Thèse de Doctorat de l'Université Bourgogne Franche-Comté

Préparée au Laboratoire de Mathématiques de Besançon

Ecole doctorale 553
Carnot-Pasteur

Doctorat de Mathématiques

Par

M. Julien Koperecz

Corps p-rationnels multiquadratiques

Manuscrit soumis aux Rapporteurs

Jean-Robert Belliard	(Directeur de Thèse) Maître de Conférences
Christine Huygue	(Examinatrice) Directrice de Recherche
Florent Jouve	(Rapporteur) Professeur Des Universités
Philippe Lebacque	(Directeur de Thèse) Maître de Conférences
Ariane Mezard	(Examinatrice) Professeure Des Universités
Christian Wuthrich	(Rapporteur) Associate Professor

Remerciements

Tout d'abord, je veux exprimer mon infinie gratitude envers mes deux directeurs de thèse, Jean-Robert Belliard et Philippe Lebacque, qui m'ont soutenu, encouragé, poussé et aidé durant ces quatre dernières années. Je tiens à leur dire ici toute ma reconnaissance. Travailler avec eux a été un honneur autant qu'un plaisir. Ces quatre années n'auraient pas été les mêmes sans eux.

Je tiens à remercier l'ensemble des membres du jury – Christine Huygue, Ariane Mezard, Florent Jouve et Christian Wuthrich – d'avoir accepté d'encadrer et juger ma soutenance de ma thèse. Merci également à Bruno Saussereau et Marc Hindry d'avoir fait partie de mon comité de suivi : leurs conseils attentifs m'ont été d'une grande aide.

J'embrasse chaleureusement tous mes amis, et les membres de ma famille, pour leur soutien sans faille. A la patrouille du bonheur : Audry, Franck, Kevin, Manon, Margaux, Marie, Meva, Solenne et Tom (et une pensée pour Tim et Billie). Merci à Paul, Lucie, Arnaud, Baptiste (les deux), Benjamin, Manon, Julien, et Antoine.

J'ai une pensée particulière pour tous les membres et anciens membres du laboratoire de Mathématiques de Besançon, en particulier pour les jeunes doctorants (et jeunes docteurs), que l'on ait partagé un bureau ou non, et tous les gens merveilleux rencontrés en conférences au cours des ces dernières années : Marine, Benjamin, Colin, Lucie, Coline, Guillaume, Loris, Marsault, Mehdi, Tao, Mathieu, Charles, Audrey, Richard, Baptiste, et tous les autres.

Merci à tous mes anciens professeurs, de la prépa à la faculté, dont beaucoup sont devenus des collègues : apprendre puis travailler avec eux a été un véritable plaisir. Merci à Vésale de m'avoir accordé le privilège de khôller ses taupins toutes ces dernières années.

Et merci à tous les étudiants à qui j'ai eu le plaisir d'enseigner depuis le début, avec qui j'ai découvert le plaisir de transmettre l'amour des mathématiques.

Enfin, et puisqu'on garde toujours le meilleur pour la fin, il en est un sans qui rien n'aurait possible, qui m'a soutenu dans cette aventure plus que personne, et qui a bataillé autant que moi dans cette affaire : merci à mon Matthieu.

Introduction

Soit K un corps de nombres, et p un nombre premier. On note S un ensemble fini de places de K. On peut alors considérer la pro-p-extension S-ramifiée (c'est-à-dire non-ramifiée en dehors de S) maximale de K, qu'on notera M_S. Comprendre la structure de M_S et de son groupe de Galois $G_S = \mathrm{Gal}(M_S/K)$ forme le cœur de la théorie de la ramification restreinte. Dans la suite, on s'intéressera uniquement au cas où S contient toutes les places de K au-dessus de p. Dans ce cadre, on dira que le corps de nombres K est *p-rationnel* lorsque $G_{S_p} = \mathrm{Gal}(M_{S_p}/K)$ est un pro-p-groupe libre, avec S_p l'ensemble des p-places de K. La p-rationalité d'un corps de nombres est donc une hypothèse simplificatrice concernant le comportement du premier p vis-à-vis de la structure arithmétique du corps. Un certain nombre d'arguments algébriques et analytiques permettent de relier la p-rationalité de K à certain de ses invariants essentiels, tels le p-groupe de classes de K ou son régulateur p-adique.

La notion est étudiée depuis les années 1980, en particulier par G. Gras, T. Nguyen Quang Do, J.-F. Jaulent, A. Movahhedi et leurs élèves. La terminologie est due à A. Movahhedi, et apparait pour la première fois en 1988 dans [28].

Pour restrictive que semble être cette notion, il est conjecturé par G. Gras (dans [15]) qu'un corps de nombres est p-rationnel pour presque tout p : cette conjecture est supportée par certaines heuristiques autant que par l'observation empirique.

Considérant qu'un corps p-rationnel satisfait la conjecture de Leopoldt en p, les résultats obtenus dans ce cadre (en particulier, sur la montée de la p-rationalité dans une extension de corps de nombres), ont permis de construire une infinité de corps de nombres non-abéliens satisfaisant la conjecture de Leopoldt.

En 2016, R. Greenberg a réinventé l'utilisation des corps p-rationnels : il conjecture que, pour tout premier p impair et tout entier naturel t non-nul, il existe un corps de nombres dont le groupe de Galois sur $\mathbb{Q}$ est iso-

morphe à $\mathbb{Z}/2^t\mathbb{Z}$ (corps multiquadratiques). Cette conjecture lui permet de construire des représentations galoisiennes dans $\mathrm{GL}_n(\mathbb{Z}_p)$ d'image ouverte. De nombreux auteurs se sont attelés à démontrer cette conjecture au cours de ces dernières années ; on citera en particulier Barbulescu et Ray ([3], 2019), Gras ([16], 2019), Assim et Bouazzaoui ([1], 2020), Benmerieme et Movahhedi ([6] et [5], 2021).

Cette conjecture de Greenberg sur l'existence de corps p-rationnels multiquadratiques est le fil rouge de la présente thèse.

Dans le chapitre 1, on rappelle quelques notions préliminaires, en particulier la notion de pro-p-groupe libre, et on redonne certaines formulations de la conjecture de Leopoldt.

Dans le chapitre 2, on définit la notion de corps p-rationnel, et on rappelle de nombreux résultats et critères connus. On présente en particulier un état de l'art concernant la conjecture de Greenberg sur le corps p-rationnels multiquadratiques.

Dans le chapitre 3, on étudie le cas particulier du corps quadratique $\mathbb{Q}(\sqrt{p})$: on donne des critères simplifiés de p-rationalité pour ces corps en fonction de la forme d'une unité fondamentale, puis on montre la façon dont la conjecture de Bateman-Horn implique que $\mathbb{Q}(\sqrt{p})$ est p-rationnel pour une infinité de premiers p.

Dans le chapitre 4, on s'applique – via une méthode analytique – à démontrer qu'il existe une infinité de premiers p tels qu'un certain corps triquadratique donné est p-rationnel. Les résultats de ce chapitre étendent au cas triquadratique les résultats connus précédemment pour les cas quadratiques et biquadratiques, et ont fait l'objet d'un article soumis au Journal of Number Theory.

En annexe, on trouvera des éléments de démonstration d'un résultat conditionnel (sous GRH) plus fort que la proposition analytique utilisée et démontrée au chapitre 4 ; on trouvera également un ensemble de tables permettant d'illustrer les résultats du chapitre 3.

Table des matières

CHAPITRE 1

Notions préliminaires

1.1. Pro-p-groupes

On rappelle ci-après quelques propriétés des groupes profinis et pro-p-groupes. La lectrice ou le lecteur avide qui ne serait pas familier avec ces notions pourra se référer à [37] pour en savoir plus sur les groupes profinis en général, ou à [23] pour les pro-p-groupes en particulier.

1.1.1 Groupes profinis

Groupes profinis et pro-p-groupes

Définition 1.1.1. Un groupe topologique G est dit *profini* lorsqu'il est isomorphe (en tant que groupe topologique) à une limite projective de groupes finis munis de la topologie discrète.

On vérifie aisément qu'un groupe profini est séparé, compact (par le théorème de Tychonoff) et totalement discontinu.

Il s'agit en fait d'une caractérisation (voir [32] Proposition 1.1.3).

Définition 1.1.2. Soit p un nombre premier. Un groupe topologique G est appelé *pro-p-groupe* lorsqu'il est isomorphe (en tant que groupe topologique) à une limite projective de p-groupes finis munis de la topologie discrète.

Rappelons quelques propriétés élémentaires des groupes profinis et des pro-p-groupes :

Proposition 1.1.3. *1. Tout sous-groupe fermé d'un groupe profini (resp. pro-p-groupe) est un groupe profini (resp. pro-p-groupe).*

2. *Tout quotient G/K d'un groupe profini (resp. pro-p-groupe), avec K un sous-groupe normal fermé dans G, est un groupe profini (resp. pro-p-groupe).*
3. *Tout produit direct d'une famille $(G_i)_{i\in I}$ de groupes profinis (resp. pro-p-groupes), muni de la topologie produit, est un groupe profini (resp. pro-p-groupe).*
4. *La limite projective d'un système projectif de groupe profinis (resp. pro-p-groupes) est un groupe profini (resp. pro-p-groupe).*

Démonstration. Cf. [37] Prop. 2.2.1 □

Groupes profinis en tant que groupes de Galois

Les groupes profinis apparaissent de manière naturelle lorsque l'on considère les groupes de Galois d'extensions galoisiennes infinies.

En effet, si K/k une extension de corps galoisienne (algébrique, séparable et normale) et G le groupe de Galois de cette extension, on peut définir une topologie sur G (appelée *topologie de Krull*) via un système fondamental de voisinages de l'identité composée de tous les groupes de Galois $\mathrm{Gal}(K/N)$, où N est un corps intermédiaire de l'extension K/k tel que N/k est une extension galoisienne finie.

Le groupe de Galois G, muni de la topologie de Krull, est alors un groupe profini, isomorphe à la limite projective des $\mathrm{Gal}(N/k)$ (avec N comme précédemment).

Il existe alors une correspondance de Galois entre – d'un côté – les corps intermédiaire M de l'extension K/k et – d'un autre côté – les sous-groupes fermés de G (voir [23] Theo. 2.9).

Cohomologie des groupes profinis

Pour l'ensemble des notions de cohomologie des groupes profinis, en renvoie au classique [32] par Neukirch, Schmidt et Wingberg.

Considérant que les groupes profinis qui interviennent dans le chapitre suivant sont des pro-p-groupes (on considérera des pro-p-extensions), nous décrirons uniquement ces derniers dans la suite.

Dans toute la suite de cette section, on fixe un nombre premier p.

1.1.2 Générateurs d'un pro-p-groupe

Définition 1.1.4. Soit G un pro-p-groupe, et E une partie de G.
On dit que E génère G (en tant que groupe topologique) lorsque

1. le sous-groupe engendré par X est dense dans G, c'est-à-dire que G est le plus petit sous-groupe fermé contenant E.
2. tout voisinage de 1 contient presque tout élément de E.

On parle alors de système de générateurs.

Un système de générateurs est dit *minimal* lorsqu'il n'admet aucune partie propre qui forme elle-même un système de générateurs.

Note : On suit ici la définition de [23]. D'autres références, tel [37], nomme *ensemble de générateurs convergeant vers* 1 ce que l'on nomme ici simplement système de générateurs.

Proposition 1.1.5. *Tout pro-p-groupe admet un système de générateurs.*

Démonstration. [37] Prop. 2.4.4 □

Si G est un pro-p-groupe, on notera $d(G)$ le plus petit cardinal d'un système de générateurs de G.
On dit que G est de *type fini* lorsque G admet un ensemble de générateurs finis. Si G est un pro-p-groupe de type fini et U un sous-groupe ouvert, alors U est aussi un pro-p-groupe de type fini.

Théorème 1.1.6. *Soit G un pro-p-groupe, et $d(G)$ le cardinal minimal d'un système de générateurs de G. Alors on a $d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$.*

Démonstration. [23] Theorem 6.2 □

1.1.3 Pro-p-groupes libres

Soit $E = \{e_i \,|\, i \in I\}$ un ensemble indexé par I.
On peut montrer qu'il existe un groupe pro-p-groupe, unique à isomorphisme près, et qu'on notera $F(E)$, appelé *pro-p-groupe libre sur les générateurs* $\{e_i \,|\, i \in I\}$, caractérisé par les deux propriétés suivantes :

1. $F(E)$ est un pro-p-groupe contenant l'ensemble E comme système de générateurs.
2. Pour toute application $\mu : E \to G$ dans un pro-p-groupe G, telle tout voisinage de $1 \in G$ contient presque tout élément de $\mu(X)$, il existe un unique morphisme de groupes topologiques $\overline{\mu} : F(E) \to G$ qui prolonge l'application μ.

Si $F(X)$, le groupe pro-p-groupe libre sur les générateurs X, est aussi le groupe pro-p-groupe libre sur les générateurs Y, on sait que X et Y ont le même cardinal ([37] Lemme 3.3.5).

On a la caractérisation suivante des pro-p-groupes libres :

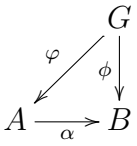
Théorème 1.1.7. *Soit G un pro-p-groupe. Les affirmations suivantes sont équivalentes :*

1. *G est un pro-p-groupe libre ;*
2. *toute extension de G par un pro-p-groupe H est scindé ; autrement dit, si H est un pro-p-groupe tel qu'on a une suite exacte courte*

$$1 \longrightarrow H \longrightarrow \overline{H} \underset{\varphi}{\longrightarrow} G \longrightarrow 1$$

   alors il existe une morphisme continu $\sigma : G \to \overline{H}$ tel que $\varphi \circ \sigma = \mathrm{id}$

3. *G est un objet projectif dans la catégorie des pro-p-groupes ; autrement dit, pour tout pro-p-groupes A et B, avec $\phi : G \to B$ morphisme continu, $\alpha : A \to B$ un épimorphisme continu, il existe un morphisme continu $\varphi : G \to B$ tel que le diagramme suivant est commutatif :*



4. *$\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 0$.*

Démonstration. Voir [23] Theorem 4.8 et Theorem 4.12 □

Pro-p-groupe abélien : structure de $\mathbb{Z}_p$-module

Soit G un pro-p-groupe abélien. Alors G possède une structure naturelle de $\mathbb{Z}_p$-module. En effet, on peut faire agir $\mathbb{Z}_p$ sur G de la façon suivante : soit $a = \lim_{n \to +\infty} a_n$ dans $\mathbb{Z}_p$ avec $a_n \in \mathbb{Z}$. Pour $g \in G$, on définit alors

$$g^a = \lim_{n \to +\infty} g^{a_n}$$

On vérifie alors que cette action définit bien une structure de $\mathbb{Z}_p$-module sur G. [1]

1. NB : cette action de $\mathbb{Z}_p$ peut-être définie pour tout pro-p-groupe, mais n'offre une structure de $\mathbb{Z}_p$-module que dans le cas où G est abélien.

1.2. Conjecture de Leopoldt

L'une des caractéristiques essentielle des corps de nombres dits *p-rationnels* est le fait que ceux-ci vérifie la conjecture de Leopoldt en p. Celle-ci peut-être considérée comme l'analogue p-adique du théorème des unités de Dirichlet.

1.2.1 Théorème des unités de Dirichlet

Théorème 1.2.1. *Le groupe U_K des unités (globales) de K est isomorphe au produit du groupe fini cyclique $\mu(K)$ des racines de l'unité de K et d'un groupe abélien libre de rang $r_1 + r_2 - 1$:*

$$U_K \simeq \mu(K) \times \mathbb{Z}^{r_1+r_2-1}$$

Plus précisément, si on pose $r = r_1 + r_2 - 1$, il existe des unités $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r$ telles que

1. *Le groupe $\mu(K)$ des racines de l'unité de K, d'ordre noté $w(K)$, est le groupe fini cyclique généré par ε_0 ;*
2. *Toute unité ε de K peut être écrite de manière unique sous la forme*

$$\varepsilon = \prod_{0 \leq i \leq r} \varepsilon_i^{n_i}$$

avec $0 \leq n_0 < w(K)$ et $n_i \in \mathbb{Z}$ pour $1 \leq i \leq r$.

Une telle famille $(\varepsilon_1, \ldots, \varepsilon_r)$ d'unités est appelée famille d'unité fondamentales de K.

Démonstration. On renvoie à [38] IV.4.4 Théorème 1, [31] Chap. I, §7, ou encore [26] Chap. 5, Theorem 38 pour une démonstration de ce résultat classique via la théorie de Minkowski. □

1.2.2 Rang p-adique des unités de K

Soit p un premier fixé. Pour toute place $\mathfrak{p} \in S_p$ ($\mathfrak{p}$ place de K au-dessus de p), on note

$K_\mathfrak{p}$ le complété de K en la place $\mathfrak{p}$;

$\mathcal{O}_\mathfrak{p}$ l'anneau des entiers de $K_\mathfrak{p}$;

$U_\mathfrak{p} = \mathcal{O}_\mathfrak{p}^\times$ le groupe des unités locales en $\mathfrak{p}$

$U_\mathfrak{p}^{(1)} = \{u \in U_\mathfrak{p} \,|\, u \equiv 1 \pmod{\mathfrak{p}\mathcal{O}_\mathfrak{p}}\}$ le sous-groupe associé des unités principales.

Le groupe des unités globales $U_K = \mathcal{O}_K^\times$ de K s'injecte diagonalement dans $\prod_{\mathfrak{p}|S_p} U_\mathfrak{p}$: on note $\Delta_p : U_K \longrightarrow \prod_{\mathfrak{p}|S_p} U_\mathfrak{p}$ ce plongement.

On considère alors

$$U'_K = \Delta_p(U_K) \cap \prod_{\mathfrak{p}|S_p} U_\mathfrak{p}^{(1)}$$

et $\overline{U'_K}$ l'adhérence de E' dans $\prod_{\mathfrak{p}|S_p} U_\mathfrak{p}^{(1)}$ pour la topologie produit.

Définition 1.2.2. On définit le rang p-adique des unités par

$$r_p := \mathrm{rang}_{\mathbb{Z}_p} \overline{U'_K}$$

Définition 1.2.3 (Conjecture de Leopoldt)**.** On dira que K satisfait à la conjecture de Leopoldt en p lorsque le rang p-adique des unités de K coïncide avec son $\mathbb{Z}$-rang, i.e. $r_p = r_1 + r_2 - 1$.

On notera $\delta = \delta_{K,p} = r_1 + r_2 - 1 - r_p \geq 0$ le défaut de la conjecture de Leopoldt. Dès lors, K satisfait la conjecture de Leopoldt en p lorsque $\delta = 0$.

1.2.3 Régulateur p-adique

Notons $\sigma_1, \ldots, \sigma_n$ les n plongements distincts de K dans $\mathbb{C}_p$. Soit $(\varepsilon_1, \ldots, \varepsilon_r)$ (avec $r = r_1 + r_2 - 1$) une famille d'unités fondamentales du corps de nombres K. On définit

$$\mathcal{R}_p(\varepsilon_1, \ldots, \varepsilon_r) := \begin{pmatrix} \log_p \sigma_1(\varepsilon_1) & \cdots & \log_p \sigma_n(\varepsilon_1) \\ \vdots & & \vdots \\ \log_p \sigma_1(\varepsilon_r) & \cdots & \log_p \sigma_n(\varepsilon_r) \end{pmatrix}$$

Proposition 1.2.4. *Le corps K satisfait la conjecture de Leopoldt en p si et seulement si le rang de la matrice $\mathcal{R}_p$ est égal maximal, i.e. égal $r = r_1 + r_2 - 1$.*

Remarque 1.2.5. Si K est totalement réel, la conjecture de Leopoldt pour K en p équivaut à la non-nullité de

$$R_p = \det \begin{pmatrix} \log_p \sigma_1(\varepsilon_1) & \cdots & \log_p \sigma_{n-1}(\varepsilon_1) \\ \vdots & & \vdots \\ \log_p \sigma_1(\varepsilon_{n-1}) & \cdots & \sigma_{n-1}(\varepsilon_r) \end{pmatrix}$$

appelé régulateur p-adique.

1.2.4 Corps de nombres abéliens

Bien qu'on ne dispose pas de démonstration de la conjecture de Leopoldt dans le cas général, on sait que :

Théorème 1.2.6 (Brumer [4])**.** *Soit $K/\mathbb{Q}$ une extension abélienne. Pour tout premier p, le corps K vérifie la conjecture de Leopoldt en p.*

Les corps considérés (multiquadratiques) à partir du chapitre 3 seront tous abéliens.

CHAPITRE 2

Corps p-Rationnels

2.1. Définitions préliminaires

2.1.1 Notations

Dans tout ce chapitre, on notera :

K un corps de nombres, i.e. une extension de $\mathbb{Q}$ de degré fini, $n = [K : \mathbb{Q}]$, $\mathcal{O}_K$ son anneau des entiers, et $U_K = (\mathcal{O}_K)^\times$,

p un nombre premier,

S_p l'ensemble des p-places de K, i.e. les places de K au-dessus de p,

S_r l'ensemble des places réelles de K, avec $|S_r| = r_1$,

S_c l'ensemble des places complexes de K, avec $|S_c| = r_2$.

On notera S un ensemble fini de places de K contenant S_p.

Les objets définis ci-après dépendent du corps K et du premier p : pour éviter une multiplication indigeste d'indices, cette dépendance n'apparaîtra pas explicitement dans les notations utilisées (à moins qu'une confusion puisse être à craindre).

On dira qu'une extension L/K est
— une *p-extension*, lorsque L/K est une extension finie galoisienne de degré une puissance de p.
— une *pro-p-extension*, lorsque L/K est une extension galoisienne dont le groupe de Galois est un pro-p-groupe.

— *S-ramifiée* lorsque les seules places de K ramifiées dans cette extension appartiennent à S, c'est-à-dire que L/K est non-ramifiée en dehors de S.
— *p-ramifiée* lorsqu'elle est S_p-ramifiée.

On note alors :

Ω_S l'extension algébrique S-ramifiée maximale de K,
et $\mathcal{G}_S = \mathrm{Gal}(\Omega_S/K)$.

$\Omega = \Omega_{S_p}$ l'extension algébrique p-ramifiée maximale de K,
et $\mathcal{G} = \mathcal{G}_{S_p} = \mathrm{Gal}(\Omega_{S_p}/K)$

M_S la pro-p-extension maximale de K contenue dans Ω_S,
i.e. la pro-p-extension S-ramifiée maximale de K,
et $G_S = \mathrm{Gal}(M_S/K)$.

$M = M_{S_p}$ la pro-p-extension p-ramifiée maximale de K,
et $G = G_{S_p} = \mathrm{Gal}(M_{S_p}/K)$.

M_S^{ab} la pro-p-extension abélienne maximale contenue dans Ω,
i.e. la pro-p-extension abélienne S-ramifiée maximale de K,
et $G_S^{\mathrm{ab}} = \mathrm{Gal}(M_S^{\mathrm{ab}}/K)$.

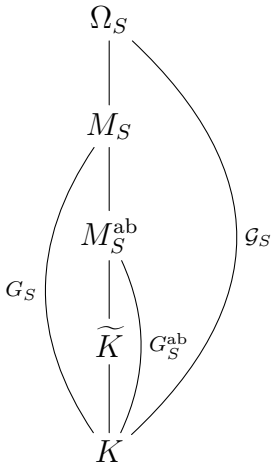
$M^{\mathrm{ab}} = M_{S_p}^{\mathrm{ab}}$ la pro-p-extension abélienne p-ramifiée maximale de K,
et $G^{\mathrm{ab}} = G_{S_p}^{\mathrm{ab}} = \mathrm{Gal}(M_{S_p}^{\mathrm{ab}}/K)$.

$\widetilde{K}$ le compositum de toutes les $\mathbb{Z}_p$-extensions de K.

Pour un corps L, on notera $\varepsilon(L) = \begin{cases} 1 & \text{si } \mu_p(L) \neq \{1\} \\ 0 & \text{si } \mu_p(L) = \{1\} \end{cases}$ et

$$\begin{aligned} V_S(K) &= \{x \in K^\times \,|\, \forall v \in S, x \in (K_v^\times)^p \text{ et } \forall v \notin S, x \in (K_v^\times)^p U_K\} \\ &= \{x \in K^\times \,|\, x \in (K_v^\times)^p, \forall v \in S \text{ et } (x) = \mathfrak{a}^p\} \end{aligned}$$

où $\mathfrak{a}$ désigne un idéal de K.



2.1.2 Structure de G^{ab}

La théorie du corps de classes, qui permet de décrire les extensions abéliennes d'un corps de nombres, offre la suite exacte suivante :

Proposition 2.1.1 ([14], p.236, III. 1.6.1 Corollary)**.**

$$1 \longrightarrow \overline{U'_K} \longrightarrow \prod_{\mathfrak{p}\in S_p} U_{\mathfrak{p}}^{(1)} \longrightarrow G^{\mathrm{ab}} \longrightarrow \mathcal{C}\ell_p \longrightarrow 1$$

On obtient donc :

Corollaire 2.1.2. *G^{ab} est un $\mathbb{Z}_p$-module de rang $1 + r_2 + \delta_K$.*

Démonstration. Il suffit de comparer les $\mathbb{Z}_p$-rangs dans cette suite exacte.

Puisque $\mathcal{C}\ell_p$ est fini, on a $\mathrm{rg}_{\mathbb{Z}_p}(\mathcal{C}\ell_p) = 0$.

Puisque, pour tout $\mathfrak{p} \in S_p$, on a $\mathrm{rg}_{\mathbb{Z}_p}\left(U_{\mathfrak{p}}^{(1)}\right) = [K_{\mathfrak{p}} : \mathbb{Q}_p]$, on a alors

$$\mathrm{rg}_{\mathbb{Z}_p}\left(\prod_{\mathfrak{p}\in S_p} U_{\mathfrak{p}}^{(1)}\right) = \sum_{\mathfrak{p}\in S_p} [K_{\mathfrak{p}} : \mathbb{Q}_p] = [K : \mathbb{Q}] = r_1 + 2r_2$$

On a donc

$$\begin{aligned}\mathrm{rg}_{\mathbb{Z}_p}(G^{\mathrm{ab}}) &= \mathrm{rg}_{\mathbb{Z}_p}\left(\prod_{\mathfrak{p}\in S_p} U_{\mathfrak{p}}^{(1)}\right) - r_p \\ &= (r_1 + 2r_2) - (r_1 + r_2 - 1 - \delta_K) \\ &= 1 + r_2 + \delta_K\end{aligned}$$

□

Ainsi, on a un isomorphisme de $\mathbb{Z}_p$-modules $G^{\mathrm{ab}} \simeq \mathbb{Z}_p^{1+r_2+\delta_K} \times T_K$, où δ_K est le défaut de la conjecture de Leopoldt de K en p et T_K est le sous-groupe de $\mathbb{Z}_p$-torsion de G^{ab}, laissant fixe le compositum $\widetilde{K}$ des $\mathbb{Z}_p$-extensions de K.

2.1.3 Corps p-rationnel : définition et critères équivalents

Théorème et Définition 2.1.3 (Corps p-rationnels)**.**
Les conditions suivantes sont équivalentes :

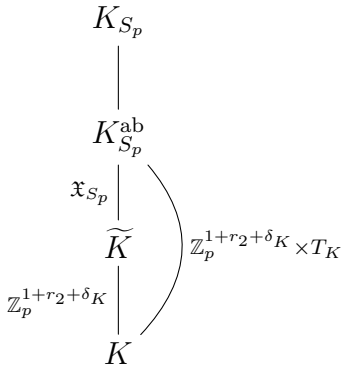
1. *K vérifie la conjecture de Leopoldt (i.e. $\delta_K = 0$) et $T_K = 0$.*
2. *$G^{\mathrm{ab}} = G_{S_p}^{\mathrm{ab}}$ est un $\mathbb{Z}_p$-module libre de rang $1 + r_2$.*
3. *$G = G_{S_p}$ est un pro-p-groupe libre sur $(1 + r_2)$ générateurs.*

4. $\varepsilon(K) = \sum_{v \in S_p} \varepsilon(K_v)$ *et* $V_{S_p}(K) = (K^\times)^p$.

   Si K *contient* μ_p, *la condition 4) équivaut alors à*

5. $\#S_p = 1$ *et* $\mathcal{C}\ell_{S_p}(K) = 0$.

Si K *vérifie l'une de ces conditions, on dira que* K *est* p*-rationnel.*



Démonstration. Voir [33] Théorème et Définition 2.1 □

Remarque. Lorsque $p \nmid h_K$, la condition $V_{S_p}(K) = (K^\times)^p$ équivaut à

$$\forall \varepsilon \in U_K, \quad \left[\forall \mathfrak{p} \in S_p, \varepsilon \in (K_\mathfrak{p})^p\right] \Rightarrow \varepsilon \in K^p$$

Démonstration. Supposons que $V_{S_p}(K) = (K^\times)^p$. Soit ε une unité de K tel que $\varepsilon \in (K_\mathfrak{p})^p$ pour tout $\mathfrak{p} \in S_p$. Puisque ε est une unité, $(\varepsilon) = \varepsilon\mathcal{O}_K = (\mathcal{O}_K)^p$. Donc $\varepsilon \in V_{S_p}(K) = (K^\times)^p$.

Réciproquement, supposons que : $\forall \varepsilon \in U_K$, $\left[\forall \mathfrak{p} \in S_p, \varepsilon \in (K_\mathfrak{p})^p\right] \Rightarrow \varepsilon \in K^p$. Soit $\alpha \in V_{S_p}(K)$. Alors $(\alpha) = \mathfrak{a}^p$: puisque $p \nmid h_K$, $\mathfrak{a}$ est principal. Il existe donc $\beta \in K$ tel que $\alpha\mathcal{O}_K = (\beta\mathcal{O}_K)^p = \beta^p\mathcal{O}_K$, i.e. $\varepsilon = \alpha\beta^{-p} \in U_K$. Pour tout $\mathfrak{p} \in S_p$, $\alpha \in (K_\mathfrak{p})^p$ donc $\varepsilon \in (K_\mathfrak{p})^p$. Donc $\varepsilon \in K^p$. Ainsi, $\alpha = \beta^p\varepsilon \in K^p$. On a donc montré que $V_{S_p}(K) = (K^\times)$. □

On dispose également de la caractérisation suivante de la p-rationalité, due à T. Nguyen Quand Do :

Proposition 2.1.4. *Un corps de nombres* K *est* p*-rationnel si et seulement si les trois propositions suivantes sont vérifiées :*

1. *le* p*-corps de classes de Hilbert de* K *est inclus dans* $\widetilde{K}$.
2. *l'application naturelle* $\mu_p(K) \to \bigoplus_{v|p} \mu_p(K)$ *est un isomorphisme.*
3. *l'application naturelle* $U_K/(U_K)^p \to \bigoplus_{v|p} U_v/(U_v)^p$.

Démonstration. [35] Appendix A ou [5] Proposition 2.3.1 □

2.2. Montée et Descente de la p-rationalité

2.2.1 Descente de la p-rationalité

Proposition 2.2.1. *Si K est p-rationnel, alors tout ses sous-corps sont p-rationnels.*

Démonstration. [14] IV. 3.4.5 (iii) ou [28] Proposition 5 □

Cette propriété découle, dans [14], du principe suivant :

Si L/K est une extension de corps de nombres, notons M_K^{ab} (resp. M_L^{ab}) la pro-p-extension p-ramifiée abélienne maximale de K (resp. de L), et T_K (resp. T_L) le sous-groupe de $\mathbb{Z}_p$-torsion de M_K^{ab} (resp. M_L^{ab}).

L'application $j_{L/K} : \mathcal{I}_K \longrightarrow \mathcal{I}_L$ d'extension des idéaux de K vers L induit (cf. [14] IV.2) une application

$$j : M_K^{\mathrm{ab}} \longrightarrow M_L^{\mathrm{ab}}$$

Or, si on suppose que la conjecture de Leopoldt est vérifiée en p pour la clôture galoisienne de L sur K, alors l'application $j : M_K^{\mathrm{ab}} \longrightarrow M_L^{\mathrm{ab}}$ est injective. En particulier, T_L contient un sous-groupe isomorphe à T_K.

2.2.2 Montée de la p-rationalité dans une p-extension

Miki et Sato (cf. [25] et [27]) ont montré que, dans une p-extension L/K de corps de nombres tel que K vérifie la conjecture de Leopoldt en p, L vérifie également la conjecture de Leopoldt en p si les deux conditions suivantes sont vérifiées : (i) K est p-rationnel et (ii) l'ensemble des places de K divisant p ou ramifiées dans L/K est *primitif* pour le couples (K, p). Movahhedi (d'un coté) et Gras-Jaulent (d'un autre côté), ont généralisé séparément ce résultat, et ont montré que ces deux propriétés étaient alors hérités par L.

Les résultats de cette section sont principalement tirés de [30]. Rappelons que K est un corps de nombres, p un premier, et $\widetilde{K}$ désigne le compositum de toutes les $\mathbb{Z}_p$-extensions de K. Suivant [30], notons $\widetilde{K}(1)$ la sous-extension élémentaire maximale de $\widetilde{K}$, c'est-à-dire le compositum des premiers étage des $\mathbb{Z}_p$-extensions de K. Soit S un ensemble de places de K contenant S_p, et notons : $T = S \backslash S_p$, $t = \mathrm{card}(T)$ et $\widetilde{K}(1, T)$ le sous-corps de $\widetilde{K}(1)$ décomposant totalement toutes les places de T.

Proposition 2.2.2 ([30] Proposition et Definition 3.1)**.**
Les conditions suivantes sont équivalentes :

1. *Les Frobenius σ_ℓ de* $\mathrm{Gal}(\widetilde{K}/K)$ *(i.e. les symboles d'Artin $(\ell, \widetilde{K}/K)$ pour $\ell \in T$, engendrent un $\mathbb{Z}_p$-facteur direct libre de* $\mathrm{Gal}(\widetilde{K}/K)$*, de rang égal à t.*
2. *Les Frobenius σ_ℓ^1 de* $\mathrm{Gal}(\widetilde{K}(1)/K)$ *(i.e. les symboles d'Artin $(\ell, \widetilde{K}(1)/K)$ pour $\ell \in T$, engendrent un sous-$\mathbb{F}_p$-espace vectoriel de* $\mathrm{Gal}(\widetilde{K}(1)/K)$*, de dimension égale à t.*
3. $\dim \mathrm{Gal}(\widetilde{K}(1)/\widetilde{K}(1,T)) = t$

Si l'une de ces conditions est vérifiée, on dit que l'ensemble S est primitif (pour K et p).

Définition 2.2.3. Une p-extension L/K (i.e. une extension galoisienne finie dont le groupe de Galois est un p-groupe) est appelée *primitivement ramifiée* si l'ensemble S des p-places de K et des places finies de K qui se ramifie dans L, est primitif (pour p et K).

Théorème 2.2.4. *Soit L/K une p-extension de corps de nombres. Les conditions suivantes sont équivalentes :*

1. *L est un corps p-rationnel.*
2. *K est un corps p-rationnel et l'extension L/K est primitivement ramifiée.*

Démonstration. [33] Théorème 3.7 □

Remarque 2.2.5. La montée de la p-rationalité dans une extension L/K est donc totalement déterminée par le comportement des places ramifiées et des p-places *lorsque L/K est une p-extension*. La situation se complexifie nettement dès lors que l'on souhaite étudier la montée de la p-rationalité dans une extension dont le degré n'est plus une puissance de p : c'est le cas en particulier dans la suite.

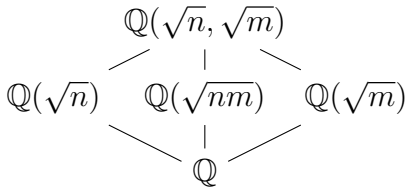
2.2.3 Critère de p-rationalité impliquant les sous-corps

Proposition 2.2.6. *Si K est une extension finie abélienne de $\mathbb{Q}$ et $[K : \mathbb{Q}]$ n'est pas divisible par p, alors K est p-rationnel si et seulement si toute extension cyclique de $\mathbb{Q}$ contenue dans K est p-rationnel.*

Démonstration. [18] Prop. 3.6 □

Corollaire 2.2.7. *Si K est un corps multiquadratique (*$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^t$ *pour $t \geq 1$) et $p \neq 2$, alors K est p-rationnel si et seulement si tous les sous-corps quadratiques de K sont p-rationnels.*

Remarque importante. Soit $\mathbb{Q}(\sqrt{n})$ et $\mathbb{Q}(\sqrt{m})$ deux corps quadratiques distincts ($m, n \in \mathbb{Z}-\{0,1\}$, $m \neq n$, sans facteur carré) et soit $p \neq 2$ premier. Il ne suffit pas que $\mathbb{Q}(\sqrt{n})$ et $\mathbb{Q}(\sqrt{m})$ soit p-rationnels pour que leur compositum $\mathbb{Q}(\sqrt{n}, \sqrt{m})$ le soit. Il faut également que $\mathbb{Q}(\sqrt{nm})$ soit p-rationnel pour obtenir le p-rationalité du compositum.



Contre-Exemple : Les corps quadratiques $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{19})$ sont 5-rationnels. Pourtant, leur compositum $\mathbb{Q}(\sqrt{2}, \sqrt{19})$ n'est pas 5-rationnel, car son sous-corps quadratique $\mathbb{Q}(\sqrt{38})$ ne l'est pas.

2.3. Conjecture de Greenberg

En 2016, R. Greenberg s'empare de la notion de corps p-rationnel dans [18] et s'en sert pour construire des représentations de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ vers $\mathrm{GL}_n(\mathbb{Z}_p)$. Cette construction repose sur une conjecture particulière, que nous appellerons dans la suite « conjecture de Greenberg » :

Conjecture 2.3.1 ([18] Greenberg)**.** *Pour tout nombre premier p, et pour tout $t \in \mathbb{N}$, $t \neq 0$, il existe un corps de nombres p-rationnel dont le groupe de Galois sur $\mathbb{Q}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^t$.*

Un corps de nombres dont le groupe de Galois sur $\mathbb{Q}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^t$ sera appelé « corps multiquadratique ».

Dans la suite, on dira que $G(t,p)$ est vérifiée s'il existe un corps de nombres multiquadratique p-rationnel de degré 2^t.

On dira également que $G_\infty(t,p)$ est vérifiée s'il existe une *infinité* de corps de nombres multiquadratiques p-rationnels de degré 2^t.

2.3.1 Corps quadratiques p-rationnels

Le cas des corps quadratiques représente le cas élémentaire de la conjecture de Greenberg ($t = 1$). Nous verrons ci-après que $G_\infty(1,p)$ est vérifiée pour tout p : quelque soit le nombre premier p, il existe une infinité de corps quadratiques p-rationnels.

Plus précisément, il est possible de montrer qu'il existe – d'un côté – une infinité de corps quadratiques p-rationnels *totalement réels*, et – d'un autre côté – une infinité de corps quadratiques p-rationnels *imaginaires*.

Corps quadratiques : critères spécifiques

On possède certains critères spécifiques de p-rationalité pour le cas particulier des corps quadratiques. Spécifiquement, on utilisera les critères suivants :

Proposition 2.3.2. *Soit K un corps quadratique et p premier tel que : soit $p \geq 5$, soit $p = 3$ et p n'est pas ramifiée dans $K/\mathbb{Q}$. Alors :*

1. *Supposons K imaginaire. Dans ce cas, K est p-rationnel si et seulement si son p-corps de classes de Hilbert est contenue dans sa $\mathbb{Z}_p$-extension anti-cylotomique. En particulier, si h_K n'est pas divisible par p, alors K est p-rationnel.*
2. *Supposons K totalement réel. Dans ce cas, K est p-rationnel si et seulement si*
   (a) *h_K n'est pas divisible par p*
   (b) *et l'unité fondamentale ε_0 de K n'est pas une puissance p-ième dans le complété K_v, pour au moins une p-place v.*

Démonstration. [18] Prop. 4.1 □

Remarque 2.3.3. Pour $p \geq 5$, puisque la condition $p \nmid h_K$ est une condition suffisante de p-rationalité dans le cas quadratique imaginaire. On en déduit que tout corps quadratique imaginaire est p-rationnel pour presque tout p.

Pour traiter le cas particulier d'un corps quadratique totalement réel K, il est possible d'employer un critère équivalent faisant intervenir le régulateur p-adique de K. Plus précisément :

Proposition 2.3.4. *Soit K un corps de nombres quadratique totalement réel, et p un nombre premier supérieur ou égal à 5. Notons R_p le régulateur p-adique de K. Alors K est p-rationnel si et seulement si les deux conditions suivantes sont vérifiées :*

1. *p ne divise pas le nombre de classes h_K*
2. $v_p(R_p) = \begin{cases} \frac{1}{2} & \text{si } p \text{ ramifié dans } K \\ 1 & \text{si } p \text{ non-ramifié dans } K \end{cases}$

Démonstration. Si K est un corps de nombres totalement réel, K vérifie la conjecture de Leopoldt en p précisément lorsque son régulateur p-adique R_p est non-nul. Dès lors, si $R_p \neq 0$, une formule démontrée par Coates ([9] Appendix, Lemma 8) lie le cardinal de T_K (qui est alors un

p-groupe fini) avec R_p : le cardinal de T_K est égal (à multiplication par une unité p-adique près) à :

$$|\mu_{p^\infty} \cap K(\mu_p)| \frac{h_K R_p}{\sqrt{d_K}} \prod_{v|p}(1-(Nv)^{-1})$$

Dans le cas particulier où K est un corps quadratique totalement réel, avec $p \geq 5$, on a alors :

$$v_p\left(|\mu_{p^\infty} \cap K(\mu_p)|\right) = 1$$

$$v_p\left(\sqrt{d_K}\right) = \begin{cases} 0 & \text{si } p \text{ est non-ramifié dans } K \\ 1/2 & \text{si } p \text{ est ramifié dans } K \end{cases}$$

$$v_p\left(\prod_{v|p}(1-(Nv)^{-1})\right) = \begin{cases} v_p\left(1-\frac{1}{p}\right) = -1 & \text{si } p \text{ ramifié dans } K \\ v_p\left((1-\frac{1}{p})^2\right) = -2 & \text{si } p \text{ totalement décomposé dans } K \\ v_p\left(1-\frac{1}{p^2}\right) = -2 & \text{si } p \text{ inerte dans } K \end{cases}$$

On obtient donc

$$v_p(T_K) = 1 + v_p(h_K) + v_p(R_p) + \begin{cases} -2 & \text{si } p \text{ non-ramifié dans } K \\ -\frac{3}{2} & \text{si } p \text{ ramifié dans } K \end{cases}$$

□

Valuation p-adique du nombre de classes

Dans le cas particulier où l'on souhaite déterminer la p-rationalité d'une famille de corps de nombres, il est parfois difficile d'obtenir des informations précises sur le comportement du nombre de classes pour cette famille de corps. Heureusement, seule la valuation p-adique du nombre de classes nous intéressera. Il est alors possible de vérifier indirectement que p ne divise pas h_K en majorant h_K par une quantité strictement inférieure à p. Pour cela, on fera usage de l'estimation suivante :

Proposition 2.3.5 ([24], Prop. 2)**.** *Soit L un corps quadratique. Alors*

$$\kappa_L \leq \frac{1}{2}(\log d_L + \mu_L)$$

où $\kappa_L = \lim_{s\to 1}(s-1)\zeta_L(s)$ est le résidu de la fonction ζ_L en $s=1$, $d_L = |\mathrm{disc}(L)|$ et

$$\mu_L = \begin{cases} 2+\gamma-\log(4\pi) & \textit{si } L \textit{ est totalement réel} \\ 2+\gamma-\log(\pi) & \textit{si } L \textit{ est imaginaire} \end{cases}$$

Si L est un corps quadratique imaginaire, il suffit d'associer la précédente proposition à la formule du nombre de classes

$$\kappa_L = \frac{2\pi h_K}{w_K\sqrt{d_L}}$$

pour obtenir :

Proposition 2.3.6. *Soit L un corps quadratique imaginaire.*
On note $d_L = |\mathrm{disc}(L)|$. On a :

$$h_L \leq \frac{w_L \cdot \sqrt{d_L}}{4\pi}(\log(d_L) + 2 + \gamma - \log(\pi))$$

où

$$w_L = \begin{cases} 6 & si\ d = 3 \\ 4 & si\ d = 4 \\ 2 & si\ d \geq 5 \end{cases}$$

et γ est la constante d'Euler.
De plus, on $2 + \gamma - \log(\pi) \leq \frac{3}{2}$.

Corps quadratiques imaginaires

Muni de la condition suffisante de p-rationalité évoquée précédemment, on peut utiliser le résultat suivant :

Théorème 2.3.7 ([20] Hartung)**.** *Soit p premier impair. Il existe une infinité de corps quadratiques imaginaires dont le nombre de classes n'est pas divisible par p.*

Remarque 2.3.8. Hartung ne prouve le théorème précédent que dans le cas $p = 3$. Mais la méthode est généralisable à tout p premier impair.

En appliquant la proposition 2.3.2 et le théorème 2.3.7, on obtient :

Corollaire 2.3.9. *Pour tout $p \geq 5$ premier, il existe une infinité de corps quadratiques imaginaires p-rationnels. Autrement dit, $G_\infty(1, p)$ est vérifiée pour tout $p \geq 5$.*

Corps quadratiques totalement réels

Le cas totalement réel s'avère d'une bien plus grande difficulté que le cas imaginaire. La p-rationalité d'un corps de nombres est liée de manière intrinsèque au comportement local (en p) des unités.

La littérature offre des exemples de corps p-rationnels. On citera tout d'abord certains résultats de D. Byeon, datant de 2000, qui offre des exemples de famille de corps p-rationnels totalement réels :

Théorème 2.3.10 ([8], Prop. 3.1)**.** *Soit un premier $p > 3$ et soit D le discriminant fondamental du corps quadratique totalement réel $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{p^2+4})$. Alors :*

1. $\left(\frac{D}{p}\right) = 1$, *i.e. p se décompose totalement dans $\mathbb{Q}(\sqrt{D})$.*
2. $h(D) \not\equiv 0 \mod p$
3. $|R_p(D)|_p = \frac{1}{p}$

Théorème 2.3.11 ([8], Prop. 3.1)**.** *Soit un premier $p > 3$, $p \equiv 3 \mod 4$, et soit D le discriminant fondamental du corps quadratique totalement réel $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{p^2-1})$. Alors :*

1. $\left(\frac{D}{p}\right) = -1$, *i.e. p reste inerte dans $\mathbb{Q}(\sqrt{D})$.*
2. $h(D) \not\equiv 0 \mod p$
3. $|R_p(D)|_p = \frac{1}{p}$

Corollaire 2.3.12. *Pour tout premier $p > 3$, le corps quadratique réel $\mathbb{Q}(\sqrt{p^2+4})$ est p-rationnel.*

Corollaire 2.3.13. *Pour tout premier $p > 3$, $p \equiv 3 \mod 4$, le corps quadratique réel $\mathbb{Q}(\sqrt{p^2-1})$ est p-rationnel.*

Plus généralement, les résultats de [8] offre, pour p premier fixé, une infinité de corps quadratiques p-rationnels.

D'autres corps quadratiques totalement réels particuliers nous serons spécialement utile dans la suite.

Proposition 2.3.14 ([6] Prop. 4.4)**.** *Pour tout premier $p \geq 5$, les corps quadratiques totalement réels*

$$\mathbb{Q}\left(\sqrt{p(p-2)}\right), \quad \mathbb{Q}\left(\sqrt{p(p+2)}\right) \quad \textit{et} \quad \mathbb{Q}\left(\sqrt{(p-2)(p+2)}\right)$$

sont p-rationnels.

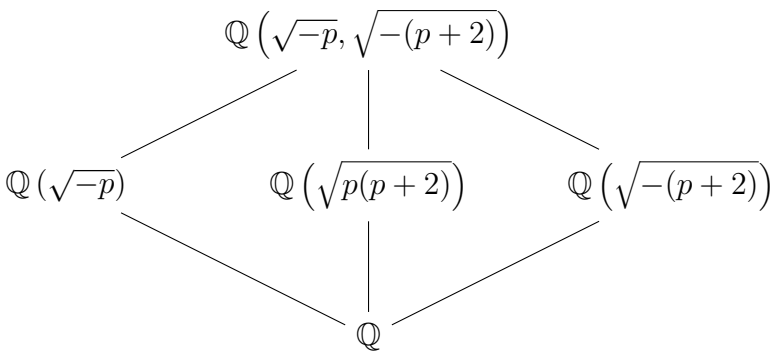
La démonstration de ce résultat repose en grande partie sur le fait que ces familles de corps quadratiques totalement réels admettent des unités fondamentales dont une expression relativement simple peut être donnée. Par exemple, l'unité fondamentale du corps $\mathbb{Q}\left(\sqrt{p(p+2)}\right)$ s'exprime simplement sous la forme $\varepsilon = p + 1 + \sqrt{p(p+2)}$.

2.3.2 Corps biquadratiques p-rationnels

Corollaire 2.3.15. *Pour tout $p \neq 3$, le corps biquadratique*

$$\mathbb{Q}\left(\sqrt{-p}, \sqrt{-(p+2)}\right)$$

est p-rationnel.



Démonstration. En effet, $\mathbb{Q}\left(\sqrt{p(p+2)}\right)$ est p-rationnel par la proposition précédente. De même, $\mathbb{Q}\left(\sqrt{-p}\right)$ et $\mathbb{Q}\left(\sqrt{-(p+2)}\right)$ sont p-rationnels car leur nombre de classes n'est pas divisible par p. Pour le montrer, il suffit de vérifier que, pour tout $p \geq 5$, on a

$$\frac{\sqrt{4p}}{2\pi}\left(\log(4p) + \frac{1}{2}\right) < p \quad \text{et} \quad \frac{\sqrt{4(p+2)}}{2\pi}\left(\log(4(p+2)) + \frac{1}{2}\right) < p+2$$

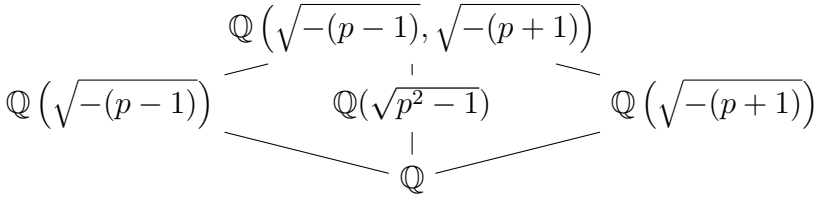
□

De même, on a

Proposition 2.3.16. *Pour tout $p \equiv 3 \mod 4$, le corps biquadratique*

$$\mathbb{Q}\left(\sqrt{-(p-1)}, \sqrt{-(p+1)}\right)$$

est p-rationnel.

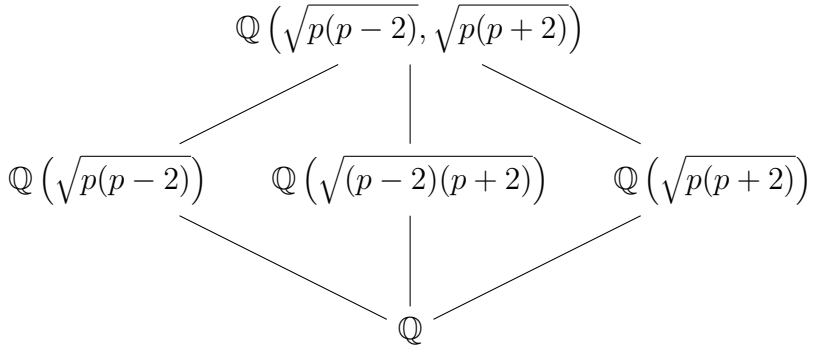


Suivant le même principe, Y. Benemerieme et A. Movahhedi sont parvenus à exhiber corps biquadratique totalement réel suivant :

Proposition 2.3.17 ([6] Prop. 4.4)**.** *Pour tout premier $p \geq 5$, le corps biquadratique totalement réel*

$$\mathbb{Q}\left(\sqrt{p(p-2)}, \sqrt{p(p+2)}\right)$$

est p-rationnel.



Remarque 2.3.18. On montrera au chapitre 4 que, lorsqu'on adjoint une racine carré de -1 à ce corps biquadratique, on obtient un corps triquadratique qui est p-rationnel pour une infinité de premiers p.

CHAPITRE 3

Etude de cas : $\mathbb{Q}(\sqrt{p})$

Introduction Nous avons vu au chapitre précédent que l'étude de la p-rationalité d'un corps quadratique est bien plus complexe dans le cas d'un corps quadratique totalement réel que dans le cas imaginaire. Pour p fixé, on ne connait que peu de corps quadratique totalement réel dont on peut démontrer la p-rationalité. La difficulté principale est à trouver au niveau des unités. C'est la raison pour laquelle on se propose ci-après d'étudier le cas particulier de $\mathbb{Q}(\sqrt{p})$. Dans [6], les auteurs se posent la question de la p-rationalité de ces corps quadratiques totalement réels. Ils remarquent que l'étude de la p-rationalité de $\mathbb{Q}(\sqrt{p})$ se ramène à l'étude de son unité fondamentale.

Dans la suite, on fixe un nombre premier p ($p \equiv 3 \pmod 4$ à partir de la section 2), et on note $K = \mathbb{Q}(\sqrt{p})$.

3.1. Critère de p-rationalité

On montrera d'abord que le nombre de classes de K n'est pas divisible par p, avant de dégager un critère de p-rationalité dans le cas où $p \equiv 3 \pmod 4$. En particulier, on montrera que la p-rationalité de $\mathbb{Q}(\sqrt{p})$, dans le cas $p \equiv 3 \pmod 4$, se ramène à une propriété arithmétique simple concernant les coefficients de l'unité fondamentale dans la base $(1, \sqrt{p})$.

3.1.1 Valuation p-adique du nombres de classes

Rappelons que, pour K un corps quadratique totalement réel, la non-divisibilité par p du nombre de classes h_K est une condition nécessaire pour que K soit p-rationnel.

Afin de montrer que p ne divise pas le nombre de classes de $\mathbb{Q}(\sqrt{p})$, on va montrer que $h_{\mathbb{Q}(\sqrt{p})} < p$. Pour cela, on peut utiliser la proposition suivante, qui est un corollaire de la proposition 2.3.5 :

Proposition 3.1.1. *Soit L un corps quadratique totalement réel de discriminant d_L et d'unité fondamentale ε. On a*

$$h_L \leq \frac{\sqrt{d_L}}{4 \cdot \log(\varepsilon)}(\log(d_L) + \mu_L)$$

Démonstration. Pour un corps quadratique totalement réel, la formule du nombre de classes et la proposition 2.3.5 donnent

$$\frac{2 \cdot \mathrm{Reg}_L \cdot h_L}{\sqrt{d_L}} = \lim_{s \to 1}(s-1)\zeta_K(s) \leq \frac{1}{2}(\log(d_L) + \mu_L)$$

avec $\mu_L = 2 + \gamma - \log(4\pi) = 0.04619\ldots$

Donc

$$h_L \leq \frac{\sqrt{d_L}}{4 \cdot \mathrm{Reg}_L}(\log(d_L) + \mu_L)$$

avec $\mathrm{Reg}_L = \log(\varepsilon)$ et $\mu_L \leq 1/10$. □

On en déduit :

Proposition 3.1.2. *Pour tout $p \neq 2$ premier, le nombre de classes de $\mathbb{Q}(\sqrt{p})$ n'est pas divisible par p.*

Démonstration. Soit p premier impair.

On note : $K = \mathbb{Q}(\sqrt{p})$, et $d_K = \mathrm{disc}(K)$.

On a $d_K \leq 4p$, $\varepsilon > \frac{\sqrt{p}}{2}$, et ε l'unité fondamentale de K.

Par la proposition précédente, on a donc :

$$h_K \leq \frac{\sqrt{4p}}{4 \cdot \log(\frac{\sqrt{p}}{2})}(\log(4p)+\mu_L) \leq \frac{2\sqrt{p}}{2\log\left(\frac{p}{4}\right)}(\log(4p)+1) = \sqrt{p} \cdot \frac{\log(4p)+1}{\log(\frac{p}{4})}$$

avec $\dfrac{\log(4p)+1}{\log\left(\frac{p}{4}\right)} < \sqrt{p}$ pour $p \geq 17$.

Donc $h_K < p$ pour $p \geq 17$ et on peut vérifier à part que, pour $p = 3, 5, 7, 11, 13$, $h_K = 1$.

□

3.1.2 Valuation du régulateur p-adique

Puisque le nombre de classe de $\mathbb{Q}(\sqrt{p})$ n'est pas divisible par p, la p-rationalité de ce corps de nombres peut être déterminé à partir d'une unité fondamentale. Plus précisément, on peut déterminer la p-rationalité de $\mathbb{Q}(\sqrt{p})$ en déterminant la valuation p-adique de son régulateur p-adique. L'intérêt pratique à étudier spécialement le corps de nombres $\mathbb{Q}(\sqrt{p})$ tient au fait qu'il est possible d'obtenir dans ce cas un certain nombre d'informations sur la forme de son unité fondamentale en fonction du nombre premier p.

On se place uniquement dans le cas $p \equiv 3 \pmod 4$, où l'anneau des entiers de $\mathbb{Q}(\sqrt{p})$ est simplement $\mathbb{Z}[\sqrt{p}]$.

Nous allons d'abord montrer la proposition suivante :

Proposition 3.1.3. *Soit p premier, $p \equiv 3 \pmod 4$. Soit $K = \mathbb{Q}(\sqrt{p})$ et $u \in U_K$ une unité de K de norme 1. Alors u est d'une des deux formes suivantes :*

1. *Soit il existe $k \in \mathbb{Z}$, $k \neq 0$, tel que $k(kp+2)$ est un carré et*

$$u = kp + 1 \pm \left(k(kp+2)\right)^{1/2} \sqrt{p}$$

2. *Soit il existe $k \in \mathbb{Z}$, $k \neq 0$, tel que $k(kp-2)$ est un carré et*

$$u = kp - 1 \pm \left(k(kp-2)\right)^{1/2} \sqrt{p}$$

Démonstration. Soit $u = x + y\sqrt{p}$ (avec $x, y \in \mathbb{Z}$) une unité de K de norme 1. Alors on a : $N(u) = x^2 - py^2 = 1$, i.e. $(x-1)(x+1) = py^2$.

— Premier cas : si p divise $x-1$, il existe $k \in \mathbb{Z}$ tel que $x = kp+1$, et on obtient $y^2 = \dfrac{(x-1)(x+1)}{p} = \dfrac{kp(kp+2)}{p} = k(kp+2)$.
On a alors : $u = kp + 1 \pm \left(k(kp+2)\right)^{1/2} \sqrt{p}$.

— Deuxième cas : si p divise $x+1$, il existe $k \in \mathbb{Z}$ tel que $x = kp-1$, et on obtient $y^2 = \dfrac{(x-1)(x+1)}{p} = \dfrac{(kp-2)kp}{p} = k(kp-2)$.
On a alors : $u = kp - 1 \pm \left(k(kp-2)\right)^{1/2} \sqrt{p}$.

□

Remarque 3.1.4. Si u est une unité de norme 1 de la forme $u = kp+1 \pm (k(kp+2))^{1/2}\sqrt{p}$, remarquons que $k(kp+2) = -k(-kp-2)$. Alors, si on pose $k' = -k$, on a $-u = k'p - 1 \mp (k'(k'p-2))^{1/2}\sqrt{p}$.

Proposition 3.1.5. *Soit p premier, $p \equiv 3 \pmod 4$. Soit $K = \mathbb{Q}(\sqrt{p})$ et $\varepsilon > 1$ l'unité fondamentale de K. Alors :*

1. *Si* $p \equiv 7 \pmod 8$*, il existe* $k \in \mathbb{N}^*$ *un carré tel que* $kp+2$ *est un carré et*
$$\varepsilon = kp + 1 + (k(kp+2))^{1/2}\sqrt{p}$$
2. *Si* $p \equiv 3 \pmod 8$*, il existe* $k \in \mathbb{N}^*$ *un carré tel que* $kp-2$ *est un carré et*
$$\varepsilon = kp - 1 + (k(kp-2))^{1/2}\sqrt{p}$$

Démonstration. Puisque $p \equiv 3 \pmod 4$, une unité fondamentale de K est nécessairement de norme 1 (cf. [34] Corollaire 3.3). Ainsi, l'unité fondamentale ε de K est nécessairement d'une des deux formes précédentes. Puisque $\varepsilon = x + y\sqrt{p}$ avec $x, y > 0$, on nécessairement $k > 0$.

Dans les deux cas, on peut remarquer que k est soit un carré, soit deux fois un carré : en effet, le seul facteur premier commun possible de k et $kp+2$ (resp. k et $kp-2$) est 2. On peut montrer que, s'il s'agit de deux fois un carré, alors ε est lui-même le carré d'une unité de K, ce qui ne peut advenir puisque ε est une unité fondamentale.

— Premier cas : Supposons que $\varepsilon = kp + 1 + [k(kp+2)]^{1/2}\sqrt{p}$ avec $k = 2b^2$. Alors $kp+2 = (2b^2p+2) = 2(b^2p+1)$ est aussi deux fois un carré, i.e b^2p+1 est un carré : notons $a^2 = b^2p+1$. Dès lors, $a + b\sqrt{p}$ est une unité de K (de norme 1), et on a

$$\begin{aligned}\varepsilon &= 1 + 2b^2p + \left[2b^2(2b^2p+2)\right]^{1/2}\sqrt{p} \\ &= a^2 - b^2p + 2b^2p + \left[4b^2(b^2p+1)\right]^{1/2}\sqrt{p} \\ &= a^2 + b^2p + \left[4b^2a^2\right]^{1/2}\sqrt{p} \\ &= (a + b\sqrt{p})^2\end{aligned}$$

— Deuxième cas : Supposons que $\varepsilon = kp-1+[k(kp-2)]^{1/2}\sqrt{p}$ avec $k = 2b^2$. Alors $kp-2 = 2b^2p-2 = 2(b^2p-1)$ est aussi deux fois un carré, donc b^2p-1 est un carré : notons $a^2 = b^2p-1$. Alors $a + b\sqrt{p}$ est une unité de K (de norme -1). Alors on a :

$$\begin{aligned}\varepsilon &= 2b^2p - 1 + \left[2b^2(2b^2p-2)\right]^{1/2}\sqrt{p} \\ &= 2b^2p + a^2 - b^2p + \left[4b^2(b^2p-1)\right]^{1/2}\sqrt{p} \\ &= a^2 + b^2p + \left[4b^2a^2\right]^{1/2}\sqrt{p} \\ &= (a + b\sqrt{p})^2\end{aligned}$$

Ainsi, $k \in \mathbb{N}^*$ est bien un carré, et on en déduit que $kp+2$ (dans le premier cas) ou $kp-2$ (dans le deuxième cas) est également un carré.

Reste à montrer que chacune de ces décompositions advient en fonction du résidu de p modulo 8. Or, on sait que ce résidu gouverne la décomposition du premier p dans les corps quadratiques $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{-2})$; plus précisément, on a :

Lemme 3.1.6. *Soit p un premier impair.*

Dans $\mathbb{Q}(\sqrt{2})$, le premier p reste inerte si $p \equiv 3$ ou $5 \pmod 8$, et est totalement décomposé si $p \equiv 1$ ou $7 \pmod 8$.

Dans $\mathbb{Q}(\sqrt{-2})$, le premier p reste inerte si $p \equiv 5$ ou $7 \pmod 8$, et est totalement décomposé si $p \equiv 1$ ou $3 \pmod 8$.

Si $p \equiv 7 \pmod 8$, alors on retrouve le premier cas (cas p décomposé dans $\mathbb{Q}(\sqrt{2})$). Si $p \equiv 3 \pmod 8$, alors on retrouve le deuxième cas (cas p inerte dans $\mathbb{Q}(\sqrt{2})$).

En effet, si on se trouve dans le premier cas, alors $kp+2$ est un carré : on a $kp + 2 = y^2$, d'où $(y - \sqrt{2})(y + \sqrt{2}) = kp$.

On a $N\left((y + \sqrt{2})\mathcal{O}_{\mathbb{Q}(\sqrt{2})}\right) = \left|N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(y + \sqrt{2})\right| = y^2 - 2 = kp$

et $N\left((y - \sqrt{2})\mathcal{O}_{\mathbb{Q}(\sqrt{2})}\right) = \left|N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(y - \sqrt{2})\right| = y^2 - 2 = kp$

On est donc dans le cas où p se décompose dans $\mathbb{Q}(\sqrt{2})$, donc $p \equiv 7 \pmod 8$ (rappelons qu'on a supposé que $p \equiv 3 \pmod 4$).

Si on est dans le deuxième cas, alors $kp - 2 = y^2$ est un carré,

et alors $kp = (y - \sqrt{-2})(y + \sqrt{-2})$, et on en déduit de la même façon que p est décomposé dans $\mathbb{Q}(\sqrt{-2})$, donc $p \equiv 3 \pmod 8$.

□

Dès lors, on peut montrer les propositions suivantes :

Proposition 3.1.7. *Soit p un premier, $p \equiv 7 \pmod 8$. On note $K = \mathbb{Q}(\sqrt{p})$, et ε l'unité fondamentale de K. On a*

$$\varepsilon = kp + 1 + (k(kp + 2))^{1/2} \sqrt{p}$$

avec $k \in \mathbb{N}$ un carré tel que $kp + 2$ est un carré.

Alors K est p-rationnel si et seulement si k n'est pas divisible par p.

Démonstration. On a montré que le nombre de classes de K n'était pas divisible par p. Dès lors, on sait que K est p-rationnel si et seulement si $v_p(\log_p(\varepsilon)) = \frac{1}{2}$ (car p se ramifie dans K). Soit $\mathfrak{p} = \sqrt{p}\mathcal{O}_K$ l'unique idéal de K au-dessus de p. Soit $x \in K_{\mathfrak{p}}$. On sait que, dès que $v_p(x) > \frac{1}{p-1}$, alors $v_p\left(\log_p(1 + x)\right) = v_p(x)$. (voir [11] Prop. 4.2.10)

D'où K est p-rationnel si et seulement si $v_p\left(kp + (k(kp + 2))^{1/2}\sqrt{p}\right) = \frac{1}{2}$. Cela est vérifié si et seulement si $k(kp + 2)$ n'est pas divisible par p, c'est-à-dire si p ne divise pas k. □

Proposition 3.1.8. *Soit p un premier, $p \equiv 3 \pmod 8$. On note $K = \mathbb{Q}(\sqrt{p})$, et ε l'unité fondamentale de K. On a*

$$\varepsilon = kp - 1 + (k(kp-2))^{1/2}\sqrt{p}$$

avec $k \in \mathbb{N}$ un carré tel que $kp-2$ est un carré.

Alors K est p-rationnel si et seulement si k n'est pas divisible par p.

Démonstration. On peut procéder de la même façon que précédemment en reconnaissant que, si $k' = -k$, alors

$$\varepsilon' = -\varepsilon = k'p + 1 - (k'(k'p+2))^{1/2}\sqrt{p}$$

est aussi *une* unité fondamentale de K. Alors, de la même façon que précédemment, la p-rationalité de K équivaut à $v_p\left(\log_p(\varepsilon')\right) = \frac{1}{2}$, ce qui équivaut encore à p ne divise pas k', i.e. p ne divise pas k. □

Nous donnons ci après une démonstration du résultat utilisé concernant la décomposition de p dans les corps quadratiques $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{-2})$.

Démonstration du Lemme. Rappelons que la décomposition d'un premier p dans un corps quadratique de discriminant D dépend de la valeur du symbole de Kronecker $\left(\frac{8}{p}\right)$ (voir [11] Proposition 3.4.3 par exemple).

1. *Décomposition des premiers dans $\mathbb{Q}(\sqrt{2})$* : le discriminant de $\mathbb{Q}(\sqrt{2})$ est 8. Ainsi, la décomposition d'un premier p dans ce corps quadratique est entièrement déterminé par la valeur du symbole de Kronecker $\left(\frac{8}{p}\right)$. On a :

$$p \text{ est } \begin{cases} \text{ramifié} & \text{si } p = 2 \\ \text{inerte} & \text{si } \left(\frac{8}{p}\right) = -1 \\ \text{totalement décomposé} & \text{si } \left(\frac{8}{p}\right) = 1 \end{cases}$$

Or, on a $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)^3$ avec $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

— Si $p \equiv 1 \pmod 8$, alors $p = 8h+1$, donc $p^2 = 64h^2+16h+1 = 16(4h^2+1)+1$; donc $\frac{p^2-1}{8} = \frac{16H+1-1}{8} = 2H$ est pair et $\left(\frac{8}{p}\right) = 1$, i.e. p est totalement décomposé.

— Si $p \equiv 3 \pmod 8$, alors $p = 8h+3$, donc $p^2 = 64h^2+48h+9 = 16(4h^2+3h)+9$; donc $\frac{p^2-1}{8} = \frac{16H+9-1}{8} = \frac{16H+8}{8} = 2H+1$ est impair, et donc $\left(\frac{8}{p}\right) = -1$, i.e. p reste inerte.

— Si $p \equiv 5 \pmod 8$, alors $p = 8h+5$, donc $p^2 = 64h^2+80h+25 = 16(4h^2+5h+1)+9$; donc $\frac{p^2-1}{8} = \frac{16H+9-1}{8} = \frac{16H+8}{8} = 2H+1$ est impair, et donc $\left(\frac{8}{p}\right) = -1$, i.e. p reste inerte.

— Si $p \equiv 7 \pmod 8$, alors $p = 8h + 7$, donc $p^2 = 64h^2 + 112h + 49 = 16(4h^2 + 7h + 3) + 1$; donc $\frac{p^2-1}{8} = \frac{16H+1-1}{8} = 2H$ est pair et $\left(\frac{8}{p}\right) = 1$, i.e. p est totalement décomposé.

En résumé, dans $\mathbb{Q}(\sqrt{2})$, un premier $p \neq 2$ est inerte si $p \equiv 3$ ou $5 \pmod 8$, et est totalement décomposé si $p \equiv 1$ ou $7 \pmod 8$.

2. *Décomposition des premiers dans* $\mathbb{Q}(\sqrt{-2})$: le discriminant de $\mathbb{Q}(\sqrt{-2})$ est -8. Ainsi, la décomposition d'un premier p dans ce corps quadratique est entièrement déterminée par la valeur du symbole de Kronecker $\left(\frac{-8}{p}\right)$. On a :

$$p \text{ est } \begin{cases} \text{ramifié} & \text{si } p = 2 \\ \text{inerte} & \text{si } \left(\frac{-8}{p}\right) = -1 \\ \text{totalement décomposé} & \text{si } \left(\frac{-8}{p}\right) = 1 \end{cases}$$

Or, on a $\left(\frac{8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^3$ avec $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ et $\left(\frac{-1}{p}\right) = (-1)^{\frac{n-1}{2}}$

— Si $p \equiv 1 \pmod 8$, alors $\left(\frac{8}{p}\right) = 1$ et $\left(\frac{-1}{p}\right) = 1$, donc $\left(\frac{-8}{p}\right) = 1$, i.e. p est totalement décomposé.
— Si $p \equiv 3 \pmod 8$, alors $\left(\frac{8}{p}\right) = -1$ et $\left(\frac{-1}{p}\right) = -1$, donc $\left(\frac{-8}{p}\right) = 1$, i.e. p est totalement décomposé.
— Si $p \equiv 5 \pmod 8$, alors $\left(\frac{8}{p}\right) = -1$ et $\left(\frac{-1}{p}\right) = 1$, donc $\left(\frac{-8}{p}\right) = -1$, i.e. p reste inerte.
— Si $p \equiv 7 \pmod 8$, alors $\left(\frac{8}{p}\right) = 1$ et $\left(\frac{-1}{p}\right) = -1$, donc $\left(\frac{-8}{p}\right) = -1$, i.e. p reste inerte.

En résumé, dans $\mathbb{Q}(\sqrt{-2})$, le premier p reste inerte si $p \equiv 5$ ou $7 \pmod 8$, et est totalement décomposé si $p \equiv 1$ ou $3 \pmod 8$.

□

3.1.3 Vérification empirique

On peut alors vérifier empiriquement que $\mathbb{Q}(\sqrt{p})$ est p-rationnel pour tout $p \leq n$, avec n assez grand.

On utilise le code PARI/GP suivant :

```
{forprime(p=3,10000000,
if(Mod(p,4)==Mod(3,4),
K = bnfinit(x^2-p,1);
e = lift(K.fu[1]) ;
a = polcoef(e,0) ;
a = sign(a)*a ;
if(Mod(a-1,p)==Mod(0,p), k = (a-1)/p ) ;
if(Mod(a+1,p)==Mod(0,p), k = (a+1)/p ) ;
if(Mod(k,p)==Mod(0,p), print(p) )))}

gp>
```

On vérifie alors que, pour tout p premier, $p \equiv 3 \pmod 4$, $p \leq 10^7$, $\mathbb{Q}(\sqrt{p})$ est p-rationnel.

3.1.4 Pour aller plus loin

On peut remarquer qu'il n'est même pas nécessaire d'avoir une unité fondamentale pour vérifier la p-rationalité de $\mathbb{Q}(\sqrt{p})$: avoir à disposition une simple unité suffit amplement.

On considère toujours le cas $p \equiv 3 \pmod 4$.

Remarquons que les propositions précédentes donnant la forme des unités sont en fait des équivalences : si on a $k \in \mathbb{Z}$ tel que $k(kp+2)$ est un carré, alors $\pm(kp+1) \pm (k(kp+2))^{1/2}\sqrt{p}$ est une unité de $\mathbb{Q}(\sqrt{p})$.

Supposons que $\varepsilon = k_0 p + 1 + (k_0(k_0 p+2))^{1/2}$. Alors k est un multiple de k_0 ; ainsi, si p ne divise pas k, alors p ne divise pas k_0, et on peut en déduire que $\mathbb{Q}(\sqrt{p})$ est p-rationnel.

On peut alors envisager de montrer que $\mathbb{Q}(\sqrt{p})$ est p-rationnel pour une infinité de premiers p en fixant k entier, et en cherchant les premiers p ne divisant pas k et tels que $k(kp+2)$ est un carré (voir annexe).

Le cas $k = 1$ se présente comme un cas particulier du développement de la section suivante.

3.2. Implications de la conjecture de Bateman-Horn

D'après les résultats de la section précédente, nous avons montré que – pour un premier $p \equiv 3 \pmod 4$ – s'il existe $k \in \mathbb{N}$ tel que p ne divise pas k et $k(kp+2)$ est un carré, alors $\mathbb{Q}(\sqrt{p})$ est p-rationnel. Concurremment, on sait que $\mathbb{Q}(\sqrt{p(p+2)})$ et $\mathbb{Q}(\sqrt{p(p-2)})$ sont p-rationnels pour tout $p \neq 5$ premier impair. Ces deux points nous amènent à considérer les premiers p tels que $p+2$ ou $p-2$ est un carré : dans ce cas, le corps quadratique $\mathbb{Q}(\sqrt{p})$ est nécessairement p-rationnel. Nous allons montrer dans la suite que la conjecture de Bateman-Horn implique que cette situation advient pour une infinité de premier p, et donc que $\mathbb{Q}(\sqrt{p})$ est premier pour une infinité de premier p.

3.2.1 Introduction

Formulée en 1962 par Paul T. Bateman et Roger A. Horn, la conjecture du Bateman-Horn s'efforce de répondre à la question suivante : étant donnée une collection de polynômes à coefficients entiers $f_1, \ldots, f_r$, à quelle fréquence les valeurs $f_1(n), \ldots, f_r(n)$ sont-elles toutes simultanément des nombres premiers ?

La conjecture de Bateman-Horn est une généralisation de théorèmes aussi importants que le théorème des nombres premiers ou le théorème de Green-Tao. Mais il s'agit aussi d'une généralisation d'autres conjectures (toujours ouvertes) de théorie analytique des nombres, telle la conjecture de Landau, ou la conjecture des nombres premiers jumeaux.

On trouvera dans [2] une exposition détaillée de cette conjecture, de ses ramifications et son histoire. On y trouvera surtout un certain nombre d'heuristiques qui supportent très fortement la véracité de cette conjecture.

La conjecture de Bateman-Horn peut s'énoncer ainsi :

Conjecture 3.2.1. *Soit f_1, f_2, ..., $f_k \in \mathbb{Z}[X]$ des polynômes irréductibles distincts, et dont les coefficients dominants sont positifs. On note*

$$Q(f_1, f_2, \ldots, f_k; x) = \#\{n \geq x \mid f_1(n), f_2(n), \ldots, f_k(n) \text{ sont premiers } \}$$

Supposons qu'il n'existe aucun premier p tel que $f = f_1 f_2 \cdots f_k$ soit identiquement nul modulo p, i.e. $f(n) \equiv 0 \pmod p$ pour tout $n \in \mathbb{Z}$. Alors

$$Q(f_1, f_2, \ldots, f_k; x) \sim \frac{C(f_1, f_2, \ldots, f_k)}{\prod_{i=1}^{k} \deg f_i} \int_2^x \frac{dt}{(\log t)^k}$$

avec

$$C(f_1, f_2, \ldots, f_k) = \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\omega_f(p)}{p}\right) = \prod_p \frac{p - \omega_f(p)}{p - 1}$$

et $\omega_f(p)$ *le nombre de solutions modulo* p *de l'équation* $f(n) \equiv 0 \pmod{p}$

3.2.2 Calcul de $C(f)$

Le fait que $C(f) \neq 0$ n'est pas trivial, mais est traité de manière extensive dans [2], Section 5.

Afin de calculer $C(f)$ pour un polynôme $f \in \mathbb{Z}[X]$ donné, il est nécessaire de calculer $\omega_f(p)$ pour tout premier p.

Rappelons le critère de factorisation de Dedekind :

> Soit $K = \mathbb{Q}(\theta)$ un corps de nombres, avec $\theta \in \mathcal{O}_K$. Soit p un nombre premier. On note f le polynôme minimal de θ sur $\mathbb{Q}$. Notons
>
> $$f(x) \equiv g_1(x)^{e_1} g_2(x)^{e_2} \cdots g_k(x)^{e_k} \pmod{p}$$
>
> la décomposition de f en produit d'irréductibles dans $\mathbb{F}_p[X]$.
> Si p ne divise pas $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, alors $p\mathcal{O}_K$ se décompose en produits d'idéaux premiers dans K sous la forme
>
> $$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_k^{e_k}$$
>
> et $\deg g_i(x)$ est le degré d'inertie de $\mathfrak{p}_i$ au-dessus de p.

Dès lors, pour $a \in \mathbb{Z}$, on a $f(a) \equiv 0 \pmod{p}$ si et seulement si $(x - a)$ divise $f(x)$ modulo p, si et seulement si $g_i(x) = x - a$ pour un certain i.

Par le critère de Dedekind, on en déduit que, lorsque p ne divise pas $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, $f(a) \equiv 0 \pmod{p}$ si et seulement si il existe un idéal $\mathfrak{p}$ au-dessus de p tel que $f(\mathfrak{p}|p) = 1$, i.e. $\mathfrak{p}$ est de norme p.

Pour presque tout premier p (dès que p ne divise pas $[\mathcal{O}_K : \mathbb{Z}[\theta]]$), le nombre de solutions $\omega_f(p)$ de l'équation $f(x) \equiv 0 \pmod{p}$ est donc égal au nombre d'idéaux premiers de $K(\theta)$ de norme p au-dessus de p.

3.2.3 $\mathbb{Q}(\sqrt{p})$ sous Bateman-Horn

On montre que :

Proposition 3.2.2. *Sous la conjecture de Bateman-Horn, il existe une infinité de premiers* p *tels que* $\mathbb{Q}(\sqrt{p})$ *est* p*-rationnel.*

Démonstration. On suppose vérifiée la conjecture de Bateman-Horn.

Notons $f(X) = X^2 + 2$ et $K = \mathbb{Q}(\sqrt{-2})$. On a $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$.

Remarquons que la décomposition en produit d'irréductibles de $f(X)$ modulo p décrit alors la décomposition de l'idéal $p\mathcal{O}_K$, selon la règle suivante

- p se ramifie dans K si et seulement si $f(x) = g(x)^2$ modulo p. Puisque f est de degré 2, $g(x) = x - \alpha$ est de degré 1, et offre une unique racine modulo p de f.
- p reste inerte dans K si et seulement si $f(x)$ est irréductible modulo p, et alors f n'admet aucune racine modulo p.
- p se décompose totalement dans K si et seulement si $f(x) = g_1(x)g_2(x)$ modulo p (où g_1 et g_2 ne sont pas égaux à multiplication par un inversible près). Alors $g_1(x) = x - \alpha$ et $g_2(x) = x - \beta$, et on obtient deux racines distinctes de f modulo p.

Notons $\omega(p)$ le nombre de solutions de l'équation $f(x) \equiv 0 \pmod{p}$. En résumé, on a

$$\omega(p) = \begin{cases} 1 & \text{si } p \text{ se ramifie dans } K \\ 0 & \text{si } p \text{ reste inerte dans } K \\ 2 & \text{si } p \text{ se décompose totalement dans } K \end{cases}$$

Ici, le déterminant de K est $D = -8$. Alors, la proposition précédente se réécrit :

$$\omega(p) = \begin{cases} 1 & \text{si } p = 2 \\ 0 & \text{si } \left(\frac{-8}{p}\right) = -1 \iff p \equiv 5 \text{ ou } 7 \pmod{8} \\ 2 & \text{si } \left(\frac{-8}{p}\right) = 1 \iff p \equiv 1 \text{ ou } 3 \pmod{8} \end{cases}$$

Puisque $\omega(2) \neq 2$, on en déduit en particulier que, pour tout p premier, $f(X)$ n'est pas identiquement nulle modulo p. Puisque f est également irréductible dans $\mathbb{Z}[X]$ et de coefficient dominant positif, on peut conclure par la conjecture de Bateman-Horn qu'il existe une infinité d'entiers n tels que $f(n) = n^2 + 2$ est premier. Il existe donc une infinité de premiers p de la forme $n^2 + 2$, donc une infinité de premiers p tels que $p - 2$ est un carré.

On obtient donc une infinité de premiers p tels que $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\sqrt{p(p-2)})$ est p-rationnel.

Notons que, de la même façon, on aurait pu appliquer la conjecture de Bateman-Horn au polynôme $g(X) = X^2 - 2$, et observer la décomposition des premiers p dans $\mathbb{Q}(\sqrt{2})$ pour en conclure qu'il existe une infinité de premiers p tels que $p + 2$ est un carré.

□

3.2.4 Estimation de $C(x^2+2)$ et $C(x^2-2)$

Reprenons : on a

$$C(f) = \prod_p \frac{p-\omega(p)}{p-1}$$

Il est alors possible de déterminer une valeur approchée de la constante via le calcul des produits partiels :

Estimation de $C(x^2+2)$

N	N-ième produit partiel $p \leq N$
10^3	$0,709843768334755632473916810911275833 11$
10^4	$0,712544427995045563528424655018244000 96$
10^5	$0,712734309505528058666447203574468149 06$
10^6	$0,713012389374450601330384180346613828 41$

Estimation de $C(x^2+2)$

N	N-ième produit partiel $p \leq N$
10^3	$1,844165067512481017872586871742469837 8$
10^4	$1,849488204012290281008019185492611367 5$
10^5	$1,849372767820253742211006736085723606 9$
10^6	$1,849874014970504383531202766833577988 0$

Premiers p entre 5 et 10^7 tels que $p+2$ est un carré :

7, 23, 47, 79, 167, 223, 359, 439, 727, 839, 1087, 1223, 1367, 1847, 2207, 2399, 3023, 3719, 3967, 4759, 5039, 5623, 5927, 7919, 8647, 10607, 11447, 13687, 14159, 14639, 16127, 17159, 18223, 19319, 21023, 24023, 25919, 28559, 29927, 31327, 33487, 36479, 42023, 44519, 47087, 49727, 53359, 54287, 56167, 57119, 61007, 64007, 66047, 67079, 70223, 71287, 74527, 77839, 81223, 85847, 89399, 90599, 91807, 95479, 97967, 99223, 104327, 112223, 113567, 116279, 126023, 127447, 128879, 137639, 149767, 152879, 159199, 164023, 172223, 177239, 180623, 184039, 189223, 194479, 196247, 199807, 201599, 218087, 219959, 231359, 239119, 241079, 245023, 247007, 255023, 263167, 273527, 275623, 281959, 292679, 297023, 314719, 319223, 323759, 328327, 330623, 339887, 344567, 354023, 368447, 370879, 378223, 385639, 405767, 416023, 426407, 439567, 444887, 450239, 458327, 508367, 511223, 516959, 528527, 537287, 552047, 558007, 563999, 573047, 579119, 582167, 600623, 606839, 616223, 622519, 635207, 651247, 657719, 667487, 680623, 707279, 744767, 765623, 776159, 804607, 811799, 866759, 889247, 893023, 904399, 919679, 946727, 958439, 974167, 986047, 990023, 1006007, 1026167, 1042439, 1046527, 1058839, 1071223, 1092023, 1104599, 1117247, 1142759, 1147039, 1151327, 1177223, 1190279, 1212199, 1238767,

1252159, 1265623, 1301879, 1306447, 1315607, 1320199, 1329407, 1338647, 1347919, 1380623, 1385327, 1432807, 1466519, 1495727, 1515359, 1520287, 1535119, 1540079, 1564999, 1570007, 1590119, 1600223, 1605287, 1656367, 1661519, 1682207, 1708247, 1718719, 1745039, 1771559, 1803647, 1841447, 1846879, 1857767, 1863223, 1868687, 1901639, 1934879, 1940447, 1985279, 2002223, 2042039, 2059223, 2082247, 2093807, 2134519, 2140367, 2223079, 2246999, 2301287, 2313439, 2325623, 2387023, 2399399, 2436719, 2442967, 2455487, 2550407, 2563199, 2569607, 2595319, 2614687, 2621159, 2686319, 2732407, 2798927, 2819039, 2825759, 2845967, 2866247, 2873023, 2893399, 2900207, 2941223, 2948087, 2961839, 2982527, 3017167, 3031079, 3058999, 3065999, 3179087, 3186223, 3229207, 3265247, 3308759, 3337927, 3381919, 3389279, 3418799, 3463319, 3485687, 3515623, 3553223, 3591023, 3598607, 3644279, 3651919, 3659567, 3697927, 3705623, 3728759, 3790807, 3814207, 3861223, 3876959, 3900623, 3916439, 3956119, 3988007, 4003999, 4084439, 4124959, 4141223, 4149367, 4173847, 4214807, 4231247, 4239479, 4297327, 4313927, 4330559, 4355567, 4372279, 4380647, 4389023, 4414199, 4431023, 4439447, 4447879, 4464767, 4532639, 4549687, 4566767, 4626799, 4678567, 4713239, 4739327, 4748039, 4765487, 4888519, 4950623, 4959527, 5013119, 5022079, 5049007, 5112119, 5148359, 5166527, 5184727, 5212087, 5230367, 5276207, 5303807, 5331479, 5359223, 5461567, 5499023, 5564879, 5640623, 5669159, 5707319, 5726447, 5764799, 5822567, 5861239, 5870927, 5909759, 5997599, 6027023, 6076223, 6095959, 6175223, 6205079, 6285047, 6305119, 6315167, 6325223, 6395839, 6416087, 6456679, 6466847, 6497399, 6528023, 6568967, 6599759, 6640927, 6682223, 6702919, 6713279, 6744407, 6754799, 6775607, 6817319, 6859159, 6880127, 6953767, 7006607, 7038407, 7102223, 7112887, 7177039, 7187759, 7295399, 7306207, 7327847, 7371223, 7382087, 7403839, 7425623, 7447439, 7480223, 7491167, 7502119, 7556999, 7612079, 7689527, 7722839, 7756223, 7812023, 7879247, 7890479, 7958039, 8048567, 8116799, 8151023, 8231159, 8242639, 8311687, 8346319, 8392607, 8473919, 8555623, 8590759, 8602487, 8649479, 8732023, 8838727, 8862527, 8982007, 9138527, 9174839, 9199087, 9235519, 9259847, 9284207, 9320807, 9443327, 9455623, 9480239, 9492559, 9517223, 9541919, 9566647, 9616199, 9628607, 9703223, 9740639, 9778127, 9790639, 9803159, 9828223, 9865879, 9891023, 9916199.

Premiers p entre 5 et 10^7 tels que $p-2$ est un carré :

11, 83, 227, 443, 1091, 1523, 2027, 3251, 6563, 9803, 11027, 12323, 13691, 15131, 21611, 29243, 47963, 50627, 56171, 59051, 62003, 65027, 74531, 88211, 91811, 95483, 103043, 119027, 123203, 131771, 136163, 140627, 149771, 173891, 178931, 184043, 194483, 199811, 205211, 227531, 251003, 263171, 301403, 308027, 314723, 328331, 363611, 370883, 423803, 455627, 463763, 488603, 505523, 567011, 603731, 651251, 670763, 700571,

751691, 783227, 804611, 815411, 826283, 870491, 915851, 938963, 962363, 1022123, 1071227, 1147043, 1238771, 1279163, 1306451, 1390043, 1461683, 1476227, 1490843, 1520291, 1535123, 1550027, 1718723, 1766243, 1879643, 2030627, 2064971, 2241011, 2277083, 2368523, 2442971, 2556803, 2595323, 2614691, 2634131, 2673227, 2772227, 2812331, 2832491, 3017171, 3059003, 3250811, 3337931, 3381923, 3493163, 3629027, 3744227, 3767483, 3814211, 3884843, 3980027, 4076363, 4100627, 4223027, 4322243, 4347227, 4549691, 4575323, 4782971, 4809251, 4862027, 4888523, 4941731, 4995227, 5103083, 5212091, 5239523, 5294603, 5546027, 5774411, 5803283, 5919491, 6007403, 6185171, 6215051, 6426227, 6579227, 6671891, 6702923, 6922163, 7017203, 7080923, 7273811, 7371227, 7403843, 7535027, 7601051, 7800851, 7868027, 7935491, 7969331, 8139611, 8661251, 8696603, 8732027, 8946083, 9018011, 9308603, 9492563, 9566651, 9678323, 9979283.

CHAPITRE 4

Corps triquadratiques p-rationnels

Le contenu de ce chapitre à fait l'objet d'une publication soumise au Journal of Number Theory.

Dans [6], Benmerieme et Movahhedi démontre que le corps

$$\mathbb{Q}\left(\sqrt{p(p-2)}, \sqrt{p(p+2)}\right)$$

est p-rationnel pour tout premier $p \geq 5$. Ils proposent alors un certain nombre de pistes afin de généraliser ce résultat. En particulier, les deux auteurs proposent de s'intéresser au corps triquadratique

$$\mathbb{Q}\left(\sqrt{p(p+2)}, \sqrt{p(p-2)}, \sqrt{-1}\right)$$

dont la p-rationalité équivaut à la p-rationalité de tous ses sous-corps quadratiques imaginaires (les sous-corps quadratiques totalement réels étant déjà inclus dans le corps biquadratique précédemment cité). Via une méthode analytique, nous démontrerons dans la suite que ce corps triquadratique est p-rationnel pour une infinité de premier p.

On pourra en déduire que $G(3,p)$ est vérifiée pour une infinité de premiers p, ce qui étend les résultats précédemment connus sur la conjecture de Greenberg au cas triquadratique pour une infinité de premiers p.

4.1. Résultat principal

Nous allons démontrer le résultat suivant :

Théorème 4.1.1. *Il existe une infinité de premiers p tel que*

$$\mathbb{Q}\left(\sqrt{p(p+2)}, \sqrt{p(p-2)}, \sqrt{-1}\right)$$

est p-rationnel.

Démonstration. Notons $K_p = \mathbb{Q}(\sqrt{p(p+2)}, \sqrt{p(p-2)}, \sqrt{-1})$, et dressons la liste exhaustive des sous-corps quadratiques de K :

1. $K_{p,1} = \mathbb{Q}\left(\sqrt{p(p+2)}\right)$
2. $K_{p,2} = \mathbb{Q}\left(\sqrt{p(p-2)}\right)$
3. $K_{p,3} = \mathbb{Q}\left(\sqrt{(p+2)(p-2)}\right)$
4. $K_{p,4} = \mathbb{Q}\left(\sqrt{-1}\right)$
5. $K_{p,5} = \mathbb{Q}\left(\sqrt{-p(p+2)}\right)$
6. $K_{p,6} = \mathbb{Q}\left(\sqrt{-p(p-2)}\right)$
7. $K_{p,7} = \mathbb{Q}\left(\sqrt{-(p+2)(p-2)}\right)$.

Dès lors, nous savons que K_p est p-rationnel si et seulement si tous les corps $K_{p,i}$ (pour $1 \leq i \leq 7$) sont p-rationnels. Nous allons donc montrer qu'il existe une infinité de premier p tels que tous les corps $K_{p,i}$ correspondants sont p-rationnels.

Rappelons d'abord quelques résultats connus :

1. Benmerieme et Movahhedi ont montré dans [6] que, pour tout $p \geq 5$, les corps quadratiques $K_{p,1}$, $K_{p,2}$ et $K_{p,3}$ sont p-rationnels : voir Proposition 2.3.14.
2. Le corps quadratique imaginaire $K_{p,4} = \mathbb{Q}\left(\sqrt{-1}\right)$ est p-rationnel pour tout p impair.
3. Soit $i = 5, 6, 7$. Le corps $K_{p,i}$ est p-rationnel dès que son nombre de classes $h_{K_{p,i}}$ n'est pas divisible par p.

Dès lors, nous pouvons utiliser la proposition analytique prouvée séparément ci-après (Proposition 4.2.1) : pour $A > 0$, il existe une infinité de premiers p tels $p-2$ et $p+2$ admettent chacun un facteur carré plus grand que $(\log p)^A$.

En particulier, on peut poser $A = 3$, et on obtient une infinité de premiers p tels que :

$$\begin{aligned}\mathrm{disc}(K_{p,5}) &\leq \frac{4p(p+2)}{(\log p)^6}\\ \mathrm{disc}(K_{p,6}) &\leq \frac{4p(p-2)}{(\log p)^6}\\ \mathrm{disc}(K_{p,7}) &\leq \frac{4(p+2)(p-2)}{(\log p)^{12}}\end{aligned}$$

A partir de maintenant, nous ne considérerons que les premiers $p \geq 5$ appartenant à cet ensemble infini de premiers décrit ci-avant, que nous noterons désormais $\mathcal{P}$.

Nous utilisons alors la proposition 2.3.6 : pour tout $p \in \mathcal{P}$, on obtient

$$h(K_{p,5}) \leq \frac{6}{4\pi}\sqrt{\frac{4p(p+2)}{(\log p)^6}}\left(\log\left(\frac{4p(p+2)}{(\log p)^6}\right)+\frac{3}{2}\right)$$

On observe que la majoration obtenue est négligeable devant $\dfrac{p}{\log p}$.

En effet, en divisant cette expression par $\frac{p}{\log p}$, on obtient :

$$\frac{6}{4\pi}\frac{\sqrt{4p(p+2)}}{p}\cdot\frac{\log\left(\frac{4p(p+2)}{(\log p)^6}\right)+\frac{3}{2}}{(\log p)^2}$$

avec $\displaystyle\lim_{p\to+\infty}\frac{\sqrt{4p(p+2)}}{p} = 2$ et

$$\begin{aligned}\frac{\log\left(\frac{4p(p+2)}{(\log p)^6}\right)+\frac{3}{2}}{(\log p)^2} &\leq \frac{\log(4p(p+2))+\frac{3}{2}}{(\log p)^2}\\ &= \frac{\log(4)+\frac{3}{2}}{(\log p)^2}+\frac{\log(p)}{\log(p)^2}+\frac{\log(p+2)}{\log(p)^2} \underset{p\to+\infty}{\longrightarrow} 0\end{aligned}$$

Ainsi, on a :

$$h(K_{p,5}) = o_{+\infty}\left(\frac{p}{\log(p)}\right)$$

Par les mêmes calculs, on obtient également :

$$h(K_{p,6}) \leq \frac{6}{4\pi}\sqrt{\frac{4p(p-2)}{(\log p)^6}}\left(\log\left(\frac{4p(p-2)}{(\log p)^6}\right)+\frac{3}{2}\right) = o_{+\infty}\left(\frac{p}{\log(p)}\right)$$

$$h(K_{p,7}) \leq \frac{6}{4\pi}\sqrt{\frac{4(p+2)(p-2)}{(\log p)^{12}}}\left(\log\left(\frac{4(p+2)(p-2)}{(\log p)^{12}}\right)+\frac{3}{2}\right) = o_{+\infty}\left(\frac{p}{\log(p)^4}\right)$$

Alors, pour $p \in \mathcal{P}$ assez grand, p est plus grand que $h(K_{p,5})$, $h(K_{p,6})$ et $h(K_{p,7})$. Ainsi, si p est assez grand dans $\mathcal{P}$, alors $p \nmid h(K_{p,5})$, $p \nmid h(K_{p,6})$ et $p \nmid h(K_{p,7})$, et les corps quadratiques imaginaires correspondants sont p-rationnels.

On conclut alors que K_p est p-rationnel pour tout $p \in \mathcal{P}$ assez grand. □

4.2. Proposition analytique : démonstration

Nous allons maintenant démontrer la proposition analytique que nous avons utilisé à la section précédente.

Proposition 4.2.1. *Soit $A > 0$.*

Il existe une infinité de premiers p tels que : il existe $m, n \in \mathbb{N}$ avec

$$\begin{cases} n^2 \mid p-2 \\ m^2 \mid p+2 \\ (\log p)^A < n \\ (\log p)^A < m \end{cases}$$

En d'autres termes, il existe une infinité de premiers p tels que $p-2$ et $p+2$ admettent chacun des facteurs carrés plus grand que $(\log p)^A$.

Notations : pour m, n des entiers naturels, on note

$$G(m) := \left\{ p \text{ premier} \;\middle|\; \begin{array}{l} p \equiv -2 \pmod{m^2} \\ (\log p)^A < m \end{array} \right\}$$

$$H(n) := \left\{ p \text{ premier} \;\middle|\; \begin{array}{l} p \equiv 2 \pmod{n^2} \\ (\log p)^A < n \end{array} \right\}$$

et

$$I(m,n) := G(m) \cap H(n) = \left\{ p \text{ premier} \;\middle|\; \begin{array}{l} p \equiv -2 \pmod{m^2} \\ p \equiv 2 \pmod{n^2} \\ (\log p)^A < m \\ (\log p)^A < n \end{array} \right\}$$

Afin de démontrer notre proposition, il suffit de montrer que la somme

$$\sum_{\substack{p \text{ premiers} \\ 3 \leq p < x}} \log(p) \left(\sum_{\substack{m \in \mathbb{N} \\ m < \sqrt{x+2} \\ p \in G(m)}} 1 \right) \times \left(\sum_{\substack{n \in \mathbb{N} \\ n < \sqrt{x-2} \\ p \in H(n)}} 1 \right)$$

tend vers l'infini lorsque $x \to +\infty$.

4.2.1 Première minoration

Tout d'abord, on peut transformer notre somme de manière élémentaire de la façon suivante :

$$\sum_{\substack{p \text{ premiers}\\ 3\leq p<x}} \log(p) \left(\sum_{\substack{m\in\mathbb{N}\\ m<\sqrt{x+2}\\ p\in G(m)}} 1 \right) \times \left(\sum_{\substack{n\in\mathbb{N}\\ n<\sqrt{x-2}\\ p\in H(n)}} 1 \right) \tag{4.1}$$

$$= \sum_{\substack{p \text{ premiers}\\ 3\leq p<x}} \sum_{\substack{m,n\in\mathbb{N}\\ m<\sqrt{x+2}\\ n<\sqrt{x-2}\\ p\in I(m,n)}} \log(p) \tag{4.2}$$

$$= \sum_{\substack{m,n\in\mathbb{N}\\ m<\sqrt{x+2}\\ n<\sqrt{x-2}}} \sum_{\substack{p \text{ premiers}\\ 3\leq p<x\\ p\in I(m,n)}} (\log p) \tag{4.3}$$

$$\geq \sum_{\substack{m,n\in\mathbb{N}\\ m<\sqrt{x+2}\\ n<\sqrt{x-2}\\ (m,n)=1\\ m,n \text{ impairs}}} \sum_{\substack{p \text{ premiers}\\ 3\leq p<x\\ p\in I(m,n)}} \log(p) \tag{4.4}$$

On a réuni les deux dernières sommes de (4.1) afin d'obtenir l'expression (4.2). On a échangé ensuite les deux sommes de (4.2) pour obtenir (4.3). On a enfin obtenu une première minoration (4.4) en restreignant la première somme (sur $m, n \in \mathbb{N}$) par les conditions $(m, n) = 1$ et m, n impairs.

La condition « m et n premiers entre eux » nous permet d'utiliser le théorème des restes chinois : puisque n et m sont premiers entre eux, alors m^2 et n^2 le sont aussi, et il existe $a_{m,n} \in \mathbb{Z}$ tel que, pour tout $k \in \mathbb{Z}$, on a :

$$\begin{cases} k \equiv 2 \pmod{n^2} \\ k \equiv -2 \pmod{m^2} \end{cases} \iff k \equiv a_{m,n} \pmod{m^2n^2}$$

Alors, si $(m, n) = 1$, on obtient :

$$I(m,n) = \left\{ p \text{ premiers} \;\middle|\; \begin{array}{l} p \equiv a_{m,n} \pmod{m^2n^2} \\ (\log p)^A < m \\ (\log p)^A < n \end{array} \right\}$$

La condition « m, n impairs » assure quant à elle que $a_{m,n}$ et m^2n^2 sont premiers entre eux.

Soit $B > 0$ tel que $A < B$. Pour x assez grand (i.e. tel que $\sqrt{x-2}$ est strictement plus grand que $(\log x)^B$), (4.4) est minoré par

$$\sum_{\substack{(\log x)^A < m,n < (\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \sum_{\substack{3 \leq p < x \\ p \in I(m,n)}} \log(p) \tag{4.5}$$

Remarquons que :

$$\begin{cases} p < x \\ (\log p)^A < n \\ (\log p)^A < m \end{cases} \iff \begin{cases} (\log p)^A < (\log x)^A \\ (\log p)^A < n \\ (\log p)^A < m \end{cases}$$
$$\iff (\log p)^A < \min\Big((\log x)^A, n, m\Big)$$

Alors, si $(\log x)^A < m, n$ (comme dans (4.5)), on obtient

$$\min((\log x)^A, n, m) = (\log(x))^A$$

et l'ensemble des conditions précédentes équivaut à $(\log p)^A < (\log x)^A$, c'est-à-dire à la condition $p < x$.

Ainsi (4.5) peut être réécrit :

$$\sum_{\substack{(\log x)^A < m,n < (\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \sum_{\substack{3 \leq p < x \\ p \equiv a_{m,n}[m^2n^2]}} \log(p) \tag{4.6}$$

et on acquière enfin une minoration bien utile de (4.1).

4.2.2 Équivalent en l'infini

Pour $(a, q) = 1$, on définit :

$$\theta(x; q, a) = \sum_{\substack{p \text{ premier} \\ p < x \\ p \equiv a[q]}} \log(p)$$

Le théorème des nombres premiers offre un équivalent en l'infini de θ. Une estimation du terme d'erreur est donné par le théorème suivant :

Théorème 4.2.2 ([13], Théorème 8.8, p. 293)**.** *Soit $a, q \in \mathbb{N}$, $q \geq 1$, $(a, q) = 1$.*

Soit $C > 0$. Pour $q \ll \log(x)^C$, on a

$$\theta(x; q, a) = \frac{x}{\varphi(q)} + O\left(\frac{x}{(\log x)^C}\right)$$

pour tout $x \geq 2$. Les constantes implicites ne dépendent que de C.

Nous avons précédemment donné une minoration de (4.1) via l'expression (4.6), qui peut alors se réécrire :

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \left[\theta\left(x, a_{m,n}, m^2n^2\right) - \log(2)\right] \tag{4.7}$$

Remark : la définition de θ que nous avons utilisée implique $p = 2$, tandis que ce terme n'intervenait pas initialement, ce qui explique l'apparition du terme $\log(2)$.

Par le théorème 4.2.2, si on pose $C > 4B$, alors on a

$$m^2n^2 \leq (\log x)^{4B} \ll (\log x)^C$$

et on obtient :

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \theta\left(x, a_{m,n}, m^2n^2\right) = \sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \left[\frac{x}{\varphi(m^2n^2)} + E_{m,n}(x)\right] \tag{4.8}$$

avec $E_{m,n}(x) \ll \dfrac{x}{(\log x)^C}$, la constante implicite ne dépendant que de C.

Remarquons que l'on peut utiliser ces estimations car on a choisit m, n impairs, ce qui assure que le résidu $a_{m,n}$ et le module m^2n^2 sont premiers entre eux.

Ainsi, nous allons montré que :

(i) le terme principal

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \frac{x}{\varphi(m^2n^2)}$$

tend vers l'infini lorsque $x \to +\infty$, et que

(ii) la croissance du terme principal n'est pas contrecarré par le terme d'erreur :

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} E_{m,n}(x) - \sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \log(2)$$

4.2.3 Estimation du terme principal

Tout d'abord, nous pouvons utiliser l'inégalité $\varphi(m^2n^2) \leq m^2n^2$, et on obtient :

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \frac{x}{\varphi(m^2n^2)} \geq \sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \frac{x}{m^2n^2} \tag{4.9}$$

Alors, on a :

$$\begin{aligned}
&\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \frac{1}{m^2n^2} \\
&= \sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ m,n \text{ impairs}}} \frac{1}{m^2n^2} - \underbrace{\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)>1 \\ m,n \text{ impairs}}} \frac{1}{m^2n^2}}_{(*)} \\
&\geq \sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ m,n \text{ impairs}}} \frac{1}{m^2n^2} - \underbrace{\sum_{2\leq d\leq(\log x)^B} \sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ m,n \text{ impairs} \\ d|m,\, d|n}} \frac{1}{m^2n^2}}_{(**)} \\
&\geq \sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ m,n \text{ impairs}}} \frac{1}{m^2n^2} - \underbrace{\sum_{2\leq d\leq(\log x)^B} \sum_{\substack{k,k' \text{ impairs} \\ (\log x)^A<dk,dk<(\log x)^B}} \frac{1}{(dk)^2(dk')^2}}_{(***)}
\end{aligned}$$

Remarquons que l'on a $(*) \leq (**) \leq (***)$, ce qui justifie les inégalités précédentes. On peut alors réécrire la dernière quantité comme :

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ m,n \text{ impairs}}} \frac{1}{m^2n^2} - \sum_{2\leq d\leq(\log x)^B} \frac{1}{d^4} \sum_{\substack{(\log x)^A<dm,dn<(\log x)^B \\ m,n \text{ impairs}}} \frac{1}{m^2n^2} \tag{4.10}$$

D'un côté, on a alors :

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ m,n \text{ impairs}}} \frac{1}{m^2n^2} = \sum_{(\log x)^A<2m+1,2n+1<(\log x)^B} \frac{1}{(2m+1)^2(2n+1)^2}$$

$$= \sum_{\frac{(\log x)^A-1}{2}<m,n<\frac{(\log x)^B-1}{2}} \frac{1}{(2m+1)^2(2n+1)^2}$$
$$= \left(\sum_{\frac{(\log x)^A-1}{2}<n<\frac{(\log x)^B-1}{2}} \frac{1}{(2n+1)^2} \right)^2$$

De l'autre, on a

$$\sum_{\substack{(\log x)^A<dm,dn<(\log x)^B \\ m,n \text{ impairs}}} \frac{1}{m^2n^2} = \sum_{(\log x)^A<d(2m+1),d(2n+1)<(\log x)^B} \frac{1}{(2m+1)^2(2n+1)^2}$$
$$= \sum_{\frac{(\log x)^A-d}{2d}<m,n<\frac{(\log x)^B-d}{2d}} \frac{1}{(2m+1)^2(2n+1)^2}$$
$$= \left(\sum_{\frac{(\log x)^A-d}{2d}<n<\frac{(\log x)^B-d}{2d}} \frac{1}{(2n+1)^2} \right)^2$$

Ainsi, l'expression (4.10) est égale à :

$$\left(\sum_{\frac{(\log x)^A-1}{2}<n<\frac{(\log x)^B-1}{2}} \frac{1}{(2n+1)^2} \right)^2 - \sum_{2\leq d\leq(\log x)^B} \frac{1}{d^4} \left(\sum_{\frac{(\log x)^A-d}{2d}<n<\frac{(\log x)^B-d}{2d}} \frac{1}{(2n+1)^2} \right)^2$$

On peut encore minorer cette dernière quantité en ayant recours à des inégalités venant de comparaisons séries-intégrales.

En particulier, on utilise l'inégalité

$$\sum_{n=a}^{b} \frac{1}{(2n+1)^2} \geq \int_a^{b+1} \frac{\mathrm{d}t}{(2t+1)^2}$$

pour obtenir

$$\sum_{\frac{(\log x)^A-1}{2}<n<\frac{(\log x)^B-1}{2}} \frac{1}{(2n+1)^2} \geq \frac{1}{2\left((\log x)^A+2\right)} - \frac{1}{2(\log x)^B}$$

De la même façon, on utilise l'inégalité

$$\sum_{n=a}^{b} \frac{1}{(2n+1)^2} \leq \int_a^{b} \frac{\mathrm{d}t}{(2t+1)^2} + \frac{1}{(2a+1)^2}$$

pour obtenir

$$\sum_{\frac{(\log x)^A-d}{2d}<n<\frac{(\log x)^B-d}{2d}} \frac{1}{(2n+1)^2} \leq \frac{d}{2(\log x)^A} - \frac{d}{2(\log x)^B} + \frac{d^2}{(\log x)^{2A}}$$

Ainsi, on obtient la suite d'inégalités suivante :

$$\begin{aligned}
&\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \frac{1}{m^2n^2} \\
&\geq \left(\sum_{\frac{(\log x)^A-1}{2}<n<\frac{(\log x)^B-1}{2}} \frac{1}{(2n+1)^2}\right)^2 - \sum_{2\leq d\leq(\log x)^B} \frac{1}{d^4}\left(\sum_{\frac{(\log x)^A-d}{2d}<n<\frac{(\log x)^B-d}{2d}} \frac{1}{n^2}\right)^2 \\
&\geq \left(\frac{1}{2\left((\log x)^A+2\right)} - \frac{1}{2(\log x)^B}\right)^2 - \sum_{2\leq d\leq(\log x)^B} \frac{1}{d^4}\left(\frac{d}{2(\log x)^A} - \frac{d}{2(\log x)^B} + \frac{d^2}{(\log x)^{2A}}\right)^2 \\
&\geq \frac{1}{4\left((\log x)^A+2\right)^2} + \frac{1}{4(\log x)^{2B}} - \frac{1}{2\left((\log x)^A+2\right)(\log x)^B} \\
&\qquad - \sum_{2\leq d\leq(\log x)^B} \frac{1}{d^2}\left(\frac{1}{4(\log x)^{2A}} + \frac{1}{4(\log x)^{2B}} + \frac{d^2}{(\log x)^{4A}} + \frac{d}{(\log x)^{3A}}\right) \\
&\geq \frac{1}{4\left((\log x)^A+2\right)^2} + \frac{1}{4(\log x)^{2B}} - \frac{1}{2\left((\log x)^A+2\right)(\log x)^B} \\
&\qquad - \left(\sum_{2\leq d\leq(\log x)^B} \frac{1}{d^2}\right)\left(\frac{1}{4(\log x)^{2A}} + \frac{1}{4(\log x)^{2B}}\right) \\
&\qquad - \left(\sum_{2\leq d\leq(\log x)^B} \frac{1}{d}\right)\frac{1}{(\log x)^{3A}} - \left(\sum_{2\leq d\leq(\log x)^B} 1\right)\frac{1}{(\log x)^{4A}} \\
&\geq \frac{1}{4\left((\log x)^A+2\right)^2} + \frac{1}{4(\log x)^{2B}} - \frac{1}{2\left((\log x)^A+2\right)(\log x)^B} \\
&\qquad - (\zeta(2)-1)\left(\frac{1}{4(\log x)^{2A}} + \frac{1}{4(\log x)^{2B}}\right) \\
&\qquad - (1+\log(\log(x)^B))\frac{1}{(\log x)^{3A}} - \frac{(\log x)^B}{(\log x)^{4A}}
\end{aligned}$$

Si on prend $A < B < 2A$, la dernière quantité est finalement équivalente à $\dfrac{2-\zeta(2)}{4}\dfrac{1}{(\log x)^{2A}}$

Ainsi, on a montré que

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \frac{1}{m^2n^2}$$

est plus grand qu'une quantité équivalente en l'infini à $\frac{2-\zeta(2)}{4}\frac{1}{(\log x)^{2A}}$.

En conséquence, le terme principal

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \frac{x}{\varphi(m^2n^2)}$$

est plus grand qu'une quantité équivalente en l'infini à

$$\frac{2-\zeta(2)}{4}\frac{x}{(\log x)^{2A}} \tag{4.11}$$

Le terme principal tend donc vers l'infini lorsque $x \to +\infty$, au moins aussi vite que (4.11).

4.2.4 Termes d'erreurs

Rappelons que $E_{m,n}(x) = \left|\theta(x;a,m^2n^2) - \frac{x}{\varphi(m^2n^2)}\right|$. On sait que, pour $C>0$ fixé, et $q \ll (\log x)^C$, on a

$$E_{m,n}(x) = O\left(\frac{x}{(\log x)^C}\right)$$

Alors, si $4B < C$, pour x assez grand, on sait que $m^2n^2 \ll (\log x)^C$ dès que $(\log x)^A < m,n < (\log x)^B$. Ainsi, chaque $E_{m,n}(x)$ est dominé par $\frac{x}{(\log x)^C}$ dans

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ odd}}} E_{m,n}(x)$$

Considérant que l'on obtient au plus $(\log x)^{2B}$ termes de la sorte, on a :

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ odd}}} E_{m,n}(x) \ll (\log x)^{2B}\frac{x}{(\log x)^C}$$

Remarquons qu'on a choisi C tel que $C > 4B$, donc $C > 2A+2B$, i.e. $2B-C<-2A$ et on peut conclure que

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} E_{m,n}(x) \ll \frac{x}{(\log x)^{2A}}$$

La deuxième partie du terme d'erreur, précisément

$$\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \log(2)$$

est au plus $(\log x)^{2B}$ fois $\log(2)$, et est donc majoré par $(\log x)^{2B}\log(2)$, qui est aussi dominé par $\dfrac{x}{(\log x)^{2A}}$.

4.2.5 Conclusion

Nous avons montré que

$$\sum_{\substack{p \text{ premier} \\ 3\leq p<x}} \log(p) \left(\sum_{\substack{m\in\mathbb{N} \\ m<\sqrt{x+2} \\ p\in G(m)}} 1 \right) \times \left(\sum_{\substack{n\in\mathbb{N} \\ n<\sqrt{x-2} \\ p\in H(n)}} 1 \right)$$

est minoré par

$$\underbrace{\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \frac{x}{\varphi(m^2n^2)}}_{A(x)} + \underbrace{\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} E(x)}_{O(A(x))} + \underbrace{\sum_{\substack{(\log x)^A<m,n<(\log x)^B \\ (m,n)=1 \\ m,n \text{ impairs}}} \log(2)}_{O(A(x))}$$

avec $A(x) \to \infty$, ce qui prouve que notre première somme tend vers l'infini lorsque $x \to \infty$. $\square$

ANNEXE A

Une proposition analytique plus forte sous GRH

A.1. Démonstration

Pour $A > 0$, nous avons montré qu'il existe une infinité de premiers p tels que $(p+2)$ et $(p-2)$ admettent simultanément des facteurs carrés plus grand que $(\log x)^A$. Nous pouvons montrer, sous GRH, un résultat plus fort. Plus précisément :

Proposition A.1.1. *Soit $\varepsilon < \frac{1}{8}$. Supposons que GRH est vérifiée pour toute fonction $L(s,\chi)$ associé à un caractère $\chi \pmod q$. Il existe une infinité de premiers p pour lesquelles il existe $m, n \in \mathbb{N}^*$, tels que*

$$\begin{cases} n^2 \mid p-2 \\ m^2 \mid p+2 \\ p^\varepsilon < n \\ p^\varepsilon < m \end{cases}$$

Démonstration. La démonstration est similaire à la première.

De la même façon, on considère la somme

$$\sum_{\substack{p \text{ premier} \\ 3 \leq p < x}} \log(p) \left(\sum_{\substack{m \in \mathbb{N} \\ m < \sqrt{x+2} \\ m^2 \mid p+2 \\ p^\varepsilon < m}} 1 \right) \times \left(\sum_{\substack{n \in \mathbb{N} \\ n < \sqrt{x-2} \\ n^2 \mid p-2 \\ p^\varepsilon < n}} 1 \right)$$

Alors, en réalisant des calculs similaires, on montre que la somme précédente est minorée par

$$\sum_{\substack{m,n\in\mathbb{N}\\ m<\sqrt{x+2}\\ n<\sqrt{x-2}\\ (m,n)=1\\ m,n \text{ impairs}}} \sum_{\substack{p \text{ premier}\\ 3\leq p<x\\ p\equiv a_{m,n}[m^2n^2]\\ p<m^{1/\varepsilon}\\ p<n^{1/\varepsilon}}} \log(p)$$

qui est plus grand (pour x assez grand) que

$$\sum_{\substack{x^\varepsilon<m,n<x^\alpha\\ (m,n)=1\\ m,n \text{ odd}}} \sum_{\substack{p \text{ premier}\\ p\equiv a_{m,n}[m^2n^2]\\ 3\leq p<x}} \log(p) \tag{A.1}$$

pour $\varepsilon < \alpha < \frac{1}{2}$.

Dès lors, sous GRH, on sait que ([21] §17.1) :

$$\theta(x; m^2n^2, a_{m,n}) = \sum_{\substack{p \text{ premier}\\ p\equiv a_{m,n}[m^2n^2]\\ p<x}} \log(p) = \frac{x}{\varphi(m^2n^2)} + O\left(x^{1/2}(\log x)^2\right)$$

Donc (A.1) est plus grand que

$$\sum_{\substack{x^\varepsilon<m,n<x^\alpha\\ (m,n)=1\\ m,n \text{ impairs}}} \left(\frac{x}{\varphi(m^2n^2)} + E_{m,n} - \log(2)\right)$$

avec $E_{m,n} \ll x^{1/2}(\log x)^2$.

D'abord, on montre que le terme principal

$$\sum_{\substack{x^\varepsilon<m,n<x^\alpha\\ (m,n)=1\\ m,n \text{ impairs}}} \frac{x}{\varphi(m^2n^2)}$$

est plus grand qu'une quantité équivalente à $\dfrac{2-\zeta(2)}{4}x^{1-2\varepsilon}$ pour $x \to +\infty$.

En effet, on a

$$\sum_{\substack{x^\varepsilon<m,n<x^\alpha\\ (m,n)=1\\ m,n \text{ impairs}}} \frac{1}{m^2n^2} = \left(\sum_{\frac{x^\varepsilon-1}{2}<n<\frac{x^\alpha-1}{2}} \frac{1}{(2n+1)^2}\right)^2$$

$$
\begin{aligned}
&- \sum_{2\leq d\leq x^\alpha} \frac{1}{d^4} \left(\sum_{\frac{x^\varepsilon-d}{2d}<n<\frac{x^\alpha-d}{2d}} \frac{1}{(2n+1)^2} \right)^2 \\
&\geq \left(\frac{1}{2(x^\varepsilon+2)} - \frac{1}{2x^\alpha} \right)^2 - \sum_{2\leq d\leq x^\alpha} \frac{1}{d^4} \left(\frac{d}{2(x^\varepsilon-2d)} - \frac{d}{2x^\alpha} \right)^2 \\
&\geq \frac{1}{4(x^\varepsilon+2)^2} - \frac{1}{2(x^\varepsilon+2)x^\alpha} + \frac{1}{4x^{2\alpha}} \\
&\quad - \frac{\zeta(2)-1}{4(x^\varepsilon-4)^2} + \frac{\zeta(2)-1}{2(x^\varepsilon-2x^\alpha)x^\alpha} - \frac{\zeta(2)-1}{4x^{2\alpha}}
\end{aligned}
$$

Dès lors, on peut considérer le premier terme d'erreur

$$\sum_{\substack{x^\varepsilon<m,n<x^\alpha \\ (m,n)=1 \\ m,n \text{ impairs}}} E_{m,n}(x)$$

avec $E_{m,n}(x) \ll x^{1/2}(\log x)^2$ (la constante implicite étant indépendante de $E_{m,n}$).

Puisqu'on obtient au plus $x^{2\alpha}$ termes qui sont $O\left(x^{1/2}(\log x)^2\right)$ (sous GRH), le terme d'erreur est $O\left(x^{\frac{1}{2}+2\alpha}(\log x)^2\right)$.

Ainsi, on prend α tel que $\varepsilon < \alpha < \frac{1}{4} - \varepsilon$ (ce qui justifie le fait que l'on a choisi préalablement $\varepsilon < \frac{1}{8}$), donc $\frac{1}{2} + 2\alpha < 1 - 2\varepsilon$.

Alors le premier terme d'erreur est $O\left(\frac{2-\zeta(2)}{4} x^{1-2\varepsilon}\right)$.

Enfin, le second terme d'erreur, c'est-à-dire

$$\sum_{\substack{x^\varepsilon<m,n<x^\alpha \\ (m,n)=1 \\ m,n \text{ impairs}}} (\log 2)$$

est au plus $x^{2\alpha}$ fois $\log(2)$, est peut être majoré par $x^{2\alpha}\log(2) = O\left(\frac{2-\zeta(2)}{4} x^{1-2\varepsilon}\right)$ (puisque α a été précédemment supposé tel que $2\alpha < \frac{1}{2} < 1 - 2\varepsilon$).

En conclusion, on a minoré notre première somme par :

$$\underbrace{\sum_{\substack{x^\varepsilon<m,n<x^\alpha \\ (m,n)=1 \\ m,n \text{ impairs}}} \frac{x}{\varphi(m^2n^2)}}_{A(x)} + \underbrace{\sum_{\substack{x^\varepsilon<m,n<x^\alpha \\ (m,n)=1 \\ m,n \text{ impairs}}} E_{m,n} + \sum_{\substack{x^\varepsilon<m,n<x^\alpha \\ (m,n)=1 \\ m,n \text{ impairs}}} \log(2)}_{O(A(x))}$$

avec $A(x) \to +\infty$, ce qui prouve notre proposition.

□

ANNEXE B

Codes et Tables

B.1. $\mathbb{Q}(\sqrt{p})$: unités fondamentales pour $p \equiv 3 \pmod 4$

Pour un premier p congrus à 3 modulo 4, la fonction Pari/Gp unif(p) renvoie l'entier $k \in \mathbb{N}$ tel qu'une unité fondamentale de $\mathbb{Q}(\sqrt{p})$ s'écrit sous la forme

$$\varepsilon = pk + 1 + (k(kp+2))^{1/2}\sqrt{p}$$

si p congrus à 7 modulo 8, et

$$\varepsilon = pk - 1 + (k(kp-2))^{1/2}\sqrt{p}$$

si p congrus à 3 modulo 8.

```
unif(p) = {
K = bnfinit(x^2 - p,1) ;
e = lift(K.fu[1]) ;
a = polcoef(e,0) ;
a = a * sign(a) ;
if(Mod(a-1,p)==Mod(0,p), k = (a-1)/p, k = (a+1)/p) ;
return(k) }
```

Table 1 : Premiers $p \equiv 7 \pmod 8$, entre 1 et 1000, et $k \in \mathbb{N}^*$ correspondant tel que l'unité ε de $\mathbb{Q}(\sqrt{p})$ s'écrit $\varepsilon = kp+1+(k(kp+2))^{1/2}\sqrt{p}$, avec décomposition en produit de facteurs premiers.

p	k
7	1
23	1
31	$49 = 7^2$
47	1
71	$49 = 7^2$
79	1
103	$2209 = 47^2$
127	$37249 = 193^2$
151	$11444689 = 17^2 \cdot 199^2$
167	1
191	$47089 = 7^2 \cdot 31^2$
199	$81739681 = 9041^2$
223	1
239	$25921 = 7^2 \cdot 23^2$
263	$529 = 23^2$
271	$427951969 = 137^2 \cdot 151^2$
311	$54289 = 233^2$
359	1
367	$51825601 = 23^2 \cdot 313^2$
383	$49 = 7^2$
431	$351649 = 593^2$
439	1
463	$534584709409 = 17^2 \cdot 41^2 \cdot 1049^2$
479	$6241 = 79^2$
487	$106583313841 = 137^2 \cdot 2383^2$
503	$49 = 7^2$
599	$41212654081 = 89^2 \cdot 2281^2$
607	$270306481 = 41^2 \cdot 401^2$
631	$77593621732169017489 = 7^2 \cdot 31^2 \cdot 40593199^2$
647	$185761 = 431^2$
719	$561168721 = 23689^2$
727	1
743	$961 = 31^2$
751	$9711475987742852762209 = 17^2 \cdot 271^2 \cdot 21390671^2$
823	$285747843139300129 = 7^2 \cdot 76364839^2$
839	1

863	$21464689 = 41^2 \cdot 113^2$
887	$529 = 23^2$
911	$408158710129 = 79^2 \cdot 8087^2$
919	$4876608281759651198641201 = 7^2 \cdot 193247^2 \cdot 1632481^2$
967	$4808203265581681 = 7^2 \cdot 41^2 \cdot 359^2 \cdot 673^2$
983	$289 = 17^2$
991	$382963068523523643428874769 = 7^2 \cdot 41^2 \cdot 68186209801^2$

Table 2 : Premiers $p \equiv 3 \pmod 8$, entre 1 et 1000, et $k \in \mathbb{N}^*$ correspondant tel que l'unité ε de $\mathbb{Q}(\sqrt{p})$ s'écrit $\varepsilon = kp - 1 + (k(kp-2))^{1/2}\sqrt{p}$, avec décomposition en produit de facteurs premiers.

p	k
3	1
11	1
19	$9 = 3^2$
43	$81 = 3^4$
59	$9 = 3^2$
67	$729 = 3^6$
83	1
107	$9 = 3^2$
131	$81 = 3^4$
139	$558009 = 3^4 \cdot 83^2$
163	$393129 = 3^2 \cdot 11^2 \cdot 19^2$
179	$23409 = 3^4 \cdot 17^2$
211	$1319215041 = 3^2 \cdot 12107^2$
227	1
251	$14641 = 11^4$
283	$488601 = 3^2 \cdot 233^2$
307	$288369 = 3^2 \cdot 179^2$
331	$8415679158441 = 3^4 \cdot 97^2 \cdot 3323^2$
347	$1849 = 43^2$
379	$34145639104329 = 3^2 \cdot 17^2 \cdot 114577^2$
419	$644809 = 11^2 \cdot 73^2$
443	1
467	$3481 = 59^2$
491	$190688481 = 3^2 \cdot 4603^2$
499	$9 = 3^2$
523	$156425049 = 2^2 \cdot 11^2 \cdot 379^2$
547	$292829252769 = 3^2 \cdot 180379^2$

563	$121 = 11^2$
571	$317205525501980361 = 3^2 \cdot 62578891^2$
587	$3249 = 3^2 \cdot 19^2$
619	$835563021895449 = 3^2 \cdot 41^2 \cdot 235009^2$
643	$3093250689 = 3^2 \cdot 18539^2$
659	$9 = 3^2$
683	$249001 = 499^2$
691	$45062374265558001 = 3^2 \cdot 11^2 \cdot 19^2 \cdot 338563^2$
739	$132632829598940111169 = 3^2 \cdot 131^2 \cdot 1291^2 \cdot 22699^2$
787	$43996689 = 3^4 \cdot 11^2 \cdot 67^2$
811	$1704158031539601 = 3^2 \cdot 11^4 \cdot 113723^2$
827	$1089 = 3^2 \cdot 11^2$
859	$2396792516856394714929 = 3^2 \cdot 1291^2 \cdot 12640601^2$
883	$39499972547697930321 = 3^2 \cdot 67^2 \cdot 547^2 \cdot 57163^2$
907	$136519746795009369 = 3^2 \cdot 11^2 \cdot 11196539^2$
947	$14265729 = 3^2 \cdot 1259^2$
971	$12852530161 = 73^2 \cdot 1553^2$

B.2. Unités de $\mathbb{Q}(\sqrt{p})$

Pour $2 \leq \alpha \leq 100$, liste des premiers p entre 3 et 10^7, $p \equiv 3 \pmod 4$, tels que $\alpha^2 p + 2$ est un carré (pour chacun de ces premiers p, le corps quadratique $\mathbb{Q}(\sqrt{p})$ est p-rationnel) :

— $\boxed{\alpha = 7}$: 31, 71, 383, 503, 1327, 2543, 5711, 6151, 8543, 14503, 21191, 22031, 25463, 36263, 46471, 47711, 60727, 66343, 73751, 81551, 91463, 98327, 160343, 195743, 218623, 221303, 245591, 248431, 262583, 339223, 352327, 369143, 389911, 403951, 421943, 444127, 462983, 478271, 482231, 497831, 521903, 538127, 558863, 623423, 627943, 645727, 650327, 696271, 714991, 738863, 768127, 787783, 864103, 922423, 943951, 976991, 1033127, 1061783, 1084871, 1120271, 1150103, 1241951, 1330727, 1337327, 1363223, 1402871, 1436231, 1469983, 1497127, 1601671, 1608911, 1644623, 1783751, 1859327, 1897703, 1905583, 2015183, 2055127, 2095463, 2103743, 2136191, 2144551, 2269327, 2397631, 2432263, 2520383, 2529463, 2747543, 2841151, 2936327, 2946127, 3082031, 3092071, 3141503, 3191327, 3281791, 3435727, 3446327, 3498503, 3540311, 3646463, 3657383, 3754183, 3765263, 3874711, 3930023, 4086751, 4143551, 4624343, 4745551, 4806743, 4979911, 4992671, 5055431, 5118583, 5426903, 5440223, 5505727, 5558143, 5571623, 5704591, 5757943, 5771663, 5893103, 6029831, 6098783, 6182327, 6252143, 6392951,

6520727, 6592423, 6679271, 6736991, 6883127, 6971863, 7045991, 7195423, 7330943, 7637327, 7966103, 8045327, 8430727, 8528903, 8610871, 8693231, 8859127, 8925583, 9538391, 9781703, 9799583, 9887431.

— $\boxed{\alpha = 17}$: 7, 983, 4271, 9871, 17783, 40543, 42703, 72551, 75431, 141863, 168631, 193031, 197711, 257407, 262807, 331031, 371311, 420743, 458807, 718007, 1035007, 1105343, 1330223, 1504663, 1676111, 1950623, 2145191, 2997583, 3380623, 3745591, 3766111, 4013423, 4312463, 4723463, 5023663, 5047423, 5491303, 5814623, 6663383, 6690743, 7047151, 8534303, 8936231, 8967911.

— $\boxed{\alpha = 23}$: 263, 887, 5743, 14831, 28151, 40087, 60623, 93503, 158231, 226783, 322871, 377263, 453983, 658991, 792487, 902087, 1183271, 1469471, 1700983, 2214791, 2353823, 2688887, 2999071, 3112463, 3795551, 3848591, 4409087, 4546351, 4947143, 5007671, 5153887, 5215663, 5427887, 5865031, 7278031, 7707383, 8304671, 9886103.

— $\boxed{\alpha = 31}$: 743, 75767, 79943, 159407, 342527, 351343, 513719, 694319, 706847, 801487, 814943, 1054199, 1624967, 1935599, 2111959, 2487743, 2511407, 2894279, 3135527, 4075319, 4329487, 4827943, 5423039, 6323927, 7253639, 7591447, 8290127, 8333279, 8695079.

— $\boxed{\alpha = 41}$: 1567, 14783, 81559, 135119, 202127, 204679, 285599, 483839, 487783, 609047, 886583, 1228583, 1834439, 2296999, 2552279, 2561327, 3409247, 3718783, 4030399, 4366367, 5091407, 5858407, 6262079, 6679199, 7553783, 8011247, 9464327.

— $\boxed{\alpha = 47}$: 103, 10847, 149111, 419711, 580871, 864623, 1518191, 1705247, 1959583, 2016823, 2231591, 2521271, 2897311, 3226151, 3496343, 3572663, 5043847, 5570303, 6022847, 6390031, 6493063, 9109223.

— $\boxed{\alpha = 49}$: 23, 10567, 36559, 83639, 340127, 769487, 786407, 951023, 1172447, 1895567, 2175023, 2759599, 2791559, 3822823, 5979023, 6516767, 7555879, 8615423, 9200327, 9258607, 9864599.

— $\boxed{\alpha = 71}$: 5903, 130199, 400903, 862727, 1121839, 1146679, 3171359, 4215503, 4263527, 4818767, 6870527, 9285239.

— $\boxed{\alpha = 73}$: 1487, 64231, 227111, 297503, 478087, 2245687, 2935871, 4337063, 5278223, 6353231, 8302687.

— $\boxed{\alpha = 79}$: 479, 32359, 114167, 659159, 857687, 1653503, 3512303, 3678287, 5721119, 6280607, 9143887, 9847759.

— $\boxed{\alpha = 89}$: 59399, 84263, 359663, 1004567, 3406679, 7484159.

— $\boxed{\alpha = 97}$: 47, 35023, 40343, 330791, 346751, 1825591, 3737047, 3790247.

Pour $2 \leq \alpha \leq 100$, liste des premiers p entre 3 et 10^7, $p \equiv 3 \pmod 4$, tels que $\alpha^2 p - 2$ est un carré (pour chacun de ces premiers p, le corps quadratique $\mathbb{Q}(\sqrt{p})$ est p-rationnel) :

— $\boxed{\alpha = 3}$: 19, 59, 107, 499, 659, 1627, 1907, 2467, 3803, 4139, 5827, 6779, 9539, 10067, 12619, 16987, 18587, 19507, 22003, 23003, 23819, 24859, 30859, 37507, 40939, 42299, 43403, 52747, 58403, 59699, 61339, 65707, 67427, 68819, 89003, 98387, 111779, 122267, 124139, 126499, 132739, 137147, 139627, 162947, 175003, 182899, 190387, 195659, 206419, 209459, 214987, 223099, 232003, 243707, 258403, 280547, 296299, 316219, 323003, 343787, 347707, 362003, 383987, 402379, 429899, 449347, 478403, 482099, 498907, 538267, 551059, 587267, 592387, 668579, 692779, 698339, 702803, 708403, 723067, 728747, 733307, 739027, 754003, 764459, 796259, 834787, 861803, 884227, 936379, 995339, 1000667, 1080907, 1118659, 1137067, 1157059, 1222499, 1235803, 1255147, 1268627, 1276147, 1295803, 1351019, 1358779, 1393187, 1401067, 1429619, 1436003, 1472987, 1508803, 1553347, 1598539, 1699547, 1738003, 1810819, 1909003, 1942307, 1992803, 2034427, 2113147, 2138419, 2255003, 2273059, 2317499, 2428403, 2484827, 2541899, 2591027, 2610379, 2649299, 2756707, 2776667, 2877547, 3000979, 3012539, 3033403, 3096427, 3138803, 3148259, 3289387, 3408947, 3453403, 3475739, 3533147, 3588499, 3601139, 3623947, 3692803, 3726187, 3796003, 3961427, 4009339, 4046803, 4081747, 4168403, 4391819, 4569619, 4698779, 4762579, 4777139, 4788803, 4841467, 4856147, 4947659, 5028059, 5043019, 5109107, 5124187, 5328403, 5343803, 5524067, 5624803, 5796859, 5854787, 5971507, 6043403, 6191803, 6208403, 6281707, 6372259, 6419467, 6511003, 6586067, 6678779, 6789499, 6834739, 6883627, 7024267, 7073827, 7313419, 7443803, 7542347, 7560667, 7626803, 7708027, 7726547, 7909219, 7927979, 7961803, 8044787, 8319379, 8458403, 8477803, 8688739, 8775419, 8846659, 8954059, 8974019, 9010003, 9082187, 9118387, 9337099, 9649307, 9744803, 9782299, 9970859.

— $\boxed{\alpha = 9}$: 43, 131, 1811, 2251, 4283, 9323, 28411, 41843, 43867, 49531, 66851, 69403, 109267, 134363, 151667, 181003, 196643, 247451, 298723, 304091, 434867, 483643, 561667, 581491, 637691, 674771, 735211, 863867, 922667, 1029323, 1260131, 1438667, 1558891, 1650083, 1662667, 1791731, 1952851, 2003483, 2472931, 2661611, 2840723, 2946563, 2963371, 3008683, 3025667, 3198931, 3329003, 3346867, 3413051, 3547363, 3753691, 3946403, 4018243, 4483571, 4616291, 4637323, 5173603, 5338667, 5591123, 5676571, 5873083, 6408211, 6499667, 6659267, 6777923, 7325443, 7548451, 7647683, 7848091, 7921723, 8464867, 8753051, 9075491, 9213923, 9403763.

- $\boxed{\alpha = 11}$: 563, 1787, 24251, 57731, 82787, 138587, 254291, 404843, 562091, 590243, 1027643, 1680323, 1805603, 2584787, 2801363, 2863787, 3754787, 3827003, 4561331, 5142587, 5446283, 6079811, 6171611, 6409643, 6748187, 7816091, 8189483, 8295971, 9361931, 9886451.
- $\boxed{\alpha = 17}$: 2459, 126443, 211979, 441443, 587387, 936227, 1144019, 2191619, 2837243, 3555443, 3566099, 4366379, 4803059, 4815443, 5752379, 6772547, 7860107, 9045587.
- $\boxed{\alpha = 19}$: 11, 12251, 13763, 53507, 119243, 204923, 2206163, 2536643, 4197107, 4705931, 5183291, 5747123, 6857507, 7467563.
- $\boxed{\alpha = 27}$: 67, 2099, 13499, 193763, 228307, 244219, 282827, 430579, 481379, 642907, 960763, 1267459, 2650987, 3340907, 3603107, 3747379, 3959363, 4244363, 5181019, 6129659, 6676099, 6958067, 8455387, 8550859, 8772347, 9758219.
- $\boxed{\alpha = 33}$: 827, 1987, 7643, 12227, 23539, 28643, 51419, 55339, 95219, 123499, 134867, 180419, 187699, 301867, 319499, 398467, 496427, 558643, 569659, 673643, 773387, 814643, 923987, 1070347, 1626707, 2001539, 2369827, 2392459, 2871587, 3044179, 3336379, 3581843, 3745867, 3774307, 4035107, 4069267, 4370507, 5237579, 5469787, 5823739, 6068459, 6183059, 6435139, 7933099, 8558107, 9087667.
- $\boxed{\alpha = 41}$: 106451, 169523, 327491, 1132667, 2421971, 3248171, 3563531, 4552811, 5263667, 5663123, 7763291.
- $\boxed{\alpha = 43}$: 347, 285827, 570587, 3329267, 6560627, 9700907.
- $\boxed{\alpha = 51}$: 9371, 11491, 162251, 220771, 254827, 265427, 517243, 568723, 657403, 674363, 732971, 960131, 1029827, 1051027, 1270571, 1350563, 1866331, 2024371, 2796043, 3024803, 3147563, 3601883, 3735731, 3776011, 3913027, 5012243, 5693651, 6476027, 6821827, 7005571, 7929083, 8127083, 8387611, 8780531, 9746027, 9965411.
- $\boxed{\alpha = 57}$: 587, 8059, 40627, 184523, 295459, 679699, 784219, 876523, 880667, 1102979, 1506907, 2125099, 3007547, 3231227, 3654067, 3850339, 3859019, 4111859, 4577723, 5078539, 6169123, 7618859, 7972499, 8273899.
- $\boxed{\alpha = 59}$: 467, 532331, 1174211, 1944323, 2066723, 3209867, 4420043, 7898291.
- $\boxed{\alpha = 67}$: 9467, 2908043, 3658427, 4440707, 7380467.
- $\boxed{\alpha = 73}$: 423587, 439787, 3909179.
- $\boxed{\alpha = 81}$: 84523, 127643, 464131, 1211603, 1362523, 3058051, 6892051, 7402363.
- $\boxed{\alpha = 83}$: 1114907, 2056667, 6501947.
- $\boxed{\alpha = 89}$: 8363, 953651, 2867771, 4961531, 7625603.
- $\boxed{\alpha = 97}$: 107699, 2010227, 4302203.

— $\boxed{\alpha = 99}$: 42083, 89051, 162523, 616003, 791363, 966011, 1189003, 1652731, 2486483, 3948731, 4328123, 4774843, 7137371, 7644443, 9991027.

Bibliographie

[1] J. Assim, Z. Bouazzaoui, Half-integral weight modular forms and real quadratic p-rational fields, *Funct. Approx. Comment. Math. 63 (2) 201 - 213, December 2020.*

[2] S.L. Aletheia-Zomlefer, L. Fukshansky, S.R. Garcia, The Bateman-Horn Conjecture : Heuristics, History, and Applications, *Expositiones Mathematicae, Vol 38, Issue 4, December 2020, Pages 430 – 479.*

[3] R. Barbulescu, J. Ray, Numerical verification of the Cohen-Lenstra-Martinet heuristics and of Greenberg's p-rationality conjecture, *Journal de Théorie des Nombres de Bordeaux, Tome 32 (2020) no. 1, pp. 159-177.*

[4] A. Brumer, On the units of algebraic number fields, *Mathematika 14 (1967), p. 121–124.*

[5] Y. Benmerieme, Les corps multi-quadratiques p-rationnels, Thèse de doctorat, Décembre 2021 (Direction : A. Movahhedi).

[6] Y. Benmerieme, A. Movahhedi, Multi-quadratic p-rational Number Fields, *Journal of Pure and Applied Algebra, Volume 225, Issue 9, 2021.*

[7] Z. Bouazzaoui, Fibonacci numbers and real quadratic p-rational fields, *Period Math Hung 81, 123–133 (2020).*

[8] D. Byeon, Indivisibility of Class Numbers and Iwasawa λ-Invariants of Real Quadratic Fields, *Compositio Mathematica 126 : 249 – 256, 2001.*

[9] J. Coates, p-adic L-functions and Iwasawa's theory, *Academic Press, Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975).*

[10] H. Cohen, A Course in Computational Algebraic Number Theory, *Graduate Texts in Mathematics, Springer-Verlag Berlin Heidelberg (1993)*

[11] H. Cohen, Number Theory, Volume I : Tools and Diophantine Equations, *Graduate Texts in Mathematics, Springer New York (2007).*

[12] P.T.D.A. Elliott, Probabilistic Number Theory I : Mean-Value Theorems, *Springer-Verlag, 1979.*

[13] W. J. Ellison, M. Mendès France, Les nombres premiers, *Publications de l'institut de mathématique de l'université de Nancago, IX, Hermann, 1975.*

[14] G. Gras, Class Field Theory, From Theory to Practice, *Springer Monographs in Mathematics, Springer-Verlag, 2003.*

[15] G. Gras, Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques, *Canadian Journal of Mathematics 68(3) (2016), 571—624.*

[16] G. Gras, On p-rationality of number fields. Applications – PARI/GP programs, *Publications Mathématiques de Besançon, no. 2 (2019), pp. 29-51.*

[17] G. Gras, Groupe de Galois de p-extension abélienne p-ramifiée maximale d'un corps de nombres, *January 1982, Journal für die reine und angewandte Mathematik (Crelles Journal).*

[18] R. Greenberg, Galois representations with open image, *Ann. Math. Québec 40, 83–119 (2016).*

[19] G.H. Hardy, M. Wright, An Introduction to the Theory of Numbers, Sixth Edition, *Oxford University Press, 2008.*

[20] P. Hartung, Proof of the Existence of Infinitely Many Imaginary Quadratic Fields Whose Class Number is Not Divisible by 3, *Journal of Number Theory, Volume 6, Issue 4, August 1974, Pages 276-278.*

[21] H. Iwaniec, E. Kowalski, Analytic Number Theory, *AMS Colloquium Publications, vol. 53, 2004.*

[22] J.-F. Jaulent, T. Nguyen Quang Do, Corps p-rationnels, corps p-réguliers, et ramification restreinte, *Journal de Théorie des Nombres de Bordeaux, Tome 5 (1993) no. 2, pp. 343-363.*

[23] Koch, Galois theory of p-extensions, *Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg (2002).*

[24] S. Louboutin, The Brauer-Siegel Theorem, *J. London Math. Soc. (2) 72 (2005) 40–52.*

[25] H. Miki, On the Leopoldt's Conjecture on the p-adic Regulators, *J. of Number Theory 26, 1987, 117 – 128.*

[26] D. Marcus, Number Fields, *Universitext, Springer (2018).*

[27] H. Miki, H. Sato, Leopoldt's Conjecture and Reiner's Theorem, *J. Math. Soc. Japan 36, num 1, 1984, 47 – 52.*

[28] A. Movahhedi, Sur les p-extensions des corps p-rationnels, *PhD Thesis, 1988.*

[29] A. Movahhedi, Sur les p-extensions des corps p-rationnels, *Math. Nachr. 149 (1990), 163–176.*

[30] 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, Volume 81, Birkhäuser Boston Inc, 1990.*

[31] J. Neukirch, Algebraic Number Theory, *Grundlehren der mathematischen Wissenschaften,Springer-Verlag Berlin Heidelberg (1999).*

[32] J. Neukirck, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Second Edition, *A Series of Comprehensive Studies in Mathematics 323.*

[33] T. Nguyen Quang Do, A. Movahhedi, Sur l'arithmétique des corps de nombres p-rationnels, *Séminaire de Théorie des Nombres, Paris 1987–88 (eds : Goldstein C.), Progress in Mathematics, vol. 81 Birkhäuser Boston.*

[34] T.Nguyen Quang Do, Unités de norme -1 d'un corps quadratique réel, *Séminaire Delange-Pisot-Poitou, Théorie des nombres, tome 17, no 2 (1975-1976), exp. no G6, p. G1-G3.*

[35] T.Nguyen Quang Do, On Greenberg's generalized conjecture for an infinite class of number fields, Preprint, 2015.

[36] F. Pitoun, F. Varescon, Computing the torsion of p-ramified module of a number field, *Mathematics of Computation, Vol.84, Num. 291, January 2015, pp. 371 – 383.*

[37] L. Ribes, P. Zaleski, Profinite groups, *A Series of Modern Surveys in Mathematics, Springer-Verlag Berlin Heidelberg (2010)*

[38] P. Samuel, Théorie algébrique des nombres.