pour avoir les *valeurs exactes* de z_π et z_ε, mais d'après la Proposition 4.1, il suffit de prendre $n_0=1$ (donc $n=n_0+1=2$ et des calculs modulo p^2 seulement) pour obtenir tous les cas où le test est positif (i.e., $z_\pi=1$ ou $z_\varepsilon=1$).

Les mentions " PROBLÈME-NORMIQUE " (resp. " PROBLÈME-CLASSES ") signifient $z_\pi<1$ & $z_\varepsilon<1$ (resp. $\mathcal{cl}_k(S_k)\neq\mathcal{C}\ell_k$). On a $p\geq 3$.

```
{for(j=2, 10, p=prime(j); m=1; n0=8; n=n0+1; while(m<10^4, m=m+1;
if(core(m)==m & kronecker(m, p)==1, y=x; Q=x^2-m; K= bnfinit(Q,1);
M=m; t=Mod(m,4); if(t!=1, M=4*m); E=quadunit(M);
h=qfbclassno(M); e1=component(E,2); e2=component(E,3);
if(t==1, e2=e2/2; e1=e1+e2); E=e1+e2*x; print(" ");
print("m = ", m," h = ",h," E = ",E);
Su=bnfsunit(K,idealprimedec(K,p));
pi1=component(component(Su,1),1);
pi2=component(pi1,2)*x-component(pi1,1);
print("p = ",p," S = ",pi1," ",pi2); Pi1= pi1^n; Pi2= pi2^n;
Z=bezout(Pi1,Pi2); U1=component(Z,1); U2=component(Z,2);
P=y^2-Mod(m,p^n); Y=Mod(y,P); x=Y;
A1=eval(U1); A2= eval(U2); B1= eval(Pi1); B2= eval(Pi2);
```

```
b1= eval(pi1); b2= eval(pi2); e=eval(E);
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^n0; ze=znorder(ne)/p^n0;
if(zpi+ze <1, print("PROBLEME-NORMIQUE"));
if(delta!=0, print("PROBLEME-CLASSES")); print(zpi," ",ze); x=y)))}
```

Donnons l'extrait suivant pour $30007 \leq m \leq 30097$, $m \equiv 1 \pmod 3$, et $p = 3$ (la dernière colonne donne la structure du 3-groupe des classes du premier étage k_1 de la $\mathbb{Z}_3$-extension cyclotomique de k) :

m	h	z_π	z_ε	$\mathcal{C}\ell_{k_1}$	m	h	z_π	z_ε	$\mathcal{C}\ell_{k_1}$
30001	1	1	1	1	30055	2	1/27	1/27	$\mathbb{Z}/3\mathbb{Z}$
30007	2	1/9	1/3	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	30058	4	1	1	1
30010	8	1	1	1	30061	1	1	1	1
30013	1	1/3	1	1	30067	2	1	1	1
30019	4	1	1/3	$\mathbb{Z}/3\mathbb{Z}$	30070	4	1	1/3	$\mathbb{Z}/3\mathbb{Z}$
30022	4	1/3	1	1	30073	4	1	1/27	$\mathbb{Z}/3\mathbb{Z}$
30031	2	1/3	1/3	$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	30079	2	1	1	1
30034	2	1	1	1	30085	2	1/3	1	1
30043	18	1	1	$\mathbb{Z}/9\mathbb{Z}$	30091	1	1	1	1
30046	2	1	1	1	30094	8	1	1/3	$\mathbb{Z}/3\mathbb{Z}$
30049	1	1	1/3	$\mathbb{Z}/3\mathbb{Z}$	30097	1	1	1	1

Si le nombre de classes est divisible par p, il faut vérifier si le p-groupe des classes de k est engendré par les idéaux premiers au-dessus de p, sinon la conclusion n'est pas valable. Pour cela le programme retient l'ordre h_0 de la classe de $\mathfrak{p}_1$ pour lequel $\mathfrak{p}_1^{h_0} = (\pi_1)$; si les valuations p-adiques de h_0 et du nombre de classes h sont égales, ceci veut dire que $\mathcal{C}\ell_k$ est cyclique et engendré par la p-classe de $\mathfrak{p}_1$. Par exemple, dans le cas de $m = 30043$ où $h = 18$, la S_k-unité génératrice est $317 + 2\sqrt{m}$, de norme 3^9, et par conséquent la classe de $\mathfrak{p}_1$, d'ordre $h_0 = 9$, est génératrice de $\mathcal{C}\ell_k$.

Selon le choix par PARI d'une S_k-unité fondamentale modulo E_k, la valeur de z_π n'est pas intrinsèque, mais le test normique est invariant.

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

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

```
{for(j=2, 100, C1=0; C2=0; m=1; p=prime(j); n0=1; n=n0+1;
while(m<10^4, m=m+1; if(core(m)==m & kronecker(m,p)==1, C1=C1+1;
y=x; Q=x^2-m; K=bnfinit(Q,1); M=m; t=Mod(m,4); if(t!=1,M=4*m);
E=quadunit(M); h=qfbclassno(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^n; Pi2=pi2^n; Z=bezout(Pi1, Pi2);
U1=component(Z,1); U2=component(Z,2); P=y^2-Mod(m,p^n);
Y=Mod(y,P); x=Y; A1=eval(U1); A2=eval(U2);
B1=eval(Pi1); B2=eval(Pi2); b1=eval(pi1); b2=eval(pi2);
e=eval(E); 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^n0; ze=znorder(ne)/p^n0;
if(zpi+ze>1&delta==0, C2=C2+1); x=y)); print(p," ",C1," ",C2," ",C1-C2))}
```

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

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

Dans **[50]** il y a deux exemples plus délicats (pour $p = 3$) :

(i) $m = 2659$, $h = 3$, $\varepsilon = 63190881\sqrt{m} + 3258468890$, $\pi_1 = -2\sqrt{m} + 103$ qui dans notre table est indiqué avec $z_\pi = \frac{1}{3}$ et $z_\varepsilon = \frac{1}{3^2}$ ($\mathcal{C}\ell_k$ est engendré par S_k). Il faut alors d'autres calculs explicites dans la tour pour démontrer que $\lambda_3 = \mu_3 = 0$ (cf. **[11]**, **[10]**, **[27]**, **[28]** utilisant soit le "Spiegelungssatz" dans $k(j)$ ($j^3 = 1,\ j \neq 1$), soit les unités cyclotomiques).

(ii) $m = 12007$, $h = 3$, $\varepsilon = 65199591367431507\sqrt{m} + 7144340241111277688$, $\pi_1 = 429331\sqrt{m} + 47044570$, avec $z_\pi = \frac{1}{3^6}$ et $z_\varepsilon = \frac{1}{3^2}$ ($\mathcal{C}\ell_k$ est engendré par S_k). Dans ce cas, la vérification utilise les fonctions L p-adiques, de nombreux arguments et aussi **[27]**, **[28]**.

Voir d'autres raisonnements dans **[2]**, **[5]**, **[8]**, **[10]**, **[11]**, **[12]**, **[26]**, **[37]** (cas $p = 3$ non décomposé), **[38]**, **[43]** (cas $p = 2$), **[51]**, **[52]** (pour des corps cubiques totalement réels et $p = 3$), et bien d'autres.

Pour une table assez complète ($p = 3, 5, 7, 11, 13, 17, 19, 23, 29$), prière de se connecter à :

https://www.dropbox.com/s/tcqfp41plzl3u60/R

Il y a identité des valeurs de $\delta_{\mathfrak{p}_1}(\pi_2)$ et $\delta_p(\varepsilon)$, pour $p = 3$, avec celles de la table de **[11]**.

Le programme suivant calcule la structure des groupes des classes de k et de k_1 pour $p = 3$ et $b \leq m \leq B$, $m \equiv 1 \pmod 3$:

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

Ce qui donne les quelques exemples suivants avec $\mathcal{C}\ell_{k_1} \neq 1$ (sous la forme $[\#\mathcal{C}\ell_{k_1}, [\text{structure}]]$) :

m	$\mathcal{C}\ell_k$	$\mathcal{C}\ell_{k_1}$	m	$\mathcal{C}\ell_k$	$\mathcal{C}\ell_{k_1}$
1000003	[3, [3]]	[27, [3, 3, 3]]	1000126	[2, [2]]	[24, [6, 2, 2]]
1000018	[4, [4]]	[12, [12]]	1000135	[4, [2, 2]]	[12, [6, 2]]
1000042	[36, [18, 2]]	[36, [18, 2]]	1000147	[30, [30]]	[90, [30, 3]]
1000051	[4, [2, 2]]	[12, [6, 2]]	1000159	[1]	[3, [3]]
1000093	[12, [6, 2]]	[48, [6, 2, 2, 2]]	1000177	[1]	[12, [6, 2]]
1000099	[1]	[3, [3]]	1000189	[1]	[9, [3, 3]]
1000102	[2, [2]]	[18, [6, 3]]	1000198	[12, [12]]	[36, [36]]
(.....)					
100000006	[12, [12]]	[36, [36]]	100000027	[6, [6]]	[72, [18, 2, 2]]

6. Filtration des $\mathcal{C}\ell_{k_n}$ – Groupes de nombres Λ_i^n

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

Dans cette section nous reprenons l'analyse de la conjecture de Greenberg sous la forme directe du "calcul" du p-groupe des classes de k_n selon l'algorithme défini dans **[17]**, et en utilisant des idéaux étrangers à p pour représenter les classes.

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

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

Remarques 6.1. — *(i) Pour $i = 0$, on obtient $M_1^n = (M^n)^{G_n}$.*
(ii) On a $M_{i+1}^n = \{c \in M^n,\ c^{1-\sigma_n} \in M_i^n\}$; ainsi :

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

(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 $1 - \sigma_n$.

Ensuite, pour les sous-G_n-modules $M_i^n =: \mathcal{A}_{k_n}(\mathcal{I}_i^n)$ de M^n (où l'on peut toujours supposer que $\mathcal{I}_i^n \subseteq \mathcal{I}_{i+1}^n$), on a la formule générale du Théorème 3.1 qui devient dans notre cas particulier :

$$\#\big(M_{i+1}^n/M_i^n\big) = \frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} \cdot \frac{p^{n\cdot(d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))}, \tag{6.1}$$

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

$$\#M^n = \prod_{i=0}^{m_n-1} \#\big(M_{i+1}^n/M_i^n\big). \tag{6.2}$$

Pour n fixé, les M_i^n et $\mathrm{N}_{k_n/k}(M_i^n)$ définissent des i-suites *croissantes* de sous-groupes de $\mathcal{C}\ell_{k_n}$ et $\mathcal{C}\ell_k$ respectivement. On obtient que les i-suites d'entiers $(i \geq 0)$:

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

sont respectivement des i-suites *décroissantes vers* 1 de diviseurs de $\#\mathcal{C}\ell_k$ et de R_k (Théorème 4.3 (iii)), en raison, pour la seconde, des injections :

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

les $\#\big(M_{i+1}^n/M_i^n\big)$ divisant $\#\mathcal{T}_k = \#\mathcal{C}\ell_k \cdot R_k$ et décroissant vers 1. Donc on a au rang final $i = m_n$, en utilisant ce qui précède pour $M_{m_n}^n = \mathcal{C}\ell_{k_n}$, les relations $\mathrm{N}_{k_n/k}\big(M_{m_n}^n\big) = \mathcal{C}\ell_k$ et $(\Lambda_{m_n}^n : \Lambda_{m_n}^n \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(d-1)}$, ce qui explique que $\#\mathcal{C}\ell_{k_n}$ dépend essentiellement du nombre de pas m_n :

Théorème 6.1. — *Soit k Galoisien réel dans lequel $p > 2$ est totalement décomposé et vérifie la conjecture de Leopoldt. Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale de k (cf. § 4.3).*
Soit $N_{\mathrm{Iw}} \geq 0$ tel que la formule d'Iwasawa $\#\mathcal{C}\ell_{k_n} = p^{\lambda\cdot n+\mu\cdot p^n+\nu}$ soit valable pour tout $n \geq N_{\mathrm{Iw}}$.

(i) On a les inégalités $m_n \leq \lambda\cdot n+\mu\cdot p^n+\nu \leq v_p(\#\mathcal{T}_k)\cdot m_n$ pour tout $n \geq N_{\mathrm{Iw}}$, où v_p désigne la valuation p-adique. Si $\mathcal{T}_k = 1$, alors $\lambda = \mu = \nu = 0$.

(ii) Si $\mathcal{T}_k \neq 1$, alors $m_n = c(n)\cdot(\lambda\cdot n+\mu\cdot p^n+\nu)$, $\frac{1}{v_p(\#\mathcal{T}_k)} \leq c(n) \leq 1$, avec en particulier l'inégalité principale sur le nombre de pas m_n de l'algorithme :

$$m_n \geq \frac{1}{v_p(\#\mathcal{T}_k)}\big(\lambda\cdot n+\mu\cdot p^n+\nu\big), \text{ pour tout } n \geq N_{\mathrm{Iw}}.$$

Démonstration. — Comme $\#\big(M_{i+1}^n/M_i^n\big) \geq p$ pour $0 \leq i \leq m_n-1$, on obtient $\#\mathcal{C}\ell_{k_n} = \#M^n \geq p^{m_n}$ en utilisant l'expression (6.2) ; on en déduit l'inégalité triviale $m_n \leq \lambda\cdot n+\mu\cdot p^n+\nu$. Ensuite, d'après le fait que $\#\big(M_{i+1}^n/M_i^n\big) \mid \#\mathcal{T}_k$, on a $\#\big(M_{i+1}^n/M_i^n\big) \leq \#\mathcal{T}_k$ pour $0 \leq i \leq m_n-1$; d'où $\#\mathcal{C}\ell_{k_n} \leq (\#\mathcal{T}_k)^{m_n}$ à nouveau par (6.2), ce qui achève la démonstration. □

Remarque 6.1. — *Une heuristique raisonnable est que m_n reste, pour tout n, d'une valeur moyenne fonction de $\mathrm{Gal}(k/\mathbb{Q})$ et de $\mathcal{T}_k$ et non de n. Or, pour tout $n \gg 0$, les $\#\big(M_{i+1}^n/M_i^n\big)$ forment, à partir de $\#M_1^n$, une i-suite décroissante vers 1 d'entiers divisant $\#\mathcal{T}_k$; une telle suite ne peut avoir, pour λ ou μ non nuls, au moins $\frac{1}{v_p(\#\mathcal{T}_k)}(\lambda\cdot n+\mu\cdot p^n+\nu)$ termes non triviaux sauf à établir un lien de type particulier avec les normes d'idéaux $\mathfrak{A}_i \in \mathcal{I}_i^n$ utilisés dans la tour, ce qui philosophiquement semble exclu, à notre avis, car ceci implique l'existence, pour $n \to \infty$, d'au moins un diviseur $t_n \neq 1$ de $\#\mathcal{T}_k$ tel que $\#\big(M_{i+1}^n/M_i^n\big) = t_n$ pour $O(1)\cdot(\lambda\cdot n+\mu\cdot p^n+\nu)$ valeurs consécutives de $i \in [1, m_n]$.*
En faisant l'hypothèse très faible que la probabilité de $\#\big(M_{i+1}^n/M_i^n\big) \geq p$ pour $m_n = O(n)$ pas consécutifs de l'algorithme est de la forme $\dfrac{1}{p^{f(n)}}$, où $f(n) \to \infty$ avec n, on peut admettre, sur un plan heuristique assez évident, qu'à partir d'un certain $n \gg N_{\mathrm{Iw}}$, ceci n'est plus vraisemblable, auquel cas c'est l'existence

même de la formule d'Iwasawa qui suggère la nullité de λ et μ et l'existence de i_0 assez grand tel que $\#\big(M_{i_0+1}^n/M_{i_0}^n\big) = 1$ pour tout $n \gg 0$ (i.e., $m_n \leq i_0$ pour tout n). Nous approfondirons cet aspect, concernant l'existence de i_0, en examinant séparément les deux facteurs :

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

qui ne sont pas de la même nature, et en énonçant les Heuristiques 7.1 et 7.2, puis nous donnerons des justifications probabilistes très naturelles (§ 7.4.2) et des statistiques numériques (Section 8).

A cet effet, rappelons l'algorithme numérique qui permet de passer de Λ_i^n à Λ_{i+1}^n, et qui détermine le nombre de pas m_n, pour analyser les phénomènes en jeu, car dès qu'un $x \in \Lambda_{i+1}^n$ se rajoute aux éléments de Λ_i^n, ses $\delta_{\mathfrak{p}}(x)$, $\mathfrak{p} \mid p$, ont une grande probabilité d'être nuls ou au moins inférieurs aux précédents, ce qui donne la i-suite des $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_i^n \ : \ \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ rapidement décroissante vers 1.

6.2. Algorithme de calcul des Λ_i^n. — On omet l'indice n qui est fixé et on se place dans l'extension $K \subset k_\infty$ de degré p^n et de groupe de Galois $G =: \langle\sigma\rangle$ d'ordre p^n. On désigne pour simplifier par N la norme arithmétique $\mathrm{N}_{K/k}$ et on pose $M := \mathcal{C}\ell_K$.

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

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

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

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

Ceci suppose que l'on a résolu suffisamment d'équations normes pour engendrer M_1. Par exemple, le cas $x_0 = y_1 = 1$ conduit normalement à inclure dans $\mathcal{I}_1$ des idéaux ambiges représentant les classes de k et les idéaux $\mathfrak{P}$ de K au-dessus de p ; en effet, $\mathfrak{A}_1$ est défini à un idéal invariant près, ce qui peut changer la classe car $\mathfrak{A}_1$ peut être principal et non $\mathfrak{A}_1 \cdot \mathfrak{P}$; mais on peut toujours représenter la classe de $\mathfrak{P}$ par un idéal $\mathfrak{A}'$ de K étranger à p. On obtient $\mathrm{N}(M_1)$ comme sous-groupe de $\mathcal{C}\ell_k$, à partir de $\mathrm{N}(\mathcal{I}_1) = \langle \mathrm{N}(\mathfrak{A}_1^1), \ldots, \mathrm{N}(\mathfrak{A}_1^{r_1}) \rangle$; alors il vient $\Lambda_1 = \{x_1 \in k^\times,\ (x_1) \in \mathrm{N}(\mathcal{I}_1)\}$ et, toujours au niveau n fixé :

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

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

(ii) Pour le calcul de $\mathcal{I}_2$, on considère les éléments x_1 de Λ_1 qui sont normes d'un $y_2 \in K^\times$ (de fait on se limite aux x_1 représentant $\Lambda_1 \cap \mathrm{N}(K^\times)$ modulo $E_k \cap \mathrm{N}(K^\times)$) ; alors $(x_1) = \mathrm{N}(y_2) = \mathrm{N}(\mathfrak{B}_1)$, $\mathfrak{B}_1 \in \mathcal{I}_1$, donc il existe $\mathfrak{A}_2 \in I_K$ tel que $\mathfrak{A}_2^{1-\sigma} \cdot \mathfrak{B}_1 = (y_2)$, avec $\mathfrak{A}_2$ choisi étranger à p. On a $\mathscr{C}\ell_K(\mathfrak{A}_2)^{1-\sigma} \in M_1$. Inversement, si $\mathscr{C}\ell_K(\mathfrak{A}'_2) \in M_2$, $\mathfrak{A}'_2$ étranger à p, il existe $y'_2 \in K^\times$ tel que $\mathfrak{A}'^{1-\sigma}_2 \cdot \mathfrak{B}'_1 = (y'_2)$, avec $\mathfrak{B}'_1 \in \mathcal{I}_1$, d'où $\mathrm{N}(\mathfrak{B}'_1) = \mathrm{N}(y'_2) =: (x'_1)$, $x'_1 \in \Lambda_1 \cap \mathrm{N}(K^\times)$.

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

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

d'où $\mathrm{N}(\mathcal{I}_2)$ et $\Lambda_2 = \{x_2 \in k^\times, \ (x_2) \in \mathrm{N}(\mathcal{I}_2)\}$, etc. On obtient donc des groupes Λ_i, étrangers à p, uniques modulo $\mathrm{N}(K^\times)$, tels que :

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

On suppose implicitement que chaque $\mathcal{I}_i$ est formé d'idéaux étrangers à p. Dans le cas $\mathcal{C}\ell_k = 1$, les groupes Λ_i sont engendrés par les unités $\varepsilon \in E_k$ et les α_i^j générateurs des $\mathrm{N}(\mathfrak{A}_i^j)$, ce qui simplifie l'expression de Λ_i.

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

Une heuristique classique est que, pour $\mathfrak{p}$ fixé, les $\delta_\mathfrak{p}(x)$, $x \in k^\times$, sont aléatoires et indépendants. Cependant, il est nécessaire de préciser cet aspect pour le cas des idéaux $\mathfrak{A}_i$ de K constituant les groupes $\mathcal{I}_i$ pour lesquels $\mathrm{N}_{K/k}(\mathcal{I}_i)$ conduit aux nombres x_i. Nous montrerons au § 7.4.2 et dans la Section 8 ce qu'il en est au plan probabiliste en utilisant des programmes établissant des statistiques très convaincantes, tenant compte de la formule du produit.

Auparavant, examinons de façon plus numérique un cas non trivial, mais le plus simple possible, en supposant la conjecture fausse.

6.3. La i-suite des Λ_i^n sous les hypothèses $\mathcal{C}\ell_k = 1$ & $\lambda \geq 1$. — Pour fixer les idées, supposons que k est un corps quadratique réel, que $p > 2$ est décomposé, que $\mathcal{C}\ell_k = 1$, que $\delta_p(\varepsilon) \geq 1$, et que (en posant pour simplifier $\mathfrak{p}_1 =: \mathfrak{p}$ et $\pi_2 =: \pi$) on a $\delta_\mathfrak{p}(\pi) \geq 1$ (cf. Section 5).

Par exemple, $m = 103$, $\varepsilon = 22419\sqrt{103} + 227528$, $\pi = \sqrt{103} + 10$, pour lesquels k est principal, $\delta_p(\varepsilon) = 1$ et $\delta_\mathfrak{p}(\pi) = 1$; ainsi la condition suffisante du Théorème 3.2 n'est pas vérifiée. On a donc $\#\mathcal{T}_k = R_k = p$ et la relation de divisibilité du Théorème 4.2 (i) pour tout n.

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

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

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

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

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

$$\#(M_2/M_1) = \frac{p^n}{(\Lambda_1 : \Lambda_1 \cap \mathrm{N}_{K/k}(K^\times))} = 1 \text{ ou } p, \quad \text{avec } \Lambda_1 = \langle \varepsilon, \alpha_1\rangle.$$

Puisque $\delta_p(\varepsilon) = 1$, l'algorithme ne peut se terminer par $M = M_1$ que si $\delta_p(\alpha_1)$ est nul ; sinon l'algorithme se poursuit, et en supposant $\delta_p(\alpha_1) \geq 1$, il faut prendre un élément convenable de Λ_1, de la forme $\alpha_1^u \cdot \varepsilon^v$, $u, v \in \mathbb{Z}$, comme norme de y_2 dans K/k et on obtient, puisque $\mathrm{N}_{K/k}(\mathfrak{A}_1) = (\alpha_1)$, une relation de la forme $\mathfrak{A}_2^{1-\sigma}\,\mathfrak{A}_1^u = (y_2)$ dans K pour définir $\mathcal{I}_2$.

Mais M_2/M_1 est annulé par p, et en supposant $M_2 \neq M_1$, on aura $\mathfrak{A}_2^p = \mathfrak{A}_1^w \cdot (z_2)$, $w \in \mathbb{Z}$, $z_2 \in K^\times$, d'où $\mathrm{N}_{K/k}(\mathfrak{A}_2^p) = (\alpha_1^w)\,\mathrm{N}_{K/k}(z_2)$ qui conduit, en posant $(\alpha_2) = \mathrm{N}_{K/k}(\mathfrak{A}_2)$, à $\omega(\alpha_2)^p = \omega(\alpha_1^w \cdot \eta_2)$ pour une unité η_2 de k ; or $\omega(\alpha_1)$ et $\omega(\eta_2)$ sont dans $\Omega(K/k)^p$. Comme précédemment, $\omega(\alpha_2)$ n'est soumis a priori à aucune obstruction pour conduire éventuellement à $\delta_p(\alpha_2) = 0$.

L'algorithme pour K se poursuit avec des calculs analogues et on obtient :

$$\omega(\alpha_1^p) \in \omega(\Lambda_0),\ \omega(\alpha_2^p) \in \omega(\Lambda_1), \ldots,\ \omega(\alpha_{i+1}^p) \in \omega(\Lambda_i), \ldots \tag{6.3}$$

où $\Lambda_i = \langle \varepsilon, \alpha_1, \ldots, \alpha_i\rangle$ et où les $\#\omega(\Lambda_i) = (\Lambda_i : \Lambda_i \cap \mathrm{N}_{K/k}(K^\times))$ forment une i-suite croissante minorée par p^{n-1} puisque $\#(M_{i+1}/M_i) = \dfrac{p^n}{\#\omega(\Lambda_i)} = p$ pour $0 \leq i \leq m_n - 1$, donc stationnaire à la valeur p^{n-1} dès l'indice 0 ; les relations $\omega(\alpha_{i+1}^p) \in \omega(\Lambda_i)$ permettent, statistiquement, une "décroissance" des $\delta_p(\alpha_i)$, ce qui semble contradictoire avec un nombre de pas $m_n \geq n + \nu$ découlant de l'hypothèse $\lambda = 1$, $v_p(\#\mathcal{T}_k) = 1$ (cf. Théorème 6.1).

Une autre façon d'aborder ces questions heuristiques est la suivante (avec les mêmes hypothèses que ci-dessus) :

Représentons la classe de $\mathfrak{A}$ dans K par un idéal premier $\mathfrak{L}$ de K ; on a $\mathrm{N}_{K/k}(\mathfrak{L}) = \mathfrak{l}^{f^n} =: (\beta)^{f^n} =: (\alpha)$ où $\mathfrak{l} = (\beta)$ est l'idéal premier de k en-dessous de $\mathfrak{L}$ et f^n son degré résiduel dans K/k (autrement dit, $\alpha = \beta^{f^n} \cdot \eta$, $\eta \in E_k$). Or la condition normique $\delta_{\mathfrak{p}}(\alpha) = 0$ ne peut avoir lieu que si $f^n = 1$ (i.e., $\mathfrak{l}$ totalement décomposé dans K/k), puisque $\delta_{\mathfrak{p}}(\eta) \geq 1$ par hypothèse sur $\delta_{\mathfrak{p}}(\varepsilon)$; ainsi $\delta_{\mathfrak{p}}(\alpha) = 0$ implique, pour ℓ en-dessous de $\mathfrak{l}$, $l^{p-1} \equiv 1 \pmod{p^{n+1}}$. Mais on montrera au § 8.1 au moyen du théorème de Tchebotarev qu'une classe de k_n est toujours (donc *nécessairement*) représentable par un $\mathfrak{L}$ totalement décomposé dans K/k.

On a donc, sous l'hypothèse $\#\mathcal{T}_k = R_k = p$ & $\lambda = 1$, $\#(M_{i+1}/M_i) = p$ pour $O(n)$ pas, alors que l'on peut conjecturer que $M = M_{O(1)}$ pour $n \to \infty$.

Le troisième programme du § 5.2, donne pour $m = 103$:

$$\mathcal{C}\ell_{k_1} \simeq \mathbb{Z}/3\,\mathbb{Z} \oplus \mathbb{Z}/3\,\mathbb{Z} \text{ (i.e., } M_2 \neq M_1 \text{ au premier étage).}$$

Le S_{k_1}-groupe des classes de k_1 est d'ordre 3, ce qui donne $\#\mathcal{C}\ell_{k_1}(S_{k_1}) = 3$, et le point (iii) du Théorème 4.2 pour $n_0 = e = 1$ conduit à $\lambda = \mu = 0$; pour ce calcul, rajouter au programme :

```
L=bnfinit(R,1); Su=bnfsunit(L,idealprimedec(L,p));
print(component(component(Su,5),1))
```

Par des méthodes de type "Spiegelungssatz" on montre aussi que $\lambda = 0$ (cf. **[3]**, **[5]**, **[11]**). On peut vérifier que $\mathcal{C}\ell_{k_2} \simeq \mathcal{C}\ell_{k_3} \simeq \mathbb{Z}/3\,\mathbb{Z} \oplus \mathbb{Z}/3\,\mathbb{Z}$.

La section suivante est l'étude, à i fixé, de la n-suite $\#M_i^n$.

7. Heuristiques sur les filtrations dans k_∞/k

Ici, contrairement aux études précédentes, on fixe l'étape i des algorithmes et on considère les n-suites des groupes $M_i^n := \mathcal{C}\ell_{k_n}(\mathcal{I}_i^n)$ et Λ_i^n. On étudie alors les entiers $\#\big(M_{i+1}^n/M_i^n\big)$ pour $i \geq 0$ fixé et $n \to \infty$ à partir de leurs deux facteurs donnés par la Formule (6.1).

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

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

On a $\mathrm{N}_{k_{n+1}/k_n}(M_i^{n+1}) \subseteq M_i^n$; donc, pour tout idéal $\mathfrak{A}^{n+1} \in \mathcal{I}_i^{n+1}$, on peut écrire $\mathrm{N}_{k_{n+1}/k_n}(\mathfrak{A}^{n+1}) = (\alpha^n)\,\mathfrak{A}^n$, où $\alpha^n \in k_n^\times$ et $\mathfrak{A}^n \in \mathcal{I}_i^n$, auquel cas, *en modifiant* $\mathcal{I}_i^n$ modulo des idéaux principaux de k_n, on peut supposer $\mathrm{N}_{k_{n+1}/k_n}(\mathcal{I}_i^{n+1}) \subseteq \mathcal{I}_i^n$ et par conséquent $\mathrm{N}_{k_{n+1}/k}(\mathcal{I}_i^{n+1}) \subseteq \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)$; ceci revient à modifier $\Lambda_i^n = \{x \in k^\times, (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)\}$ modulo des normes d'éléments de $k_n^\times$ ce qui laisse invariant $(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))$. On peut alors supposer que, pour tout $h \geq 1$, on a :

$$E_k \subseteq \Lambda_i^{n+h} \subseteq \cdots \subseteq \Lambda_i^{n+1} \subseteq \Lambda_i^n. \tag{7.1}$$

Lemme 7.1. — *Pour tout $i \geq 0$ fixé, les $\#\big(M_{i+1}^n/M_i^n\big)$ forment une n-suite croissante stationnaire de diviseurs de $\#\mathcal{T}_k$, et les $\#M_i^n$ définissent une n-suite croissante stationnaire d'entiers.*

Démonstration. — Considérons pour $i \geq 0$ fixé la n-suite définie par :

$$\#\big(M_{i+1}^n/M_i^n\big) = \frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} \cdot \frac{p^{n\cdot(d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))}. \tag{7.2}$$

Comme $\mathrm{N}_{k_{n+1}/k}(M_i^{n+1}) \subseteq \mathrm{N}_{k_n/k}(M_i^n)$, la n-suite $\dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} =: p^{c_i^n}$ est *croissante* stationnaire à une valeur maximale notée $p^{c_i^\infty} \mid \#\mathcal{C}\ell_k$.

Le second facteur $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))} = \dfrac{p^{n\cdot(d-1)}}{\#\omega_n(\Lambda_i^n)} =: p^{\rho_i^n}$ définit une n-suite *croissante* d'entiers. En effet, on a $p^{\rho_i^{n+1}-\rho_i^n} = p^{d-1}.\dfrac{\#\omega_n(\Lambda_i^n)}{\#\omega_{n+1}(\Lambda_i^{n+1})}$, et comme on peut supposer que l'on a $\Lambda_i^{n+1} \subseteq \Lambda_i^n$ (cf. Relation (7.1)), alors $\#\omega_{n+1}(\Lambda_i^{n+1}) \leq \#\omega_{n+1}(\Lambda_i^n)$ puis $p^{\rho_i^{n+1}-\rho_i^n} \geq p^{d-1}.\dfrac{\#\omega_n(\Lambda_i^n)}{\#\omega_{n+1}(\Lambda_i^n)}$; dans la restriction des symboles de Hasse $\Omega(k_{n+1}/k) \twoheadrightarrow \Omega(k_n/k)$ (dont le noyau est d'ordre p^{d-1}), l'image de $\omega_{n+1}(\Lambda_i^n)$ est $\omega_n(\Lambda_i^n)$, d'où le résultat pour la n-suite $p^{\rho_i^n}$, stationnaire à une

valeur maximale $p^{\rho_i^\infty} \mid R_k$ (Théorèmes 4.2, 4.4), et au total le premier point du lemme en résulte pour la n-suite $\#\big(M_{i+1}^n/M_i^n\big)$; on a $\lim\limits_{n\to\infty} \#\big(M_{i+1}^n/M_i^n\big) = p^{c_i^\infty} \cdot p^{\rho_i^\infty} \mid \#\mathcal{T}_k$.
Enfin, si l'on suppose, par récurrence, que la n-suite $\#M_i^n$ est croissante stationnaire, la propriété en résulte pour la n-suite $\#M_{i+1}^n$. □

Lemme 7.2. — *Les i-suites $p^{c_i^\infty}$, $p^{\rho_i^\infty}$, et $\lim\limits_{n\to\infty} \#(M_{i+1}^n/M_i^n) = p^{c_i^\infty} \cdot p^{\rho_i^\infty}$ sont décroissantes stationnaires, respectivement vers un diviseur de $\#\mathcal{C}\ell_k$, R_k, et $\#\mathcal{T}_k$.*

Démonstration. — Provient facilement de l'expression des deux facteurs de (7.2) pour n pris assez grand (voir aussi la Remarque 6.1 (iii)). □

Corollaire 7.1. — *Il existe $i_{\min} \geq 0$ et des constantes $c \geq 0$ et $\rho \geq 0$ telles que $c_i^\infty = c$ et $\rho_i^\infty = \rho$ pour tout $i \geq i_{\min}$.*

Mais la i-suite $p^{c_i^\infty} \cdot p^{\rho_i^\infty}$ n'est pas nécessairement de limite 1 ; en effet, on a seulement que $\lim\limits_{i\to\infty} \big(p^{c_i^\infty} \cdot p^{\rho_i^\infty}\big) = p^{c+\rho}$ divise $\#\mathcal{T}_k$ et il convient d'examiner chacun des deux facteurs. Auparavant, donnons la définition suivante :

Définition 7.1. — *On dira que le processus limite sur i est fini (ce qui équivaut à $\lambda = \mu = 0$) s'il existe $i_0 \in \mathbb{N}$ tel que $p^{c_{i_0}^\infty} \cdot p^{\rho_{i_0}^\infty} = 1$.*

Dans ce cas on a donc $i_0 = i_{\min}$, $c = \rho = 0$, et pour tout $n \gg 0$, $\#M^n$ est une constante notée p^ν, indépendante de n.

7.2. Comportement heuristique de $\omega_n(\Lambda_i^n) \subseteq \Omega(k_n/k)$, $n \to \infty$. — Le processus limite sur i peut être infini (i.e., $p^{\rho_i^\infty} \neq 1$ $\forall i \geq 0$, ou encore $\rho > 0$) si pour tout i il existe $n \gg 0$ tel que $\omega_n(\Lambda_i^n) \subset \Omega(k_n/k)$ ou encore $(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times)) < p^{n\cdot(d-1)}$. Il existerait $n_1 \gg 0$ tel que pour $n \geq n_1$, $\dfrac{p^{n\cdot(d-1)}}{\omega_n(\Lambda_i^n)} = p^\rho \neq 1$, pour $i_{\min} \leq i \leq m_n - 1$ (Corollaire 7.1). Ceci signifie que sous l'hypothèse $\lambda \geq 1$ ou $\mu \geq 1$, l'algorithme au niveau n devrait comporter $m_n = O(\lambda\cdot n + \mu\cdot p^n)$ "i-étapes" successives (cf. Théorème 6.1), avec $\omega_n(\Lambda_i^n) \subset \Omega(k_n/k)$, et ceci pour n arbitrairement grand. Par conséquent la finitude du processus limite dans ce cas ne peut provenir que de l'heuristique suivante, en raison des propriétés des quotients de Fermat (nous y reviendrons au § 7.4.2 au moyen d'une justification globale) :

Conjecture 7.1. — *On considère les groupes Λ_i^n associés à l'ensemble des algorithmes de détermination des sous-groupes M_i^n, $0 \leq i \leq m_n$, des filtrations des $M^n := \mathcal{C}\ell_{k_n}$, $n \geq 0$. Alors il existe i_1 assez grand, indépendant de n, tel que $\dfrac{p^{n\cdot(d-1)}}{(\Lambda_{i_1}^n : \Lambda_{i_1}^n \cap \mathrm{N}_{k_n/k}(k_n^\times))} = 1$ pour $n \to \infty$.*

7.3. Comportement heuristique de $\mathrm{N}_{k_n/k}(M_i^n) \subseteq \mathcal{C}\ell_k$, $n \to \infty$. — Lorsque $\mathcal{C}\ell_k \neq 1$, la non finitude du processus limite sur i peut provenir du fait que pour tout $i \in \mathbb{N}$ il existe $n \gg 0$ tel que $\mathrm{N}_{k_n/k}(M_i^n) \subset \mathcal{C}\ell_k$ (i.e., $p^{c_i^\infty} \neq 1$, ou encore $c > 0$). Comme pour l'Heuristique 7.1, il existerait $n_2 \gg 0$ tel que pour $n \geq n_2$, $\dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} = p^c \neq 1$, pour $i_{\min} \leq i \leq m_n - 1$, et une conclusion analogue sur le nombre d'étapes m_n.

Or on peut se baser sur l'heuristique naturelle suivante stipulant que les classes des idéaux de k de la forme $\mathrm{N}_{k_n/k}(\mathfrak{A})$ (ou $\mathrm{N}_{k_n/k}(\mathcal{L})$ avec $\mathcal{L}$ premier totalement décomposé dans k_n/k) sont aléatoires, indépendantes, et se répartissent dans le groupe fini $\mathcal{C}\ell_k$ selon les probabilités standard dans la mesure où $\mathrm{N}_{k_n/k}(\mathcal{C}\ell_{k_n}) = \mathcal{C}\ell_k$ (voir de même le § 7.4.2 pour des justifications précises à ce sujet) :

Conjecture 7.2. — *On considère les groupes $\mathrm{N}_{k_n/k}(M_i^n)$ associés à l'ensemble des algorithmes de calcul des sous-groupes M_i^n, $0 \leq i \leq m_n$, des filtrations des $M^n := \mathcal{C}\ell_{k_n}$, $n \geq 0$. Alors il existe i_2, assez grand, indépendant de n, tel que $\mathrm{N}_{k_n/k}(M_{i_2}^n) = \mathcal{C}\ell_k$ pour $n \to \infty$.*

Remarque 7.1. — *Dans le cas où p est non décomposé dans le corps totalement réel k et en supposant k_∞/k totalement ramifiée en l'unique $\mathfrak{p} \mid p$, le critère de Greenberg est que $\lambda = \mu = 0$ si et seulement si $\mathcal{C}\ell_k$ capitule dans un k_{n_0}* [**21**, Theorem 1] *(critère indépendant de la conjecture de Leopoldt). On a dans ce cas, pour tout $n \geq 0$ et tout i, $0 \leq i \leq m_n - 1$:*

$$\#(M_{i+1}^n/M_i^n) = \frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)},$$

le "facteur normique" étant trivial en raison de la formule du produit.

La i-suite des Λ_i^n (n fixé) est alors telle que tout $x_i \in \Lambda_i^n$ est de la forme $\mathrm{N}_{k_n/k}(y_i)$, $y_i \in k_n^\times$, et $(x_i) = \mathrm{N}_{k_n/k}(\mathfrak{B}_i)$ pour un idéal $\mathfrak{B}_i$ de $\mathcal{I}_i^n$ de sorte qu'il existe $\mathfrak{A}_{i+1}$ étranger à p de k_n tel que $\mathfrak{A}_{i+1}^{1-\sigma_n} \cdot (y_i) = \mathfrak{B}_i$; d'où $\mathrm{N}_{k_n/k}(\mathfrak{A}_{i+1})$ dont la classe dans $\mathrm{N}_{k_n/k}(M_{i+1}^n) \supseteq \mathrm{N}_{k_n/k}(M_i^n)$ assure la croissance de la i-suite $\#\mathrm{N}_{k_n/k}(M_i^n) \mid \#\mathcal{C}\ell_k$.

L'algorithme est donc identique et définit, pour chaque $n \gg 0$, la i-suite croissante des diviseurs $\#\mathrm{N}_{k_n/k}(M_i^n)$ de $\#\mathcal{C}\ell_k$ pour laquelle, sous l'hypothèse $\lambda \geq 1$ ou $\mu \geq 1$, l'algorithme devrait comporter un palier de $O(\lambda \cdot n + \mu \cdot p^n)$ "i-étapes" consécutives pour lesquelles $\mathrm{N}_{k_n/k}(M_i^n) \subset \mathcal{C}\ell_k$, ce qui est totalement irréaliste lorsque $n \to \infty$ comme expliqué au point précédent, ce qui sera analysé au § 7.4.2.

Ce premier cas de la conjecture de Greenberg est donc susceptible de l'Heuristique 7.2 précédente affirmant l'existence de i_2 assez grand tel que $\mathrm{N}_{k_n/k}(M_{i_2}^n) = \mathcal{C}\ell_k$ pour $n \to \infty$. Comme expliqué dans l'Introduction, le principe "algorithmique" adopté couvre grosso modo la totalité de la conjecture de Greenberg pour les corps totalement réels.

7.4. Principales propriétés p-adiques dans k_∞/k. — On a les propriétés locales et globales suivantes qui confortent l'absence d'obstruction dans les considérations et heuristiques probabilistes précédentes sur les propriétés normiques des nombres et idéaux dans k_∞/k ; le § 7.4.2 montrera, de façon essentielle, que l'analyse probabiliste dans la tour est de fait de "type fini" et ne concerne que l'invariant $\mathcal{T}_k$.

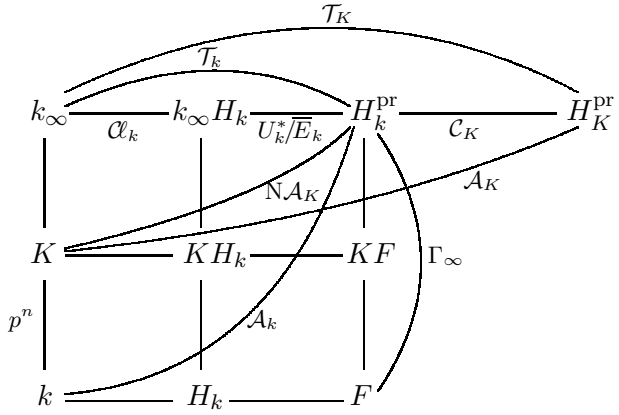
7.4.1. Propriétés locales dans k_∞/k. — On considère les d normes locales dans k_n/k, en les $\mathfrak{p} \mid p$, $n \geq 0$ fixé ; on désigne par $\mathfrak{p}_n$ l'idéal premier de k_n au-dessus de $\mathfrak{p}$. La proposition suivante est une formulation exclusivement locale des calculs de la Section 4 :

Proposition 7.1. — *Soit π_n (resp. π_{n+h}) une uniformisante du complété $\overline{k}_n$ de k_n en $\mathfrak{p}_n \mid p$ (resp. de celui de k_{n+h} en $\mathfrak{p}_{n+h} \mid p$).*

(i) Pour tout $h \geq 1$ et toute unité locale α_{n+h} de $\overline{k}_{n+h}$, il existe une unité locale α_n de $\overline{k}_n$ telle que l'on ait $\mathrm{N}_{\overline{k}_{n+h}/\overline{k}_n}(1+\alpha_{n+h}\cdot\pi_{n+h}) = 1+\alpha_n\cdot\pi_n$.
(ii) Pour tout $h \geq 1$, il existe une unité locale β_n de $\overline{k}_n$ telle que l'on ait $(1+\alpha_{n+h}\cdot\pi_{n+h})^{p^h} = 1+\beta_n\cdot\pi_n$.
(iii) Soient $U_{\mathfrak{p}_n}$ et $U_{\mathfrak{p}}$ les groupes d'unités locales principales de $\overline{k}_n$ et $\overline{k}$. Alors l'indice de $\mathrm{N}_{\overline{k}_n/\overline{k}}(U_{\mathfrak{p}_n})$ dans $U_{\mathfrak{p}}$ est égal à p^n.

Démonstration. — Utiliser [**46**, Ch. V, § 3, Lemme 5 & Ch. V, § 3, Lemme 4] pour le premier point. Le second est immédiat et le dernier est la théorie du corps de classes local dans l'extension totalement ramifiée $\overline{k}_n/\overline{k}$. □

7.4.2. Propriétés globales en p-ramification Abélienne dans k_∞/k. — On considère (sous la conjecture de Leopoldt pour p dans k_∞) le schéma suivant où l'on pose $K = k_n$ pour simplifier et où H_k^{pr} et H_K^{pr} sont les pro-p-extensions Abéliennes p-ramifiées maximales de k et K ; on désigne par F une extension de k, contenant le p-corps de classes de Hilbert H_k de k, telle que H_k^{pr} soit le composé direct de F et k_∞ sur k :



On considère les symboles d'Artin $\left(\frac{H_k^{\mathrm{pr}}/k}{\cdot}\right)$ et $\left(\frac{H_K^{\mathrm{pr}}/K}{\cdot}\right)$ sur $\mathcal{I}_k := I_k \otimes \mathbb{Z}_p$ et $\mathcal{I}_K := I_K \otimes \mathbb{Z}_p$, où I_k et I_K sont les groupes des idéaux étrangers à p de k et K. Leurs images sont respectivement les groupes de Galois $\mathcal{A}_k$ et $\mathcal{A}_K$; les noyaux de ces symboles d'Artin sont les groupes d'idéaux principaux infinitésimaux $\mathcal{P}_{k,\infty} \subset \mathcal{I}_k$ et $\mathcal{P}_{K,\infty} \subset \mathcal{I}_K$, où $\mathcal{P}_{k,\infty}$ est l'ensemble des idéaux (x_∞) où $x_\infty \in k^\times \otimes \mathbb{Z}_p$ est d'image triviale dans U_k, et de même avec K (cf. [**14**, Theorem III.2.4, Proposition III.2.4.1], [**31**, § 2]).

Les groupes $\mathcal{T}_k$ et $\mathcal{T}_K$ sont les groupes de torsion respectifs de $\mathcal{A}_k$ et $\mathcal{A}_K$.

L'application $\mathrm{N}_{K/k}$ sur $\mathcal{I}_K$ induit la restriction $\mathcal{A}_K \longrightarrow \mathcal{A}_k$ qui s'exprime par la suite exacte suivante, où $\Gamma_\infty = \mathrm{Gal}(H_k^{\mathrm{pr}}/F)$ et où $\mathrm{N}_{K/k}(\mathcal{A}_K)$ est d'indice p^n dans $\mathcal{A}_k$:

$$1 \longrightarrow \mathcal{C}_K \longrightarrow \mathcal{A}_K \longrightarrow \mathrm{N}_{K/k}(\mathcal{A}_K) = \Gamma_\infty^{p^n} \oplus \mathcal{T}_k \longrightarrow 1.$$

Il en résulte que si $\mathfrak{A} \in I_K$ (idéal ordinaire vu dans $\mathcal{I}_K$), $\mathrm{N}_{K/k}(\mathfrak{A})$ peut s'écrire, modulo des idéaux principaux infinitésimaux, sous la forme :

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

Pour $n \gg 0$, $\mathfrak{a}^{p^n}$ est p-principal de la forme (α), avec $\alpha \equiv 1 \pmod{p^{n'}}$ où $n' \to \infty$ avec n ; pour la détermination des $\delta_{\mathfrak{p}}(x)$ pour $x \in k^\times$ de la forme $(x) = \mathrm{N}_{K/k}(\mathfrak{A})$, on aura $(x) = (\alpha(x))\cdot\mathfrak{t}(x)$ où le nombre $\alpha(x)$ est "négligeable"

quant à ses $\delta_{\mathfrak{p}}(\alpha(x))$, et les $\delta_{\mathfrak{p}}(x)$ ne dépendront que de $\mathfrak{t}(x)$ modulo $\delta_{\mathfrak{p}}(E_k)$; on peut ainsi dire que les groupes $\mathrm{N}_{K/k}(\mathcal{I}_i^n)$ sont engendrés (modulo des (α) "quasi-infinitésimaux") par des $\mathfrak{t} \in \mathcal{T}_k$, et que les groupes Λ_i^n sont obtenus via les idéaux principaux (x) qui s'en déduisent.

Hypothèse 7.1. — *On suppose que les idéaux $\mathfrak{A}$ de $K = k_n$, obtenus par l'algorithme, définissent une variable aléatoire ainsi que la composante $\mathfrak{t}$ de $\mathrm{N}_{K/k}(\mathfrak{A})$ et que $\left(\frac{F/k}{\mathfrak{t}}\right)$ parcourt uniformément $\mathrm{Gal}(F/k) \simeq \mathcal{T}_k$.*

Ceci a les conséquences essentielles suivantes :

(i) La classe de $\mathfrak{t}$ parcourt uniformément $\mathcal{C}\ell_k$.

(ii) Lorsque $\mathfrak{t} = (x)$, puisque $\mathrm{Gal}(F/H_k) \simeq \mathrm{Gal}(H_k^{\mathrm{pr}}/k_\infty H_k) \simeq U_k^*/\overline{E}_k$ est d'exposant p^e, on a $x^{p^e} = x_\infty \cdot \varepsilon$, avec $\varepsilon \in E_k \otimes \mathbb{Z}_p$ et x_∞ infinitésimal (donc $\mathrm{N}_{k/\mathbb{Q}}(x) = 1$ dans $U_{\mathbb{Q}}$), et l'image de x est définie dans $U_k^*/\overline{E}_k$.

Ainsi les familles $\big(\delta_{\mathfrak{p}}(x)\big)_{\mathfrak{p}|p}$ modulo les $\big(\delta_{\mathfrak{p}}(\varepsilon)\big)_{\mathfrak{p}|p}$ parcourent un domaine représentatif effectif fini, ne dépendant que de E_k, et soumis aux probabilités habituelles sur les quotients de Fermat ; dans le cas quadratique, si $\delta_p(\varepsilon) = r \geq 1$, ce domaine est $[0, r[$ car si $\delta_p(x) \geq r$, $\delta_p(x \cdot E_k) = [r, \infty[$.

Si l'on revient aux i-suites des $\mathrm{N}_{K/k}(\mathcal{I}_i^n)$, représentant $\mathrm{N}_{K/k}(M_i^n)$, et aux groupes $\Lambda_i^n = \{x \in k^\times,\ (x) \in \mathrm{N}_{K/k}(\mathcal{I}_i^n)\}$, ce qui précède justifie à nouveau les Heuristiques 7.1, 7.2 et l'existence de $i_0 \geq \max(i_1, i_2)$, indépendant de n, assurant la finitude du processus limite (Définition 7.1) et conduisant à l'Heuristique probabiliste finale 7.3.

7.5. Conjecture de Greenberg faible. — Elle s'énonce (pour k réel, p-décomposé) sous la forme :

$$\text{“}\mathcal{cl}_{k_n}(S_{k_n}) = 1 \text{ pour tout } n \implies \lambda = \mu = 0\text{”}$$

(voir **[35]** pour différentes conditions équivalentes sous la conjecture de Gross-Kuzmin et **[40]**, **[41]** pour une preuve dans le cadre Abélien sous certaines hypothèses sur les unités cyclotomiques). Or le critère de Greenberg (Théorème 2.1) s'énonce :

$$\lambda = \mu = 0 \text{ si et seulement si } \mathcal{C}\ell_{k_n}^{G_n} = \mathcal{cl}_{k_n}(S_{k_n}) \text{ pour tout } n \gg 0.$$

d'où il résulte l'implication conjecturale qui serait à démontrer :

$$\mathcal{cl}_{k_n}(S_{k_n}) = 1 \text{ pour tout } n \implies \mathcal{C}\ell_{k_n}^{G_n} = 1 \text{ pour tout } n \gg 0.$$

Puisque $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{T}_k$ pour $n \geq e$ (Théorème 4.2 (ii)), ceci devient :

$$\mathcal{cl}_{k_n}(S_{k_n}) = 1 \text{ pour tout } n \implies k \text{ est } p\text{-rationnel (i.e., } \lambda = \mu = \nu = 0\text{)}.$$

Si l'on suppose k non p-rationnel (e.g., $p = 3$, $k = \mathbb{Q}(\sqrt{103})$ où $\mathcal{C}\ell_k = 1$ et $R_k = 3$), alors nécessairement $\mathcal{cl}_{k_n}(S_{k_n}) \neq 1$ pour tout $n \gg 0$.[(2)]

D'après la Remarque 3.2 (ii), on a $\mathrm{H}^1(G_n, \mathcal{cl}_{k_n}(S_{k_n})) = 0$ si et seulement si $\mathcal{C}\ell_{k_n}(S_{k_n}) = 1$, donc si et seulement si $\mathcal{C}\ell_{k_n}^{G_n} = \mathcal{C}\ell_{k_n}^{S_{k_n} G_n}$ (autrement dit, dans ce cas, la condition suffisante du Théorème 3.2 est aussi nécessaire).

Dans le cadre de l'algorithme déterminant, au niveau n, les i-suites M_i^n et Λ_i^n, la condition $\mathcal{cl}_{k_n}(S_{k_n}) = 1$ ne modifie en rien les aspects probabilistes du § 7.4.2 précédent, puisqu'on ne travaille qu'avec des idéaux étrangers à p pour représenter les classes de k_n, calculer leurs normes dans $\mathcal{C}\ell_k$ et les quotients de

[(2)] Noter que les $\mathcal{cl}_{k_{n+h}}(S_{k_{n+h}})$ se surjectent (par la norme) sur $\mathcal{cl}_{k_n}(S_{k_n})$, ce qui fait que si l'un des groupes est nul à un étage $n_0 \gg 0$, ils sont tous nuls pour $n \leq n_0$.

Fermat des $x \in \Lambda_i^n$; la conjecture faible ne semble pas être de nature différente de celle de la conjecture générale.

7.6. Heuristique finale. — Les Heuristiques 7.1, 7.2, et les arguments du § 7.4.2 se résumeraient par l'existence de i_0 assez grand, indépendant de n, tel que pour tout $n \gg 0$, $\mathcal{C}\ell_{k_n}$ soit atteint au i_0-ième pas au plus (i.e., $m_n \leq i_0$) ; ceci est alors équivalent à $\#\mathcal{C}\ell_{k_n} = p^\nu$ pour tout $n \gg 0$. Pour $0 \leq i \leq i_0$, on a donc une suite de diviseurs successifs de $\#\mathcal{T}_k$, de la forme :

$$\{t_0 = \#\mathcal{T}_k, \dots, t_i, \dots, (t_{m_n} = \dots = t_{i_0}) = 1\},$$

définis, pour chaque $i \geq 0$ fixé, comme $\max\limits_{n\to\infty} \big(\#(M_{i+1}^n/M_i^n)\big)$ (cf. § 7.1).

On peut donc proposer l'heuristique probabiliste suivante (précisant les fondements p-adiques de la conjecture de Greenberg), reposant sur les heuristiques ci-dessus et en notant que, grosso modo, l'existence de chacune des $m_n = O(1) \cdot \big(\lambda \cdot n + \mu \cdot p^n + \nu\big)$ étapes de l'algorithme a une probabilité fonction de celles des $\delta_\mathfrak{p}$ à avoir une valeur "non triviale" (un cas emblématique simple étant celui des $\#(M_{i+1}^n/M_i^n) = p$ pour tout i pour un corps quadratique ; dans le cas général, la formule proposée en (iii) est seulement un ordre de grandeur largement suffisant pour conclure) :

Conjecture 7.3. — *Soit k un corps de nombres totalement réel et soit $p > 2$ totalement décomposé dans $k/\mathbb{Q}$. Soit $\mathcal{T}_k$ le groupe de torsion du groupe de Galois de la pro-p-extension Abélienne p-ramifiée maximale de k ; on suppose $\mathcal{T}_k \neq 1$. On considère l'algorithme associé à la filtration de $\mathcal{C}\ell_{k_n}$, $n \geq 1$ fixé, et la i-suite des groupes Λ_i^n, $1 \leq i \leq m_n$, pour laquelle on a $m_n \geq \frac{1}{v_p\left(\#\mathcal{T}_k\right)} \big(\lambda \cdot n + \mu \cdot p^n + \nu\big)$ (Théorème 6.1). Alors :*
(i) La probabilité que, pour un $x \in \Lambda_i^n$, on ait $\delta_\mathfrak{p}(x) \geq r$ (resp. $\delta_\mathfrak{p}(x) = 0$), pour tout $\mathfrak{p} \mid p$, est $\frac{1}{p^{\,r\,(d-1)}}$ $\Big($resp. $1 - \frac{1}{p^{\,d-1}}$ $\Big)$.
(ii) Soit $c \in \mathcal{C}\ell_k$. La probabilité que, pour un idéal $\mathfrak{A}$ de k_n étranger à p, la p-classe de $\mathrm{N}_{k_n/k}(\mathfrak{A})$ soit égale à c, est $\frac{1}{\#\mathcal{C}\ell_k}$.
(iii) Pour λ ou μ non nuls, la probabilité d'avoir $\#\mathcal{C}\ell_{k_n} = p^{\lambda\cdot n+\mu\cdot p^n+\nu}$ est au plus en $\frac{1}{p^{\,O(1)\,\cdot\,(\lambda\cdot n+\mu\cdot p^n)}}$, lorsque $n \to \infty$.

7.7. Perspectives. — Cette heuristique (même imparfaite) montre la légitimité de la conjecture de Greenberg mais aussi que la n-suite des $\#\mathcal{C}\ell_{k_n}$ est probablement très rapidement stationnaire, ce qui est plutôt un élément favorable pour une approche plus analytique. Il semble en effet difficile de trouver des arguments théoriques qui "obligeraient" les classes des normes $\mathrm{N}_{k_n/k}(\mathfrak{A})$ d'idéaux aléatoires $\mathfrak{A}$ de k_n à ne pas se répartir uniformément dans $\mathcal{C}\ell_k$, ou les $\delta_\mathfrak{p}(x)$ des quotients de Fermat des $x \in k^\times$ à ne pas suivre des lois binomiales reposant sur la probabilité de nullité en $1 - \frac{1}{p}$ (voire encore plus proches de 1 comme nous l'avons longuement analysé dans [**18**] et [**19**] pour les nombres algébriques en général). Voir à ce sujet [**22**] qui établit déjà la répartition uniforme des quotients de Fermat des entiers rationnels et qui est probablement générale.

Cette question risque de rester sans réponse, d'autant plus qu'un éminent mathématicien français m'avait conforté en affirmant, dans un échange au sujet des quotients de Fermat des rationnels (Janvier 2012) :

"Or vous savez bien que c'est la pire des situations : quand quelque chose est aléatoire (par exemple un quotient de Fermat) on est souvent complètement désarmé pour le démontrer".

Ceci explique la difficulté rencontrée en "théorie d'Iwasawa algébrique" concernant le "calcul" des invariants λ, μ, ν de la limite projective des $\mathcal{C}\ell_{k_n}$ pour le cas totalement réel en l'absence d'une conjecture très ambitieuse qui gouvernerait beaucoup de problèmes arithmétiques analogues où interviennent de tels objets p-adiques "aléatoires", d'autant plus que tout ce qui précède repose sur la conjecture de Leopoldt ; or celle-ci revient à dire grosso modo que la probabilité, pour le régulateur R_k, d'être divisible par p^n est en $\frac{1}{p^{f(n)}}$, $f(n) \to \infty$ si $n \to \infty$, c'est-à-dire analogue à celle de l'Heuristique 7.3 (iii), et que $R_k = 0$ est "presque sûrement" impossible.

On peut donc se demander si une aproche de type transcendance p-adique ne serait pas mieux adaptée puisque c'est l'une des voies démontrant quelques cas non triviaux de la conjecture de Leopoldt.

Tout ceci est aussi lié à un point de vue différent qui est celui de fixer le corps k et de faire tendre p vers l'infini, auquel cas un cadre conjectural p-adique analogue [**19**, Section 7] conduirait à la p-rationalité de k pour tout premier $p \gg 0$, donc à la conjecture de Greenberg pour laquelle on aurait $\lambda_p = \mu_p = \nu_p = 0$ indépendamment de toute technique d'Iwasawa.

8. Statistiques sur les $\delta_{\mathfrak{p}}(x)$ et les classes des $\mathrm{N}_{k_n/k}(\mathfrak{A})$

Le point essentiel est le comportement, pour n fixé, des "quotients de Fermat" $\mathfrak{p}^{\delta_{\mathfrak{p}}(x_i)}$ (Définition 4.1), pour les $x_i \in \Lambda_i^n$ tels que $(x_i) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)$ ainsi que les classes des idéaux $\mathrm{N}_{k_n/k}(\mathfrak{A}_i)$ où les $\mathfrak{A}_i \in \mathcal{I}_i^n$ représentent les classe de M_i^n.

L'étape de l'algorithme calculant le $(i+1)$-ième sous-groupe M_{i+1}^n de la filtration repose sur les $x_i = \mathrm{N}_{k_n/k}(y_i) \in \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times)$, tels que $(x_i) = \mathrm{N}_{k_n/k}(\mathfrak{B}_i)$, $\mathfrak{B}_i \in \mathcal{I}_i^n$, ce qui conduit à $\mathfrak{A}_{i+1}^{1-\sigma_n} \cdot \mathfrak{B}_i = (y_i)$, $\mathfrak{A}_{i+1}$ étranger à p dont on prend la norme, etc.

On a alors $\omega_n(\Lambda_{m_n}^n) = \Omega(k_n/k)$ et $\mathrm{N}_{k_n/k}(M_{m_n}^n) = \mathcal{C}\ell_k$, pour le nombre de pas m_n de l'algorithme.

D'après le Théorème 6.1, en supposant par exemple $\mathcal{T}_k \neq 1$ et $\mathcal{C}\ell_k = 1$, l'hypothèse λ ou $\mu \geq 1$ doit conduire à au moins $\frac{1}{v_p(\#\mathcal{T}_k)}\,(\lambda \cdot n + \mu \cdot p^n + \nu)$ valeurs consécutives de l'indice i pour lesquelles tous les x_i sont tels que $\delta_{\mathfrak{p}}(x_i) \geq 1$ pour certains $\mathfrak{p} \mid p$ de telle sorte que $\omega_n(\Lambda_i^n) \subset \Omega(k_n/k)$; ceci rend indispensable la confrontation avec l'expérimentation numérique.

Pour cela on commence par un cadre simple, mais non trivial, utilisant des idéaux $\mathfrak{A}_i$ premiers, dans le cas $\mathcal{C}\ell_k = 1$. Ensuite, on aura à examiner le facteur "classes" et le facteur "normique" dans l'expression de M_{i+1}^n / M_i^n.

8.1. Représentation des classes par des idéaux premiers $\mathfrak{L}_i$. — D'après le théorème de Tchebotarev, pour tout $c \in \mathcal{C}\ell_{k_n}$ il existe une infinité de nombres premiers ℓ tels que, pour un idéal premier convenable $\mathfrak{L}' \mid \ell$ dans H_{k_n} (le p-corps de classes de Hilbert de k_n), $\left(\frac{H_{k_n}/\mathbb{Q}}{\mathfrak{L}'}\right)$ soit l'élément de $\mathrm{Gal}(H_{k_n}/k_n)$ correspondant à c par le corps de classes ; comme H_{k_n}/k_n est Abélienne, ce Frobenius ne dépend que de l'idéal premier $\mathfrak{L}$ de k_n au-dessous

de $\mathfrak{L}'$. L'image de $\left(\frac{H_{k_n}/k_n}{\mathfrak{L}}\right)$ dans $\mathrm{Gal}(H_{k_n}/k_n)$ est encore c et est représentée par $\mathfrak{L}$ totalement décomposé dans $k_n/\mathbb{Q}$.

Autrement dit, lorsque par exemple k est principal, en se limitant à des idéaux premiers $\mathfrak{L}$ totalement décomposés dans $k_n/\mathbb{Q}$ et en considérant $\mathfrak{l} = (\alpha)$ pour l'idéal premier $\mathfrak{l} = \mathrm{N}_{k_n/k}(\mathfrak{L})$ de k en-dessous de $\mathfrak{L}$, on peut effectuer des statistiques sur les valeurs prises par les $\delta_{\mathfrak{p}}(\alpha)$ *indépendamment de tout contexte conjecture de Greenberg* puisque les $\mathfrak{L}_i$ de l'algorithme seront aléatoirement certains $\mathfrak{L}$ particuliers.

On reprend ici les même hypothèse simplificatrices faites au § 6.3, où le corps $k = \mathbb{Q}(\sqrt{m})$ est principal et les entiers $\delta_p(\varepsilon)$ et $\delta_{\mathfrak{p}}(\pi)$ non nuls, de sorte que la condition suffisante du Théorème 3.1 ne s'applique pas (en réalité, les résultats n'en dépendent pas.

Le nombre α tel que $\mathrm{N}_{k_n/k}(\mathfrak{L}) = \mathfrak{l} = (\alpha)$ est un entier de k (unique à une unité près) de norme $\ell = \mathfrak{l} \cap \mathbb{Z}$ sur $\mathbb{Q}$, où $\ell^{p-1} \equiv 1 \pmod{p^{n+1}}$. On a $\alpha^{p-1} = 1 + p \cdot p^{\delta_p(\alpha)} \cdot \beta$, β étranger à p si $\delta_p(\alpha) < n$.

Le choix par PARI de α modulo E_k influe de façon marginale sur les statistiques (voir ci-après un cas sans équivoque avec $\delta_3(\varepsilon) = 6$). Ceci vaut pour tous les résultats de cette section où le "choix" de α intervient.

(i) Dans l'expérimentation numérique, pour $p = 3$, on prend n assez grand de sorte que l'on compte dans C_r les nombres premiers $\ell \equiv \pm 1 \pmod{3^{n+1}}$ pour lesquels $\delta_p(\alpha) = r$, où r varie de 0 à $n-1$ au plus, et on compare le résultat aux probabilités naturelles $\frac{2}{3}$, $\frac{2}{3^2}$, $\cdots$, $\frac{2}{3^r}$, $\cdots$.

```
{p=3; m=103; n=12; B=10^13; M=p^(n+1); Q=x^2-m;
K=bnfinit(Q,1); C0=0; C1=0; C2=0; C3=0; C4=0; C5=0; NL=0;
for(t=-1, 0, L=2*t+1; while(L<B, L=L+2*M;
if(isprime(L)==1 & kronecker(m,L)==1, NL=NL+1;
Su=bnfsunit(K, idealprimedec(K,L));
A=component(component(Su,1),1);
AA=(Mod(A,Q)^2-1)/3; v=valuation(AA,3);
if(v==0, C0=C0+1); if(v==1, C1=C1+1); if(v==2, C2=C2+1);
if(v==3, C3=C3+1); if(v==4, C4=C4+1); if(v>=5, C5=C5+1))));
print(p,"   ",m,"   ",n,"   ",B);
print(NL,"  ",C0," ",C1," ",C2," ",C3," ",C4," ",C5);
print(C0/NL+0.0,"  ",C1/NL+0.0,"  ",C2/NL+0.0,"  ",C3/NL+0.0,"  ",
C4/NL+0.0,"  ",C5/NL+0.0); print("  ");
S=0.0; for(j=1,8, S=S+(p-1.0)/p^(5+j));
print(2./3,"  ",2./9,"  ",2./27,"  ",2./81,"  ",2./243,"  ", S)}
```

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

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

Il y a alors $N_L = 325644$ nombres premiers ℓ dans l'intervalle, dont respectivement $C_0 = 217122$, $C_1 = 72353$, $C_2 = 24174$, $C_3 = 8043$, $C_4 = 2620$, $C_5 = 1332$, sont tels que $\delta_p(\alpha) = 0, 1, 2, 3, 4, \geq 5$.

proportions	probabilités
$C_0 = 0.6667465084$	$\frac{2}{3} = 0.6666666666$
$C_1 = 0.2221843485$	$\frac{2}{3^2} = 0.2222222222$
$C_2 = 0.0742344400$	$\frac{2}{3^3} = 0.0740740740$
$C_3 = 0.0246987507$	$\frac{2}{3^4} = 0.0246913580$
$C_4 = 0.0080455958$	$\frac{2}{3^5} = 0.0082304526$
$C_5 = 0.0040903563$	$\sum_{j \geq 6} \frac{2}{3^j} = 0.0041152264$

Le même calcul pour $m = 2149$, où $\delta_p(\varepsilon) = \delta_{\mathfrak{p}}(\pi) = 3$, conduit à des résultats similaires : $N_L = 325538$, $C_0 = 216955$, $C_1 = 72406$, $C_2 = 24145$, $C_3 = 8063$, $C_4 = 2667$, $C_5 = 1302$ (première proportion 0.6664506140).

L'exemple suivant pour lequel $\delta_3(\varepsilon) = 6$ est donc tel que $\delta_3(\alpha)$ est indépendant du représentant modulo E_k donné par PARI, au moins pour $r \leq 5$ ($m = 1213$, $n = 12$, $B = 10^{13}$) : $N_L = 325778$, $C_0 = 217298$, $C_1 = 72322$, $C_2 = 24144$, $C_3 = 8075$, $C_4 = 2621$, $C_5 = 1318$, avec les proportions 0.6670125054, 0.2219978021, 0.0741118184, 0.0247868180, 0.0080453560, 0.0040456998.

En prenant $m = 397$, $n = 100$, $B = 10^{54}$, et $\ell \equiv \pm 1 \pmod{3^{101}}$, on obtient les valeurs très stables : $N_L = 7947$, $C_0 = 5305$, $C_1 = 1702$, $C_2 = 646$, $C_3 = 207$, $C_4 = 55$, $C_5 = 32$, et la proportion 0.6675475022 de $\delta_p(\alpha) = 0$.

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

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

On considère l'exemple pour lequel $\delta_p(\varepsilon) = \delta_{\mathfrak{p}}(\pi) = 1$: $p = 7$, $m = 44853$, $n = 5$, $\ell^{p-1} \equiv 1 \pmod{7^6}$, $1 < \ell < 10^{12}$. On a alors $N_L = 1118955$, $C_0 = 959051$, $C_1 = 137487$, $C_2 = 19118$, $C_3 = 2842$, $C_4 = 388$, $C_5 = 69$.

proportions	probabilités
$C_0 = 0.8570952361$	$\frac{6}{7} = 0.8571428571$
$C_1 = 0.1228708929$	$\frac{6}{7^2} = 0.1224489795$
$C_2 = 0.0170855843$	$\frac{6}{7^3} = 0.0174927113$
$C_3 = 0.0025398697$	$\frac{6}{7^4} = 0.0024989587$
$C_4 = 0.0003467521$	$\frac{6}{7^5} = 0.0003569941$
$C_5 = 0.0000616646$	$\sum_{j\geq 6} \frac{6}{7^j} = 0.0000059499$

On considère enfin le cas suivant pour lequel $\delta_p(\varepsilon) = \delta_{\mathfrak{p}}(\pi) = 1$: $p = 29$, $m = 683$, $n = 5$, $\ell^{p-1} \equiv 1 \pmod{29^6}$, $1 < \ell < 10^{15}$.
$N_L = 728880$, $C_0 = 703535$, $C_1 = 24450$, $C_2 = 857$, $C_3 = 38$, $C_4 = C_5 = 0$.

proportions	probabilités
$C_0 = 0.9652274722$	$\frac{28}{29} = 0.9655172413$
$C_1 = 0.0335446163$	$\frac{28}{29^2} = 0.0332936979$
$C_2 = 0.0011757765$	$\frac{28}{29^3} = 0.0011480585$
$C_3 = 0.0000521347$	$\frac{28}{29^4} = 0.0000395882$
$C_4 = 0$	$\frac{28}{29^5} = 0.0000013651$
$C_5 = 0$	$\sum_{j\geq 6} \frac{28}{29^j} = 0.0000000488$

(iii) Les groupes $\Lambda_i^n = \{x \in k^\times, (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)\}$ des exemples précédents sont de la forme $\Lambda_i^n = \langle \varepsilon, \alpha_1, \ldots, \alpha_i \rangle$ pour $1 \leq i \leq m_n$ (§ 6.3), et la probabilité d'avoir m_n générateurs (outre ε) suit une loi binomiale *indépendamment de la*

valeur de $n \to \infty$, ce qui suggère une probabilité nulle d'avoir λ ou $\mu \geq 1$, c'est-à-dire $m_n = O(\lambda \cdot n + \mu \cdot p^n)$ (Théorème 6.1).

(iv) Exemple avec le sous-corps cubique K de $\mathbb{Q}(\mu_7)$ défini par le polynôme $Q = x^3 + x^2 - 2\,x - 1$, $p = 13$, $n = 3$, $\ell^{p-1} \equiv 1 \pmod{p^4}$, $1 < \ell < 10^{12}$. Pour avoir les ℓ décomposés dans k, le programme factorise Q modulo ℓ et teste le nombre de facteurs d (principe qui permet de varier Q facilement).

```
{p=13; n=3; B=10^12; M=p^(n+1); Q=x^3+x^2-2*x-1; K= bnfinit(Q,1);
ro=znprimroot(M)^(p^n); C0=0; C1=0; C2=0; C3=0; NL=0;
for(k=1, p-1, R=Mod(ro,M)^k; L=component(R,2); while(L<B, L=L+M;
if(isprime(L)==1, QL=x^3+x^2-2*x-Mod(1,L); F=factor(QL);
d=component(matsize(F),1); if(d==3, NL=NL+1;
Su=bnfsunit(K, idealprimedec(K,L)); A=component(component(Su,1),1);
AA =(Mod(A,Q)^(p-1)-1)/p; v=valuation(AA,p);
if(v==0, C0=C0+1); if(v==1, C1=C1+1); if(v==2, C2=C2+1);
if(v==3, C3=C3+1))))); print(p," ",n," ",B);
print(NL," " ,C0," ",C1," ",C2," ",C3);
print(C0/NL+0.0," ",C1/NL+0.0," ",C2/NL+0.0," ",C3/NL+0.0);
print((p^2-1.0)/p^2," ",(p^2-1.0)/p^4," ",
                                (p^2-1.0)/p^6," ",(p^2-1.0)/p^8)}
```

Il y a alors $N_L = 5707184$ nombres ℓ dans l'intervalle, dont $C_0 = 5673504$, $C_1 = 33487$, $C_2 = 192$, $C_3 = 1$, sont tels que $\delta_p(\alpha) = 0, 1, 2, 3$.

	proportions		probabilités
$C_0 =$	0.9940986658	$\frac{p^2-1}{p^2} =$	0.9940828402
$C_1 =$	0.0058675171	$\frac{p^2-1}{p^4} =$	0.0058821469
$C_2 =$	0.0000336418	$\frac{p^2-1}{p^6} =$	0.0000348056
$C_3 =$	0.0000001752	$\frac{p^2-1}{p^8} =$	0.0000002059

8.2. Statistiques sur m_n. — Rappelons, pour l'algorithme, que si $x_i = \mathrm{N}_{k_n/k}(y_i) \in \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times)$, où $(x_i) = \mathrm{N}_{k_n/k}(\mathfrak{B}_i) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)$, la relation $\mathfrak{A}_{i+1}^{1-\sigma_n} \cdot \mathfrak{B}_i = (y_i)$ fournit le nouvel $\mathfrak{A}_{i+1}$ dont on calcule $\mathrm{N}_{k_n/k}(\mathfrak{A}_{i+1})$ pour constituer Λ_{i+1}^n, puis les $\delta_p(x_{i+1})$, etc. Considérons alors un corps quadratique k et le n-ième étage de k_∞ pour lequel on souhaite tester l'indépendance des $\delta_p(x_i) \geq 0$, $x_i \in \Lambda_i^n$, obtenus successivement par l'algorithme de calcul de $\mathcal{C}\ell_{k_n}$ pour $1 \leq i \leq m_n$ et de même celle des classes des $\mathrm{N}_{k_n/k}(\mathfrak{A}_i)$ dans $\mathcal{C}\ell_k$.

Comme la recherche numérique, par programme PARI, des idéaux $\mathfrak{A}_i$ et des $x_i \in \Lambda_i^n$ tels que $(x_i) = \mathrm{N}_{k_n/k}(\mathfrak{B}_i)$, est particulièrement difficile on procède de façon indirecte par le biais du calcul de m_n ($n = 1$ en pratique) à partir de celui de $\#\mathcal{C}\ell_{k_n}$.

Pour étudier les deux facteurs de $\#(M_{i+1}^n/M_i^n)$ on considère séparément les cas $\mathcal{C}\ell_k = 1$ et $\delta_p(\varepsilon) = 0$ qui permettent des statistiques respectivement sur :

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

8.2.1. Calcul de m_n dans le cas $\mathcal{C}\ell_k = 1$ & $\delta_p(\varepsilon) = 1$, k quadratique. — On se place dans les conditions pour lesquelles le nombre de classes ambiges dans k_n/k est égal à p, donc avec la seule hypothèse :

$$(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n-1},$$

qui équivaut au fait que $\delta_p(\varepsilon) = 1$. Il en résulte qu'il est équivalent de faire des statistiques sur l'ordre de $\mathcal{C}\ell_{k_n}$ lorsque $k = \mathbb{Q}(\sqrt{m})$ varie, ce que PARI effectue assez rapidement ; en effet, on a la filtration correspondante $(M_i^n)_{i\geq 0}$,

de $M^n = \mathcal{C}\ell_{k_n}$, telle que $\#(M^n_{i+1}/M^n_i) = p$ pour $0 \leq i \leq m_n - 1$, et telle que $\#\mathcal{C}\ell_{k_n} = \prod_{i=0}^{m_n-1} \#(M^n_{i+1}/M^n_i) = p^{m_n}$.
On a $M^n = M^n_1$ si et seulement si $M^n_2 = M^n_1$, ce qui est équivalent à $\delta_p(\alpha_1) = 0$, de probabilité $1 - \frac{1}{p}$ et qui ne dépend pas du représentant α_1 modulo $\langle\varepsilon\rangle$.
Ensuite, on a $M^n = M^n_2$ si et seulement si $M^n_2 \neq M^n_1$ et $M^n_3 = M^n_2$, équivalent à $\delta_p(\alpha_1) \geq 1$ et $\delta_p(\alpha_2) = 0$, de probabilité $(1 - \frac{1}{p}) \cdot \frac{1}{p}$, etc.

Remarque 8.1. — *Noter que puisque* $\mathrm{N}_{k/\mathbb{Q}}(\varepsilon) = 1$, *la condition* $R_k \equiv 0 \pmod p$ *est équivalente à* $\delta_p(\varepsilon) \geq 1$ *et est donc de probabilité* $\frac{1}{p}$, *alors que pour* $x \in k^\times$ *arbitraire, la condition* $\delta_{\mathfrak{p}}(x) \geq 1$ *pour tout* $\mathfrak{p} \mid p$ *est de probabilité* $\frac{1}{p^2}$ *(cf. Lemme 5.1 et Remarque 5.1).*
Plus généralement, si $\alpha = 1 + p \cdot p^r \cdot \beta$, $0 \leq r < n$, *est tel que* $\mathrm{N}_{k/\mathbb{Q}}(\alpha) \equiv 1 \pmod{p^{n+1}}$, *ce qui est le cas si* (α) *est norme d'un idéal de* k_n, *on a la relation exceptionnelle* $\beta + \beta' + p^{r+1} \cdot \beta\,\beta' = u \cdot p^{n-r}$ *qui reflète la formule du produit et modifie la probabilité de p-divisibilité de* β *en* $\frac{1}{p}$ *au lieu de* $\frac{1}{p^2}$ *puisque* $p \mid \beta$ *équivaut à* $p \mid \beta'$, *d'où les probabilités pour les* $\delta_p(\alpha_i)$.
Si α *est une unité* ε, *on a* $\beta' + \beta \cdot \varepsilon' = 0$ *qui rend la propriété ci-dessus vraie pour tout n.*
Les deux programmes suivants ($k = \mathbb{Q}(\sqrt{7})$, $p = 3$) *justifient à nouveau le phénomène, pour* $y \in k^\times$, *selon la proximité p-adique de* $\mathrm{N}_{k/\mathbb{Q}}(y)$ *avec* 1 *:*

(i) On impose que la norme de l'élément aléatoire y soit assez proche de 1 (on peut remplacer 9 *par toute puissance de* 3 *plus grande) :*

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

Densité de $\delta_p(y) = 0$ *obtenue :* $0.6667709837 \sim \frac{2}{3}$.

(ii) Aucune condition de norme locale en dehors de p pour y :

```
{m=7; Q=x^2-m; X=Mod(x, Q); pi1=X-2; pi2=X+2; N=10^5; NY=0.0; NY0=0.0;
B=10^7; for(k=1, B, a=random(N); b=random(N); Y=a*X+b; n=norm(Y);
if(Mod(n, 3)!=0, NY=NY+1; Z=(Y^2-1)/3; Z1=Z*pi1; Z2=Z*pi2;
v1=valuation(component(Z1,2), 3); v2=valuation(component(Z2,2), 3);
v=min(v1, v2); if(v==0, NY0=NY0+1))); print(NY0/NY)}
```

Densité de $\min(\delta_{\mathfrak{p}}(y), \delta_{\mathfrak{p}'}(y)) = 0$ *obtenue :* $0.8889293692 \sim \frac{8}{9}$.

Dans le cas $n = 1$, il suffit de supposer $R_k = p$, donc que k est tel que $\delta_p(\varepsilon) \geq 1$. Autrement dit, ε est partout norme locale et n'intervient pas dans les raisonnements. L'indépendance des α_i est alors mesurée par les probabilités $\frac{p-1}{p^h}$ d'avoir $\#\mathcal{C}\ell_{k_1} = p^h$, $h \geq 1$ (même raisonnement que dans le cas précédent).
Le programme ci-dessous (écrit pour $n = 1$) est valable pour $p \geq 3$, mais pour $p > 3$, le temps de calcul devient prohibitif ; pour $n > 1$ remplacer $polsubcyclo(p^2, p)$ par $polsubcyclo(p^{n+1}, p^n)$.

```
{p=3; Cyclo=polsubcyclo(p^2, p); C1=0; C2=0; C3=0; C4=0; CM=0;
b=1; B=3*10^5;  m=b; while(m<b+B, m=m+1;
if(core(m)==m & kronecker(m, p)==1, Q=x^2-m; M=m; t=Mod(m,4);
if(t!=1, M=4*m); h=qfbclassno(M); if(valuation(h,p)==0, E=quadunit(M);
e1=component(E,2); e2=component(E,3); if(t==1, e2=e2/2; e1=e1+e2);
E=Mod(e1+e2*x, Q); EE=component(E^(p-1)-1,2);
ve=valuation(EE, p)-1; if(ve>=1, CM=CM+1;
P=polcompositum(Cyclo, Q); R=component(P,1); K=bnfinit(R, 1);
```

```
H=bnrinit(K,1); G=component(component(H,5),1); w=valuation(G,p);
if(w==1, C1=C1+1);  if(w==2, C2=C2+1);
if(w==3, C3=C3+1); if(w>=4, C4=C4+1)))));
print(CM,"  ",C1,"  ",C2,"  ",C3,"  ",C4);
print(C1/CM+0.0, "   " ,C2/CM+0.0, "   " ,
C3/CM+0.0,"   ",C4/CM+0.0); S=0.0; for(j=0, 8, S=S+(p^2-1)/p^(8+2*j));
print((p^2-1.0)/p^2,"  ",(p^2-1.0)/p^4,"  ",(p^2-1.0)/p^6,"  ",S)}
```

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

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

Remarque 8.2. — *La différence de nature entre d'une part les résultats numériques obtenus ici sur le comportement "fictif" des $\delta_p(\alpha_i)$ déduit du calcul effectif de $\#\mathcal{C}\ell_{k_n}$, et d'autre part les expérimentations du § 8.1 sur la représentation des classes par des idéaux premiers $\mathfrak{L}$ décomposés dans $k_n/\mathbb{Q}$, provient des faits suivants :*

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

Or $\#\big(M_2^n/M_1^n\big) = \dfrac{p^n}{(\Lambda_1 : \Lambda_1 \cap \mathrm{N}_{k_n/k}({k_n}^{\times}))}$, où $\Lambda_1 = \langle \varepsilon, \alpha_1 \rangle$, et la condition $M^n = M_1^n$ a lieu si et seulement si $M_2^n = M_1^n$, soit $\delta_p(\alpha_1) = 0$; si la S_k-unité η_1 est non norme dans k_n/k, quel que soit α'_1 on peut faire en sorte que $\alpha_1 = \alpha'_1 \cdot \eta_1$ soit norme, auquel cas on a au contraire $M_2^n \neq M_1^n$.

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

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

8.2.2. Calcul de m_n dans le cas $\#\mathcal{C}\ell_k = p$ & $\delta_p(\varepsilon) = 0$, k quadratique. — Lorsque $\delta_p(\varepsilon) = 0$, on a $\omega_n(\varepsilon)$ d'ordre p^n, d'où $\omega_n(\Lambda_i^n) = p^n$ pour tout i et tout n, et on obtient :

$$\#\big(M_{i+1}^n/M_i^n\big) = \frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} = \frac{p}{\#\mathrm{N}_{k_n/k}(M_i^n)}.$$

On se limite au cas $p = 3$, $n = 1$ et pour des corps k de nombre de classes 3. On a $\#\mathcal{C}\ell_{k_1} = p^w$, $w \geq 1$, puisque $\#\mathcal{C}\ell_k = p$, et le groupe des classes ambiges, d'ordre p, est engendré par les classes des idéaux invariants (cf. Relation (2.1)), donc par la classe de $(\mathfrak{a})$ (étendu à k_1 de $\mathfrak{a}$ tel que $\mathcal{C}\ell_k(\mathfrak{a}) \neq 1$), et celle de $\mathfrak{p}_1 \mid \mathfrak{p}$ dans k_1.

On a alors $\mathrm{N}_{k_1/k}(M_1^1) = \langle \mathscr{C}\ell_k(\mathfrak{a}^p), \mathscr{C}\ell_k(\mathfrak{p})\rangle = \langle \mathscr{C}\ell_k(\mathfrak{p})\rangle$ d'ordre p (i.e., $w = 1$) si et seulement si $\mathfrak{p}$ est non principal.

Le programme fournit $C_r := \#\{k = \mathbb{Q}(\sqrt{m}),\ w = r\}$, pour les $\mathbb{Q}(\sqrt{m})$ vérifiant les hypothèses précédentes et pour un intervalle donné pour m. On pourrait aussi prendre des m aléatoires.

```
{p=3; n=1; b=10^3; B=10^6; Cyclo=polsubcyclo(p^(n+1),p^n);
C1=0; C2=0; C3=0; C4=0; Cm=0.0; m=b;
while(m<B, m=m+1; if(core(m)==m & kronecker(m,p)==1, Q=x^2-m;
M=m; t=Mod(m,4); if(t!=1, M=4*m); h=qfbclassno(M);
if(valuation(h,p)==1, E=quadunit(M);
e1=component(E,2); e2=component(E,3);
if(t==1, e2=e2/2; e1=e1+e2); E=Mod(e1+e2*x, Q);
E=component(E^(p-1)-1,2);
ve=valuation(E,p)-1; if(ve==0, Cm=Cm+1;
P=polcompositum(Cyclo,Q);
R=component(P,1); K=bnfinit(R,1); H=bnrinit(K,1);
H=component(component(H,5),1); w=valuation(H,p);
if(w==1, C1=C1+1); if(w==2, C2=C2+1);
if(w==3, C3=C3+1); if(w>=4, C4=C4+1)))));
print(C1/Cm,"  ",C2/Cm,"  ",C3/Cm,"  ",C4/Cm)}
```

On obtient les résultats numériques suivants pour $p = 3$, $10^3 < m < 10^6$: $C_M = 8508$, $C_1 = 6362$, $C_2 = 1944$, $C_3 = 178$, $C_4 = 24$, et le tableau :

proportions	probabilités
$\frac{C_1}{C_M} = 0.7477668077$	$\frac{8}{11} = 0.72727272$
$\frac{C_2}{C_M} = 0.2284908321$	$\frac{8}{3.11} = 0.24242424$
$\frac{C_3}{C_M} = 0.0209214856$	$\frac{8}{3^3.11} = 0.02693602$
$\frac{C_4}{C_M} = 0.0028208744$	$\frac{8}{11}\sum_{j\geq 0}\frac{p-1}{p^{5+2j}} = 0.00336702$

La probabilité pour $\mathfrak{p} \mid p$ d'être non principal (i.e., $r = 1$) est difficile à établir car contrairement aux heuristiques générales, $\mathscr{C}\ell_k(\mathfrak{p})$ n'est pas "aléatoire". Un programme indépendant testant la principalité de $\mathfrak{p}$ (sans hypothèse sur ε mais pour des m beaucoup plus grands que dans le programme ci-dessus) donne une proportion de l'ordre de $O(1) \cdot \frac{p^2-1}{p^2+p-1}$. Ensuite on aurait des probabilités en $O(1) \cdot \frac{p^2-1}{p^2+p-1} \cdot \frac{1}{p^{2\cdot(r-1)-1}}$ pour tout $r \geq 2$.

9. Conclusion

Cette étude (qui a, au moins pour la première partie, des points généralisant les approches de **[8]**, **[10]**, **[11]**, **[12]**, **[21]**, **[26]**, **[27]**, **[28]**, **[50]**, **[51]**, **[52]**) montre que la question de la conjecture de Greenberg (pour les corps totalement réels) est essentiellement p-adique et sans doute moins "théorie d'Iwasawa algébrique" qu'admis généralement.

En outre, il s'agit probablement d'une question liée au seul invariant λ dans la mesure où la nullité de μ peut être admise plus facilement pour les corps totalement réels (voire démontrée, comme dans le cas Abélien) car, d'après l'étude de **[24]** dans un cadre très général :

Both in Iwasawa's work, and in the present one, the size of the μ-invariant appears to be intimately related to the existence of primes that split completely in the tower.

Le cas $\mu \neq 0$ serait donc lié à l'existence d'idéaux premiers totalement décomposés dans la $\mathbb{Z}_p$-extension de k considérée (premiers exemples de telles $\mathbb{Z}_p$-extensions dûs, entre autres, à Iwasawa **[29]**, Serre **[48]**, § 4.5], Cuoco **[7]**,

Hubbard–Washington [**25**]), ce qui est évidemment impossible pour la $\mathbb{Z}_p$-extension cyclotomique (cf. Section 8.1 sur l'utilisation des idéaux premiers pour représenter les classes dans k_∞).

Le cas des corps k Abéliens réels peut être de nature plus particulière en raison des "formules analytiques p-adiques" du nombre de classes introduisant les unités cyclotomiques et conduisant, avec des hypothèses "ad hoc", à de nombreux travaux spécifiques (voir [**9**], [**3**], [**4**], [**37**], [**40**], [**41**] et leurs références), bien que nous pensions que la version fonctions L p-adiques classique (au sens de [**49**], [**54**]) ne soit qu'une traduction analytique de l'aspect "modules sur l'algèbre d'Iwasawa", et n'apporte pas d'information supplémentaire au niveau "diophantien p-adique".

Si le passage à la limite (algébrique ou analytique p-adique) est au demeurant plus concis et structurant que les calculs aux niveaux finis, ceux-ci sont nécessaires pour localiser les profonds phénomènes arithmétiques sous-jacents. En effet, du seul point de vue théorie d'Iwasawa, le problème porte sur la détermination du quotient de Herbrand :

$$q(\mathcal{X}_k) := \#(\mathcal{X}_k^G)/\#({}^G\mathcal{X}_k)$$

de $\mathcal{X}_k := \varprojlim_{n\to\infty} \mathcal{C}\ell_{k_n}$ (pour la norme arithmétique), où $\mathcal{X}_k^G$ (resp. ${}^G\mathcal{X}_k$) est le noyau (resp. le conoyau) de l'opération de $1-\sigma$ sur $\mathcal{X}_k$, où σ est un générateur topologique de $G := \mathrm{Gal}(k_\infty/k)$ (voir [**35**, § 1.1] et [**42**, § 3] pour quelques rappels sous des approches différentes). La pseudo-nullité de $\mathcal{X}_k$ (i.e., $\lambda = \mu = 0$) est équivalente à $q(\mathcal{X}_k) = 1$.

Si la détermination de ${}^G\mathcal{X}_k$ équivaut grosso modo aux résultats du § 4.3, c'est-à-dire à la théorie du corps de classes global, la détermination de $\mathcal{X}_k^G$ semble non triviale et probablement liée aux considérations p-adiques précédentes où l'on rencontre manifestement des problèmes de type "quotients de Fermat" de nombres algébriques dont les heuristiques impliquent que les conjectures énoncées sont très raisonnables.

Pour conclure, nous nous proposons de faire quelques remarques sur les groupes $\mathcal{T}_{k_n}$ sous la conjecture de Leopoldt pour p dans k_∞, quelle que soit la décomposition de p dans le corps totalement réel k, ce qui nous paraît plus canonique en raison de la spécificité de ces groupes de torsion associés à la p-ramification Abélienne et plus susceptibles d'une approche essentiellement p-adique de la conjecture de Greenberg pour laquelle il serait utile de tester numériquement l'Hypothèse 7.1.

Pour tout $n \gg 0$, on a encore $\#\mathcal{T}_{k_n} = \#\mathcal{C}\ell_{k_n} \cdot \#(U_{k_n}^*/\overline{E}_{k_n})$, avec des notations analogues à celles du § 4.3, où les $\mathbb{Z}_p$-modules $U_{k_n}^*$ et $\overline{E}_{k_n}$ sont $\mathbb{Z}_p$-libres de $\mathbb{Z}_p$-rangs $d \cdot p^n - 1$.

On peut également noter $R_{k_n} := \#(U_{k_n}^*/\overline{E}_{k_n})$ le régulateur convenablement normalisé de k_n.

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

On a $\widetilde{\lambda} = 0$ si et seulement si $\mathcal{T}_k = 1$ (i.e., k est p-rationnel) pour les raisons suivantes : les "transferts" $j_{k_{n+h}/k_n} : \mathcal{T}_{k_n} \longrightarrow \mathcal{T}_{k_{n+h}}$ sont injectifs pour tous n, h (en raison de la conjecture de Leopoldt pour p dans la tour) [**14**, Theorem IV.2.1] ; on a en particulier la formule de points fixes (k_{n+h}/k_n étant trivialement *p-primitivement ramifiée*, [**14**, Theorem IV.3.3]), $\mathcal{T}_{k_{n+h}}^{\mathrm{Gal}(k_{n+h}/k_n)} = j_{k_{n+h}/k_n}(\mathcal{T}_{k_n}) \simeq \mathcal{T}_{k_n}$.
Considérons alors $\nu_{k_{n+1}/k_n} := j_{k_{n+1}/k_n} \circ \mathrm{N}_{k_{n+1}/k_n}$; si $\widetilde{\lambda} = 0$, on a $\mathcal{T}_{k_{n+1}} = j_{k_{n+1}/k_n}(\mathcal{T}_{k_n})$ et puisque l'on a $\mathrm{N}_{k_{n+1}/k_n} \circ j_{k_{n+1}/k_n} = p$, on obtient, à partir de l'égalité précédente (la norme arithmétique est surjective, cf. Schéma du § 7.4.2), $\mathcal{T}_{k_n} = \mathcal{T}_{k_n}^p$, d'où $\mathcal{T}_{k_n} = 1$, et comme $\mathcal{T}_{k_n}^{G_n} \simeq \mathcal{T}_k$, on a $\mathcal{T}_k = 1$. Réciproque évidente. On notera que $\widetilde{\lambda} = 0$ implique $\widetilde{\nu} = 0$.

Ainsi $\widetilde{\lambda} = 0$ est équivalent à $\mathcal{C}\ell_{k_n} = R_{k_n} = 1$ pour tout n (p-rationalité dans la tour), ce qui peut suggérer que $\widetilde{\lambda}$ est davantage accessible puisque $\#\mathcal{T}_{k_n}$ est essentiellement donné par le résidu de la fonction zêta p-adique de k_n (cf. [**6**], [**47**], [**54**]), ce qui permet, comme dans [**5**], [**27**], [**28**], d'en déduire des cas de nullité de λ lorsque $\widetilde{\lambda} \geq 1$.
On remarque que $\dfrac{\#\mathcal{T}_{k_n}}{\#\mathcal{T}_k} = \#(\mathcal{T}_{k_n}/\mathcal{T}_{k_n}^{G_n})$ et que le calcul de $(\mathcal{T}_{k_n}/\mathcal{T}_{k_n}^{G_n})^{G_n}$ serait le second pas de l'algorithme définissant la filtration habituelle dans le cadre différent de la p-ramification Abélienne qui, à notre connaissance, n'a pas été étudié.

Remerciements. — Je remercie J-F. Jaulent, T. Nguyen Quang Do et C. Maire pour plusieurs échanges, commentaires et indications (techniques et bibliographiques).

Références

[1] J. Assim & T. Nguyen Quang Do – "Sur la constante de Kummer–Leopoldt d'un corps de nombres", *Manuscripta Math.* **115** (2004), no. 1, p. 55–72. https://link.springer.com/article/10.1007/s00229-004-0482-9

[2] K. Belabas & J-F. Jaulent – "The logarithmic class group package in PARI/GP", *Publ. Math. Fac. Sci. Besançon (Théorie des Nombres)* 2016, p. 5–18. http://pmb.cedram.org/cedram-bin/article/PMB_2016____5_0.pdf

[3] R. Badino & T. Nguyen Quang Do – "Sur les égalités du miroir et certaines formes faibles de la conjecture de Greenberg", *Manuscripta Math.* **116** (2005), no. 3, p. 323–340. https://link.springer.com/article/10.1007/s00229-004-0531-4

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

[5] L. Caputo & F.A.E. Nuccio – "A criterion for Greenberg's conjecture", *Proc. of the Amer. Math. Soc.* **136** (2008), no. 8, p. 2741–2744. http://www.ams.org/journals/proc/2008-136-08/S0002-9939-08-09283-6/

[6] 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.

[7] A.A. Cuoco – "Generalized Iwasawa invariants in a family", *Compositio Math.* **51** (1984), no. 1, p. 89–103.
http://www.numdam.org/item/CM_1984__51_1_89_0

[8] T. Fukuda – "Greenberg's Conjecture and Relative Unit Groups for Real Quadratic Fields", *Journal of Number Theory* **65** (1997), no. 1, p. 23–39. http://www.sciencedirect.com/science/article/pii/S0022314X97921260

[9] T. Fukuda – "Cyclotomic Units and Greenberg's Conjecture for Real Quadratic Fields", *Math. Comp.* **65** (1996), no. 215, p. 1339–1348. http://www.ams.org/journals/mcom/1996-65-215/S0025-5718-96-00730-2/

[10] T. Fukuda & K. Komatsu – "On $\mathbb{Z}_p$-extensions of real quadratic fields", *J. Math. Soc. Japan* **38** (1986), no. 1, p. 95–102. https://projecteuclid.org/euclid.jmsj/1230395094

[11] T. Fukuda & H. Taya – "The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields", *Acta Arith.* **69** (1995), no. 3, p. 277–292. http://matwbn.icm.edu.pl/ksiazki/aa/aa69/aa6936.pdf

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

[13] G. Gras & J-F. Jaulent – "Sur les corps de nombres réguliers", *Math. Z.* **202** (1989), p. 343–365. https://eudml.org/doc/174095

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

[15] G. Gras – "Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ, I & II" (Thèse d'Etat), *Annales de l'Institut Fourier* **23** (1973), no. 3, p. 1–48, **23** (1973), no. 4, p. 1–44. http://www.numdam.org/item?id=AIF_1973__23_3_1_0 http://www.numdam.org/item?id=AIF_1973__23_4_1_0

[16] G. Gras – "Classes généralisées invariantes", *J. Math. Soc. Japan* **46** (1994), no. 3, p. 467–476. http://projecteuclid.org/euclid.jmsj/1227104692

[17] 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

[18] G. Gras – "Nombre de φ-classes invariantes. Application aux classes des corps abéliens", *Bulletin de la Société Mathématique de France* **106** (1978), p. 337–364. http://www.numdam.org/item?id=BSMF_1978__106__337_0

[19] G. Gras – "Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques", *Canadian Journal of Mathematics* **68** (2016), no. 3, p. 571–624. http://dx.doi.org/10.4153/CJM-2015-026-3

[20] G. Gras – "The p-adic Kummer-Leopoldt Constant – Normalized p-adic Regulator" (preprint 2017). https://arxiv.org/pdf/1701.06857.pdf

[21] 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

[22] R. Heath-Brown – "An Estimate For Heilbronn's Exponential Sum", In: *Conference in honor of Heini Halberstam, Analytic Number Theory* **2** (1996), Birkhüser 1996. http://eprints.maths.ox.ac.uk/157/1/heilbron.pdf

[23] Y. Hiroshi – "On the iwasawa invariants of totally real number fields", *Manuscripta Math.* **79** (1993), no. 6, p. 1–6. http://www.digizeitschriften.de/download/PPN365956996_0079/PPN365956996_0079___log4.pdf

[24] F. Hajir & C. Maire – "Prime decomposition and the Iwasawa mu-invariant" (preprint 2016). https://arxiv.org/pdf/1601.04195.pdf

[25] D. Hubbard & L.C. Washington – "Iwasawa invariants of some non-cyclotomic $\mathbb{Z}_p$-extensions" (2017). https://arxiv.org/abs/1703.06550

[26] A. Inatomi – "On $\mathbb{Z}_p$-extensions of real Abelian fields", *Kodai Math. J.* **12** (1989), no. 3, p. 420–422.
http://projecteuclid.org/download/pdf_1/euclid.kmj/1138039105

[27] H. Ichimura & H. Sumida – "On the Iwasawa invariants of certain real abelian fields, II", *Internat. J. Math.* **7** (1996), no. 6, p. 721–744.
http://www.worldscientific.com/doi/pdfplus/10.1142/S0129167X96000384

[28] H. Ichimura & H. Sumida – "On the Iwasawa invariants of certain real abelian fields", *Tohoku Math. J.* **49** (1997), no. 2, p. 203–215.
http://projecteuclid.org/download/pdf_1/euclid.tmj/1178225147

[29] K. Iwasawa – "On the μ-invariants of $\mathbb{Z}_\ell$-extensions", In: *Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki*, Kinokuniya, Tokyo 1973, p. 1–11.

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

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

[32] J-F. Jaulent – "Classes logarithmiques des corps de nombres", *J. Théorie des Nombres de Bordeaux* **6** (1994), no. 2, p. 301–325.
http://archive.numdam.org/article/JTNB_1994__6_2_301_0.pdf

[33] J-F. Jaulent – "Normes cyclotomiques naïves et unités logarithmiques" (preprint 2016). http://arxiv.org/abs/1609.01901

[34] J-F. Jaulent – "Sur les normes cyclotomiques et les conjectures de Leopoldt et de Gross-Kuz'min", *Annales. Math. Québec* (2016), p. 1–22. http://link.springer.com/article/10.1007/s40316-016-0069-3

[35] J-F. Jaulent – "Note sur la conjecture de Greenberg" (preprint 2016). https://arxiv.org/abs/1612.00718

[36] J-F. Jaulent & T. Nguyen Quang Do – "Corps p-rationnels, corps p-réguliers et ramification restreinte", *J. Théorie des Nombres de Bordeaux* **5** (1993), no. 2, p. 343–363.
http://www.numdam.org/article/JTNB_1993__5_2_343_0.pdf

[37] J.S. Kraft & R. Schoof – "Computing Iwasawa modules of real quadratic number fields", *Compositio Math.* **97** (1995), no. 1-2, p. 135–155. http://imaging.uniroma2.it/~schoof/ks.pdf

[38] M. Le Floc'h & A. Movahhedi & T. Nguyen Quang Do – "On capitulation cokernels in Iwasawa Theory", *American Journal of Mathematics* **127** (2005), no. 4, p. 851–877.https://www.jstor.org/stable/40067984

[39] A. Movahhedi & T. Nguyen Quang Do – "Sur l'arithmétique des corps de nombres p-rationnels", *Séminaire de Théorie des Nombres, Paris* 1987–88, Progress in Mathematics **81** (1990), p. 155–200. https://link.springer.com/chapter/10.1007%2F978-1-4612-3460-9_9

[40] T. Nguyen Quang Do – "Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé", *Int. J. of Number Theory* **2** (2006), no. 1, p. 49–64. http://www.worldscientific.com/doi/pdf/10.1142/S1793042106000395

[41] T. Nguyen Quang Do – "Sur une forme faible de la conjecture de Greenberg II", *Int. J. Number Theory* **13** (2017), no. 4, p. 1061-1070.
http://www.worldscientific.com/doi/pdf/10.1142/S1793042117500567

[42] T. Nguyen Quang Do – "Formules de genres et conjecture de Greenberg" (preprint 2017). https://www.researchgate.net/publication/311846783

[43] Y. Nishino – "On the Iwasawa Invariants of the Cyclotomic $\mathbb{Z}_2$-Extensions of Certain Real Quadratic Fields", *Tokyo J. Math.* **29** (2006), no. 1, p. 239–245.
https://projecteuclid.org/euclid.tjm/1166661877

[44] M. Ozaki & H. Taya – "A note on Greenberg's conjecture for real abelian number fields", *Manuscripta Math.* **88** (1995), no. 1, p. 311–320. http://link.springer.com/article/10.1007/BF02567825

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

[46] J-P. Serre – *Corps Locaux*, Actualités Scientifiques et Industrielles 1296, Hermann, quatrième édition revue et corrigée 2004.

[47] 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.

[48] J-P. Serre – "Quelques applications du théorème de densité de Chebotarev", *Publ. Math. IHES* **54** (1981), p. 123–201.
http://www.numdam.org/article/PMIHES_1981__54__123_0.pdf

[49] W. Sinnott – "On p-adic L-functions and the Riemann-Hurwitz genus formula", *Comp. Math.* **53** (1984), no. 1, p. 3–17.
http://www.numdam.org/item?id=CM_1984__53_1_3_0

[50] H. Sumida – "On Capitulation of S-Ideals in $\mathbb{Z}_p$-Extensions", *Journal of Number Theory* **86** (2001), no. 1, p. 163–174. http://www.sciencedirect.com/science/article/pii/S0022314X00925617

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

[52] H. Taya – "On p-adic zêta functions and $\mathbb{Z}_p$-extensions of certain totally real number fields", *Tohoku Math. J.* **51** (1999), no. 1, p. 21–33.
https://projecteuclid.org/download/pdf_1/euclid.tmj/1178224850

[53] H. Taya – "Iwasawa λ_5 and μ_5-invariants of a totally real cubic field with discriminant 1396", *Bulletin of Miyagi University of Education* **49** (2015), p. 91–94. http://id.nii.ac.jp/1138/00000408/

[54] L.C. Washington – *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

Georges Gras, Villa la Gardette, Chemin Château Gagnière, F–38520 Le Bourg d'Oisans, France – https://www.researchgate.net/profile/Georges_Gras
E-mail : `g.mn.gras@wanadoo.fr`