# Les corps multi-quadratiques p-rationnels

Youssef Benmerieme

# THÈSE

PRÉSENTÉE POUR OBTENIR LE GRADE DE

## DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Discipline : **Mathématiques et Applications**

Par **Youssef BENMERIEME**

# Les corps multi-quadratiques $p$-rationnels

Sous la direction de **Abbas MOVAHHEDI**

Soutenue le 13 décembre 2021

Membres du jury :

M. Denis BENOIS, Professeur, Université de Bordeaux, Rapporteur.

M. Cornelius GREITHER, Professeur, Universität der Bundeswehr Müchen, Rapporteur.

M. Abdelmalek AZIZI, Professeur, Université Mohammed Premier (Maroc), Examinateur.

M. Stéphane René LOUBOUTIN, Professeur, Aix-Marseille Université, Examinateur.

M. Abbas MOVAHHEDI, Professeur, Université de Limoges, Directeur de thèse.

M. Hassan OUKHABA, Maître de conférences HDR, Université de Besançon, Examinateur.

M. Alain SALINIER, Professeur, Université de Limoges, Examinateur.

## Titre : Les corps multi-quadratiques $p$-rationnels

**Résumé :** Pour chaque nombre premier $p$, nous prouvons l'existence d'une infinité de corps quadratiques réels $p$-rationnels ainsi que l'existence d'un corps bi-quadratique réel et d'un corps bi-quadratique imaginaire $p$-rationnel. De plus pour $p = 3$, nous montrons l'existence d'une infinité de corps bi-quadratiques imaginaires 3-rationnels. Pour $p > 5$ et $F$ un corps multi-quadratique réel $p$-rationnel tels que le noyau modéré de $F$ est d'ordre premier à $p$, nous montrons l'existence d'une infinité d'extensions quadratiques imaginaires $p$-rationnelles de $F$. En utilisant une méthode récente développée par Greenberg, nous déduisons l'existence des extensions galoisiennes de $\mathbf{Q}$ dont les groupes de Galois sont isomorphes à des sous-groupes ouverts de $GL_n(\mathbf{Z}_p)$ pour $n = 4$ et $n = 5$ et au moins pour tout $p \leq 718.328.637$. Finalement, nous donnons une nouvelle reformulation des conjectures de Ankeny-Artin-Chowla et de Mordell, en terme de la $p$-rationalité de $\mathbf{Q}(\sqrt{p})$.

**Mots clés :** Corps de nombres $p$-rationnels, corps $(p,i)$-réguliers, représentations galoisiennes, conjectures de AAC et de Mordell.

---

## Title : Multi-quadratic $p$-rational number fields

**Abstract :** For each prime $p$, we prove the existence of infinitely many real quadratic $p$-rational number fields as well as the existence of a real and an imaginary bi-quadratic $p$-rational number field. Moreover for $p = 3$, we show the existence of infinitely many imaginary bi-quadratic 3-rational number fields. For $p > 5$ and $F$ a real multi-quadratic $p$-rational number field with tame kernel of ordre prime to $p$, we prove the existence of infinitely many imaginary quadratic extensions of $F$, $p$-rational. Using a recent method developed by Greenberg, we deduce the existence of Galois extensions of $\mathbf{Q}$ whose Galois groups are isomorphic to open subgroups of $GL_n(\mathbf{Z}_p)$ for $n = 4$ and $n = 5$ and at least for all $p \leq 718.328.637$. Finally, we give a new reformulation of the conjectures of Ankeny-Artin-Chowla and Mordell, in terms of the $p$-rationality of $\mathbf{Q}(\sqrt{p})$.

**Keywords :** $p$-rational number fields, $(p,i)$-regular fields, Galois representations, AAC and Mordell conjectures.

---

# Remerciement

D'abord, je remercie profondément mon directeur de thèse, M. Abbas Movahhedi, pour sa grande disponibilité, ses précieux conseils, sa sympathie. Il m'a transmis sa passion pour les mathématiques et plus particulièrement la théorie algébrique des nombres depuis tout mon premier contact avec lui en Master 2.

Je voudrais remercier également M. Denis Benois et M. Cornelius Greither pour l'intérêt qu'ils ont porté à mon travail en acceptant d'en être rapporteurs.

J'associe à ces remerciement M. Abdelmalek Azizi (mon ancien professeur à Oujda), M. Stéphane René Louboutin, M. Hassan Oukhaba et M. Alain Salinier qui m'ont fait l'honneur de participer au jury.

Je n'oublie pas les membres du département de mathématiques en particulier Henri Massias, Annie Nicolas, Sophie Queille, Débora Thomas et Yolande Vieceli que je remercie de tout mon coeur pour leur aide et support. Je remercie aussi les enseignants avec qui j'ai fait mes premiers pas dans l'enseignement en tant que moniteur puis comme ATER. Je pense à Pascale Sénéchaud et Pierre Dusart.

J'exprime ma gratitude à tous les professeurs qui m'ont enseigné depuis toute mon enfance ainsi à tous mes amis qui m'ont toujours encouragé.

Merci beaucoup à tous les thésards, pour l'ambiance : merci particulièrement à Hamza pour son amitié et les nombreuses questions mathématiques qu'on essayait de résoudre pendant les pauses, Gaurav pour les nombreuses discussions, Don pour sa gentillesse, Ali, Duc, Maxime ainsi Shahrzad avec qui j'ai partagé mon bureau ces dernières années.

Je souhaite dédier ce diplôme de doctorat à tous les membres de ma famille qui m'ont soutenu et encouragé. J'adresse mes plus sincères remerciements à mes parents pour tout ce qu'ils ont fait pour moi, je ne peux pas trouver les mots pour dire à quel point je leur suis reconnaissant. Je tiens à exprimer ma reconnaissance à ma chère femme Doha pour ces deux meilleures dernières années ensemble.

Enfin et surtout, que toutes les personnes qui n'ont pas été cité nommément trouvent ici l'expression de mes remerciements et de ma sincère gratitude.

*À la mémoire de :*
*mon père 1964-1993*
*mon grand-père 1932-2015*
*et ma grand-mère 1930-2015*

# *Table des matières*

# *Introduction*

Soit $p$ un nombre premier et $F$ un corps de nombres. Notons par $S$ l'ensemble des places de $F$ au-dessus de $p$ et par $F_S$ la pro-$p$-extension maximale de $F$ non-ramifiée en dehors des places de $S$. On dit que $F$ est $p$-rationnel lorsque le groupe de Galois $G(F_S/F)$ est un pro-$p$-groupe libre. Cette notion a été introduite et étudiée dans [59, 60, 61], notamment pour construire des familles infinités de corps de nombres non-abéliens satisfaisant la conjecture de Leopoldt en $p$. Récemment, les corps $p$-rationnels ont été revisité par Greenberg dans le but d'étudier certaines représentations du groupe de Galois absolu du corps $\mathbf{Q}$ des nombres rationnels. Il a conjecturé l'existence, pour tout nombre premier impair $p$ et tout entier naturel $t$, d'un corps $p$-rationnel dont le groupe de Galois sur $\mathbf{Q}$ est isomorphe à $(\mathbf{Z}/2)^t$ ([31, Conjecture 4.8]), ce qui a motivé ce travail. En fait, cette conjecture a motivé de nombreux auteurs tels que Assim et Bouazzaoui ([5]), Barbulescu et Ray ([8]), Gras ([26]) et le tout dernier travail de Koperecz ([47]).

Cette thèse est organisée comme suit. Dans le Chapitre 1, nous passons en revue les différentes notions que nous utiliserons le long de ce manuscrit. Nous commençons par les fonctions $L$ de Dirichlet et les fonctions $L$ $p$-adiques qui nous permettent de caractériser la $p$-rationalité des corps quadratiques réels, puis nous faisons le lien avec la fonction zêta de Dedekind en donnant la formule du nombre de classes, ensuite nous rappelons la formule de Coates qui interprète l'ordre du $p$-groupe $T_F$ où $T_F$ est le groupe de torsion du groupe de Galois de la pro-$p$-extension abélienne maximale de $F$ non-ramifiée en dehors des places de $S$, en fonction des invariants de $F$ et à la fin, nous présentons le théorème de Wiles qui est une conséquence de la preuve de la conjecture principale dans la théorie d'Iwasawa et qui nous permet surtout dans le Chapitre 3 de donner une condition nécessaire et suffisante pour la montée de la $p$-rationalité dans certains cas.

Dans le Chapitre 2, nous rappelons en détail la notion de corps de nombres $p$-rationnel et nous fournissons plusieurs équivalences pour qu'un corps de nombres arbitraire soit $p$-rationnel, en accordant une attention particulière au cas où le corps de nombres est totale-

ment réel. En particulier, nous donnons des preuves alternatives pour qu'un corps quadratique soit $p$-rationnel, ce qui nous permet de montrer l'existence d'une part, d'une infinité de corps bi-quadratiques imaginaires 3-rationnels et d'autre part, d'une infinité de corps quadratiques réels $p$-rationnels pour chaque nombre premier $p$. Nous prouvons pour un corps multi-quadratique réel $p$-rationnel $F$ avec $p > 5$ ne divisant pas l'ordre du noyau modéré $K_2(o_F)$, l'existence d'une infinité d'extensions quadratiques imaginaires $p$-rationnelles de $F$. Ensuite pour chaque premier $p$, nous construisons un corps bi-quadratique réel et un corps bi-quadratique imaginaire $p$-rationnels, à savoir, $\mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{p(p-2)}\right)$ et $\mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{-p}\right)$. En utilisant une méthode récente développée par Greenberg, nous déduisons l'existence des extensions galoisiennes de $\mathbf{Q}$ dont les groupes de Galois sont isomorphes à des sous-groupes ouverts de $GL_n(\mathbf{Z}_p)$ pour $n = 4$ et $n = 5$ et au moins pour tout $p \leq 718.328.637$.

Enfin dans le Chapitre 3, nous donnons une caractérisation de la $p$-rationalité de $\mathbf{Q}(\sqrt{p})$ à l'aide des nombres de Bernoulli ordinaires ou généralisés suivant que $p$ est congru à 1 ou 3 (mod 4). Plus précisément, pour $p \equiv 1 \pmod 4$ (resp. $p \equiv 3 \pmod 4$), $\mathbf{Q}(\sqrt{p})$ est $p$-rationnel si et seulement si $B_{\frac{p-1}{2}}$ (resp. $B_{\frac{p-1}{2},\chi_{\mathbf{Q}(\sqrt{-1})}}$) est une unité $p$-adique. Cela nous permet ensuite, d'interpréter la conjecture AAC et la conjecture de Mordell concernant l'unité fondamentale de $\mathbf{Q}(\sqrt{p})$, en terme de la $p$-rationalité. Finalement, pour $p \equiv 1 \pmod 4$, nous donnons une condition nécessaire et suffisante pour la montée de la $p$-rationalité en rajoutant $\sqrt{p}$ à un corps multi-quadratique réel.

# *Introduction*

Let $p$ be a prime number and let $F$ be a number field. Let $S$ denote the set of places of $F$ above $p$ and $F_S$ denote the maximal pro-$p$-extension of $F$ unramified outside $S$. We say that $F$ is $p$-rational when the Galois group $G(F_S/F)$ is a free pro-$p$-group. This notion was introduced and studied in [59, 60, 61], in particular to construct infinite families of non-abelian number fields satisfying the Leopoldt conjecture at $p$. Recently, the $p$-rational fields have been revisited by Greenberg in order to study some representations of the absolute Galois group of the field $\mathbf{Q}$ of rational numbers. He conjectured that for any odd prime $p$ and any natural integer $t$, there exists a $p$-rational number field whose Galois group over $\mathbf{Q}$ is isomorphic to $(\mathbf{Z}/2)^t$ ([31, Conjecture 4.8]), which motivated this work. In fact, this conjecture has motivated many authors such as Assim and Bouazzaoui ([5]), Barbulescu and Ray ([8]), Gras ([26]) and the latest work of Koperecz ([47]).

This thesis is organized as follows. In Chapter 1, we review the different notions that we will use throughout this manuscript. We start with Dirichlet $L$-functions and $p$-adic $L$-functions which allow us to characterize the $p$-rationality of real quadratic fields, then we make the link with the Dedekind $\zeta$-function by giving class number formula. Next, we recall Coates's formula which interprets the order of the $p$-group $T_F$ where $T_F$ is the torsion group of Galois group of maximal abelian pro-$p$-extension of $F$ unramified outside $S$, in terms of invariants of $F$ and at the end, we present Wiles's theorem which is a consequence of the proof of the main conjecture in Iwasawa theory and which allows us especially in Chapter 3 to give a necessary and sufficient condition for $p$-rationality to arise in certain cases.

In Chapter 2, we recall in details the notion of $p$-rational number field and provide several equivalences for an arbitrary number field to be $p$-rational, with particular attention to the case where the number field is totally real. In particular, we give alternative proofs for a real quadratic field to be $p$-rational, which allows us to show the existence of infinitely many imaginary bi-quadratic 3-rational number fields on the one hand, and of infinitely many real quadratic $p$-rational fields for each prime $p$ on the other hand. We prove for a

real multi-quadratic $p$-rational field $F$ with $p > 5$ not dividing the order of the tame kernel $K_2(o_F)$, the existence of infinitely many imaginary quadratic $p$-rational extensions of $F$. Then for each prime $p$, we construct a real and an imaginary bi-quadratic $p$-rational fields, namely, $\mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{p(p-2)}\right)$ and $\mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{-p}\right)$. Using a recent method developed by Greenberg, we deduce the existence of Galois extensions of $\mathbf{Q}$ whose Galois groups are isomorphic to open subgroups of $GL_n(\mathbf{Z}_p)$ for $n = 4$ and $n = 5$ and at least for all $p \leq 718.328.637$.

At the end, in Chapter 3, we give a characterization of $p$-rationality of $\mathbf{Q}(\sqrt{p})$ using ordinary or generalized Bernoulli numbers depending on whether $p$ is congruent to 1 or 3 (mod 4). More precisely, for $p \equiv 1 \pmod 4$ (resp. $p \equiv 3 \pmod 4$), $\mathbf{Q}(\sqrt{p})$ is $p$-rational if and only if $B_{\frac{p-1}{2}}$ (resp. $B_{\frac{p-1}{2},\chi_{\mathbf{Q}(\sqrt{-1})}}$) is a $p$-adic unit. This allows us then, to interpret the AAC conjecture and Mordell's conjecture concerning the fundamental unit of $\mathbf{Q}(\sqrt{p})$, in terms of $p$-rationality. Finally, for $p \equiv 1 \pmod 4$, we give a necessary and sufficient condition for $p$-rationality to arise by adding $\sqrt{p}$ to a real multi-quadratic field.

# 1 Préliminaires

*Dans ce chapitre nous passons en revue les différentes notions que nous utiliserons le long de ce manuscrit. Nous commençons par les fonctions L de Dirichlet et les fonctions L $p$-adiques pour donner des caractérisations de la $p$-rationalité dans les chapitres suivants, puis nous faisons le lien avec la fonction zêta de Dedekind en donnant la formule du nombres de classes, ensuite nous rappelons la formule de Coates qui interprète l'ordre du $p$-groupe $T_F$ où $T_F$ est le groupe de torsion du groupe de Galois de la pro-$p$-extension abélienne maximale de $F$ non-ramifiée en dehors des places de $S$, en fonction des invariants du corps de nombres $F$ et à la fin, nous présentons le théorème de Wiles qui est une conséquence de la preuve de la conjecture principale dans la théorie d'Iwasawa et qui nous permet surtout dans le Chapitre 3 de donner une condition nécessaire et suffisante pour la montée de la $p$-rationalité dans certains cas.*

## 1.1 Fonctions $L$ de Dirichlet et la fonction $L$ $p$-adique

Commençons par introduire les fonctions $L$ de Dirichlet. Soit $n \in \mathbf{N}^\times$. Un caractère de Dirichlet $\chi$ est défini comme étant un morphisme :

$$\chi : (\mathbf{Z}/n\mathbf{Z})^\times \to \mathbf{C}^\times,$$

que l'on étend à $\mathbf{Z}$ en posant $\chi(k) = 0$ pour $k$ non premier à $n$. Pour un entier $m$ tel que $n \mid m$, on a un morphisme naturel de $(\mathbf{Z}/m\mathbf{Z})^\times$ vers $(\mathbf{Z}/n\mathbf{Z})^\times$ et $\chi$ induit un morphisme $(\mathbf{Z}/m\mathbf{Z})^\times \to \mathbf{C}^\times$. Le caractère $\chi$ est le même que ce soit (mod $m$) ou (mod $n$) et on peut alors choisir l'entier $n$ de tel sorte que ça soit le plus petit, un tel $n$ noté $f_\chi$ (ou simplement $f$) est appelé le conducteur de $\chi$. Si $\chi$ est défini (mod $f_\chi$), le caractère est dit primitif. On dit que $\chi$ est pair (resp. impair) si $\chi(-1) = 1$ (resp. $\chi(-1) = -1$).

La fonction $L$ de Dirichlet associée à $\chi$ est donc donnée par :

$$L(s,\chi) = \sum_{k \geq 1} \frac{\chi(k)}{k^s},$$

où $s \in \mathbf{C}$ dont la partie réelle $\Re(s) > 1$. Lorsque $\chi$ est trivial ($\chi(k) = 1$, pour tout $k \in \mathbf{N}^\times$, ce caractère sera noté par la suite $\chi_0$), nous obtenons la fameuse fonction $\zeta$ de Riemann. Notons que si $\chi \neq \chi_0$, $L(s,\chi)$ converge pour tout $s \in \mathbf{C}$ avec $\Re(s) > 0$ et peut être étendue en une fonction analytique à tout point du plan complexe. Dirichlet a introduit la notion de fonctions $L$ dans le but de montrer, pour chaque couple d'entiers $(a,m)$ premiers entre eux, l'existence d'une infinité de nombres premiers congrus à $a \pmod{m}$. L'une des utilisations de ces fonctions et que l'on va voir plus tard, est pour avoir des informations sur le nombre de classes d'un corps de nombres qui reste toujours difficile à calculer.

Pour des valeurs spécifiques pour $s$, nous pouvons décrire ces fonctions en terme de nombres de Bernoulli ordinaires ou généralisés. D'abord, les nombres de Bernoulli ordinaires $B_n$ sont définis par :

$$\frac{t}{e^t - 1} = \sum_{n \geq 0} B_n \frac{t^n}{n!}.$$

Et plus généralement, pour un caractère $\chi$ ayant $f$ comme conducteur, les nombres de Bernoulli généralisés $B_{n,\chi}$ sont définis par :

$$\sum_{a=1}^{f} \frac{\chi(a)\, t e^{at}}{e^{ft} - 1} = \sum_{n \geq 0} B_{n,\chi} \frac{t^n}{n!}.$$

Lorsque $\chi$ est trivial, $B_{n,\chi} = B_n$ sauf pour $n = 1$. Nous avons donc le théorème suivant :

**Théorème 1.1.1.** *([74, Theorem 4.2]) Soit $\chi$ un caractère de Dirichlet. Pour tout entier naturel non nul $n$,*

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}.$$

Notons que $L(1-n,\chi)$ est non nul si et seulement si $\chi$ et $n$ ont la même parité ([37, Theorem 2]). Il est démontré que si $\chi \neq \chi_0$, $f_\chi B_{n,\chi}$ est un entier pour tout $n \geq 1$ (([37, fin du Chap. 2])) et lorsque le conducteur $f_\chi$ est divisible par au moins deux nombres premiers, alors $L(1-n,\chi)$ est aussi un entier ([17, Theorem 1]). Lorsque $\chi$ est trivial, nous avons :

$$\zeta(1-n) = -\frac{B_n}{n}.$$

Pour définir la fonction $L$ $p$-adique, nous aurons besoin des notations suivantes. Soit $p$ un nombre premier, on pose :

$$q := \begin{cases} p & \text{si } p \neq 2, \\ 4 & \text{si } p = 2. \end{cases}$$

Nous rappelons que l'anneau des entiers $p$-adiques $\mathbf{Z}_p$ contient exactement $\phi(q)$ racines

distinctes de l'unité où $\phi$ est l'indicatrice d'Euler.

**Définition 1.1.2.** *Le caractère de Teichmüller $\omega$ est un homomorphisme de groupes multiplicatifs :*

$$\omega : \quad (\mathbf{Z}/q\mathbf{Z})^\times \quad \to \quad \mathbf{Z}_p^\times$$

*de sorte que $\omega(a)$ est l'unique $\phi(q)^{ème}$ racine de l'unité dans $\mathbf{Z}_p$ qui est congrue à $a \pmod p$.*

Soit $\overline{\mathbf{Q}_p}$ une clôture algébrique de $\mathbf{Q}_p$. D'après la théorie générale, la valuation $p$-adique $v_p$ se prolonge de manière unique en une valuation sur $\overline{\mathbf{Q}_p}$. On note par $\mathbf{C}_p$ le complété de $\overline{\mathbf{Q}_p}$. La fonction $L$ $p$-adique est définie grâce au théorème suivant :

**Théorème 1.1.3.** *([74, Theorem 5.11]) Soit $\chi$ un caractère de Dirichlet de conducteur $f$. Alors il existe une fonction $p$-adique méromorphe (analytique si $\chi \neq \chi_0$) $L_p(s,\chi)$ sur $\{s \in \mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$ telle que,*

$$L_p(1-n,\chi) = -\left(1-\chi\omega^{-n}(p)p^{n-1}\right)\frac{B_{n,\chi\omega^{-n}}}{n}, \quad n \geq 1.$$

*Si $\chi = \chi_0$, alors $L_p(s,\chi)$ est analytique sauf en un pôle simple en $s = 1$ de résidu $(1-1/p)$.*

Notons que pour tout entier non nul $n$ divisible par $p-1$ (par 2 si $p = 2$), nous avons

$$L_p(1-n,\chi) = \left(1-\chi(p)p^{n-1}\right)L(1-n,\chi). \tag{1.1}$$

Une des propriétés de ces fonctions est la suivante :

**Lemme 1.1.4.** *([74, Corollary 5.13]) Soit $\chi$ un caractère non trivial de conducteur $f$ tel que $pq \nmid f$. Soit $m, n \in \mathbf{Z}$. Alors*

$$L_p(m,\chi) \equiv L_p(n,\chi) \pmod p,$$

*et les deux membres sont $p$-entiers.*

Par la suite, le caractère $\chi$ est le plus souvent quadratique, i.e. associé à un corps quadratique, dans ce cas, nous savons l'expression explicite de $\chi$ que nous allons détailler maintenant. Soit $F$ un corps quadratique de discriminant $d$. On appelle caractère associé à $F$, le caractère non trivial noté $\chi_F$, ayant $f = |d|$ pour conducteur et défini par :

$$\chi_F(m) = \left(\frac{d}{m}\right),$$

où $\left(\frac{d}{\cdot}\right)$ est le symbole de Kronecker. En particulier,

$$\chi_F(-1) = \begin{cases} 1 & \text{si } F \text{ est réel,} \\ -1 & \text{si } F \text{ est imaginaire.} \end{cases}$$

De plus nous avons l'interprétation de la ramification d'un nombre premier $p$ dans $F$ en terme de la valeur de $\chi_F(p)$, plus précisément, $p$ est ramifié, décomposé ou inerte dans $F$ respectivement lorsque $\chi_F(p) = 0$, $\chi_F(p) = 1$ ou $\chi_F(p) = -1$.

## 1.2 Fonction zêta de Dedekind et le nombre de classes

La fonction zêta de Dedekind d'un corps de nombres est liée aussi aux fonctions $L$ de Dirichlet. Soit $F$ un corps de nombres et $o_F$ son anneau des entiers. Pour un idéal non-nul $I$ de $o_F$, l'anneau $o_F/I$ est toujours fini dont le cardinal est noté $N(I)$. La fonction zêta de Dedekind $\zeta_F$ de $F$ est alors définie par :

$$\zeta_F(s) = \sum N(I)^{-s},$$

où $s > 1$ est un nombre complexe tel que $\Re(s) > 1$ et $I$ parcourt l'ensemble des idéaux non-nuls de $o_F$. Le théorème suivant permet de faire le lien entre la fonction zêta de Dedekind et les fonctions $L$ de Dirichlet :

**Théorème 1.2.1.** *Soit $F$ un corps de nombres abélien sur $\mathbf{Q}$, alors*

$$\zeta_F(s) = \prod L(s, \chi),$$

*où $\chi$ parcourt l'ensemble des caractères du groupe de Galois* $\mathrm{Gal}(F/\mathbf{Q})$.

Il est connu que $\zeta_F$ admet un prolongement méromorphe à $\mathbf{C}$ tout entier, holomorphe en dehors d'un pôle simple en $s = 1$ avec résidu encodant des informations sur les invariants de $F$ comme le nombre de classes. Plus précisément [22, Théorème 1.6.1] :

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{w_F\sqrt{|d_F|}}, \tag{1.2}$$

où $h_F$, $R_F$ et $d_F$ sont respectivement le nombre de classes, le régulateur et le discriminant de $F$, $r_1$ (resp. $r_2$) est le nombre de places réelles (resp. complexes) de $F$ et $w_F$ est le nombre des racines de l'unité dans $F$. En particulier si $F = \mathbf{Q}$, le résidu de la fonction zêta de Riemann en

$s = 1$ est égal à 1 et lorsque $F$ est quadratique, le Théorème 1.2.1 entraine que

$$\lim_{s\to 1}(s-1)\zeta_F(s) = L(1,\chi_F).$$

Si de plus $F$ est imaginaire. Par l'égalité (1.2) on trouve :

$$h_F = \frac{w_F\sqrt{|d_F|}}{2\pi}L(1,\chi_F).$$

Landau a montré ([48, Theorem 219] ) qu'on peut re-écrire cette dernière égalité en fonction du symbole de Kronecker :

**Théorème 1.2.2.** *Soit $d_F$ le discriminant du corps quadratique imaginaire $F$, Alors*

$$h_F = \frac{w_F}{2[2-\left(\frac{d_F}{2}\right)]}\sum_r\left(\frac{d_F}{r}\right),$$

*où $w_F = 2,4$ ou $6$ est le nombre des racines de l'unité dans $F$ et la somme est prise sur tous les entiers $r$ entre $1$ et $-d_F/2$.*

En utilisant ce théorème, nous pouvons avoir une borne supérieure pour le nombre de classes, par exemple si $F = \mathbf{Q}(\sqrt{-p})$ où $p > 3$ est un nombre premier, nous avons $w = 2$ et

$$d_F = \begin{cases} -p & \text{si } p \equiv 3 \pmod 4, \\ -4p & \text{si } p \equiv 1 \pmod 4. \end{cases}$$

Lorsque $d_F = -p$, on a $\left(\frac{d_F}{2}\right) = \pm 1$, ainsi

$$h_F = \frac{1}{2-\left(\frac{d_F}{2}\right)}\sum_1^{p/2}\left(\frac{d_F}{r}\right) \leq 1 \times p/2 < p.$$

Dans l'autre cas, si $d_F = -4p$, alors $\left(\frac{d_F}{2}\right) = 0$ et donc

$$h_F = \frac{1}{2}\sum_1^{2p}\left(\frac{d_F}{r}\right) \leq 1/2 \times 2(p-1) < p.$$

Par conséquent, le nombre de classes de $\mathbf{Q}\left(\sqrt{-p}\right)$ est toujours strictement inférieur à $p$. Comme nous le verrons au chapitre 2, ce résultat suffit pour assurer la $p$-rationalité de $\mathbf{Q}(\sqrt{-p})$.

Si maintenant $F$ est réel, la situation est plus difficile dû à la nécessité de connaitre l'unité

fondamentale. Plus précisément, la formule du nombre de classes qu'on peut déduire par l'égalité (1.2) est donnée par :

$$h_F = \frac{L(1,\chi_F)\sqrt{d_F}}{2R_F}, \tag{1.3}$$

où $R_F = \log(\varepsilon)$ avec $\varepsilon$ est l'unité fondamentale de $F$. Souvent, nous ne savons pas comment calculer le nombre de classes d'un corps quadratique réel, cependant, nous avons des bornes supérieurs, nous citons par exemple le théorème de Mao hua Le qui sera utilisé dans le chapitre suivant :

**Théorème 1.2.3.** *( [49, Theorem (a)] ) Soit $d$ le discriminant d'un corps quadratique réel et $h$ son nombre de classes, alors*

$$h < \frac{\sqrt{d}}{2}.$$

Ce résultat était aussi démontré plus tard par Ramaré pour les $d \geq 16$ (voir [67, Corollary 2]). Nous avons aussi les travaux de Louboutin qui a beaucoup travaillé sur les fonctions $L$ de Dirichlet, nous citons par exemple l'une des majorations du terme $L(1,\chi_F)$ que nous allons utiliser par la suite. Pour un résultat plus général, nous renvoyons le lecteur vers [52, Corollary 2].

**Corollaire 1.2.4.** *Soit $F$ un corps quadratique réel de conducteur $f$. Alors*

$$L(1,\chi_F) \leqslant \begin{cases} \left(\log f + \kappa_1\right)/2 & si\ \chi_F(2) = +1, \\ \left(\log f + \kappa_2\right)/4 & si\ \chi_F(2) = 0, \\ \left(\log f + \kappa_3\right)/6 & si\ \chi_F(2) = -1 \end{cases}$$

*où*

$$\begin{cases} \kappa_1 := 2 + \gamma - \log(4\pi) = 0.04619\cdots \\ \kappa_2 := 2 + \gamma - \log(\pi) = 1.43248\cdots \\ \kappa_3 := 2 + \gamma - \log(\pi/4) = 2.81878\cdots \end{cases}$$

*et $\gamma = 0,577\ldots$ désigne la constante d'Euler.*

## 1.3 L'ordre de $T_F$

Soit $p$ un nombre premier. Une extension de corps de nombres sera appelée une $p$-extension (resp. pro-$p$-extension) si elle est galoisienne et si son groupe de Galois est un $p$-groupe fini (resp. pro-$p$-groupe). Pour un corps de nombres $F$, on note par $S$ l'ensemble des places de $F$ au-dessus de $p$. Une extension de $F$ est dite $S$-ramifiée ou $p$-ramifiée, si elle est non ramifiée en dehors des places de $S$. Une $\mathbf{Z}_p$-extension de $F$ est une extension galoisienne dont le

groupe de Galois est isomorphe au groupe additif $\mathbf{Z}_p$. Toute $\mathbf{Z}_p$-extension est $p$-ramifiée. Notons par $F_S^{ab}$ la pro-$p$-extension abélienne $p$-ramifiée maximale de $F$. D'après la théorie du corps de classes :

$$\mathrm{Gal}(F_S^{ab}/F) \cong T_F \oplus \mathbf{Z}_p^{r_2+1+\delta_F}, \tag{1.4}$$

où $T_F$ est un $p$-groupe fini appelé le groupe de torsion de $\mathrm{Gal}(F_S^{ab}/F)$, $r_2$ le nombre de places imaginaires de $F$ et $\delta_F$ est le défaut de la conjecture de Leopoldt de $F$ en $p$. Cette conjecture affirme que $\delta_F$ est toujours nul. Autrement dit, si $\tilde{F}$ désigne le composé de toutes les $\mathbf{Z}_p$-extensions de $F$, alors la conjecture de Leopoldt est équivalente au fait que :

$$\mathrm{Gal}(\tilde{F}/F) \cong \mathbf{Z}_p^{r_2+1}.$$

Cette conjecture a été démontrée pour les extensions abéliennes de $\mathbf{Q}$ ou d'un corps quadratique imaginaire [7, 15].

Lorsque le corps $F$ est totalement réel, la conjecture de Leopoldt est équivalente dans ce cas, avec l'égalité entre $\tilde{F}$ et la $\mathbf{Z}_p$-extension cyclotomique, de plus lorsque $p$ est impair, ceci est exprimé par le fait que le régulateur $p$-adique $R_{p,F}$ est non nul (lorsque le corps totalement réel $F$ est quadratique, le régulateur $p$-adique $R_{p,F}$ est égal au $\log_p(\epsilon_0)$ où $\epsilon_0$ est l'unité fondamentale de $F$ et $\log_p$ est le logarithme $p$-adique). Nous avons alors, la formule remarquable suivante qui lie l'ordre de $T_F$ avec $R_{p,F}$ qui a été prouvée par Coates :

**Lemme 1.3.1.** *([20, Appendix, Lemma 8]) Soient $F$ un corps de nombres totalement réel et $p$ un nombre premier impair. Supposons que $R_{p,F} \neq 0$, alors*

$$|T_F| \sim_p |\mu_{p^\infty} \cap F(\mu_p)| \frac{h_F R_{p,F}}{\sqrt{d_F}} \prod_{\mathfrak{p}|p} (1 - (N(\mathfrak{p}))^{-1}). \tag{1.5}$$

$\sim_p$ représente l'égalité modulo une unité $p$-adique, i.e. Les deux termes ont même valuation $p$-adique, et $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de $o_F$ au-dessus de $p$. La formule ci-dessus fournit théoriquement un moyen de tester la $p$-rationalité des corps de nombres totalement réels. Nous donnerons les détails dans le chapitre suivant.

Soit $\zeta_{F,p}$ la fonction zêta $p$-adique de $F$. Le résidu de $\zeta_{F,p}$ en $s = 1$ est donné par [23]

$$\lim_{s\to 1}(s-1)\zeta_{F,p}(s) = \frac{2^{r-1} h_F R_{p,F}}{\sqrt{d_F}} \prod_{\mathfrak{p}|p} (1 - (N\mathfrak{p})^{-1}),$$

et la conjecture de Leopoldt pour $F$ en $p$ (qui affirme la non nullité de $R_{p,F}$) est valable pré-

cisément lorsque $\zeta_{F,p}$ a un pôle simple en $s = 1$. Ainsi, par la formule (1.5), l'ordre de $T_F$ est exprimé par le résidu de $\zeta_{F,p}$ en $s = 1$

$$|T_F| \sim_p |\mu_{p^\infty} \cap F(\mu_p)| \lim_{s\to 1}(s-1)\zeta_{F,p}(s). \tag{1.6}$$

## 1.4 Noyau modéré $K_2$ de l'anneau des entiers

Soit $F$ un corps de nombres et $o_F$ son anneau des entiers. Le $K$-groupe de Milnor $K_2(o_F)$, appelé aussi le noyau modéré de $F$, est un groupe abélien d'ordre fini. Il peut être défini comme étant le noyau de l'application modérée

$$K_2(F) \longrightarrow \oplus_{\mathfrak{p}}(o_F/\mathfrak{p})^\times,$$

où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de $o_F$ et $K_2(F)$ est le quotient de $F^\times \otimes F^\times$ par le sous-groupe engendré par les éléments $a \otimes (1-a)$, avec $a \neq 0, 1$. L'application ci-dessus est définie par $\oplus\tau_{\mathfrak{p}}$ où $\tau_{\mathfrak{p}}$ est le symbole modéré : pour chaque idéal premier $\mathfrak{p}$ de $o_F$, l'application

$$\tau_{\mathfrak{p}} : K_2(F) \to (o_F/\mathfrak{p})^\times$$

est définie par

$$\tau_{\mathfrak{p}}(a,b) = (-1)^{v_{\mathfrak{p}}(a)v_{\mathfrak{p}}(b)} a^{v_{\mathfrak{p}}(b)} b^{-v_{\mathfrak{p}}(a)} \pmod{\mathfrak{p}},$$

où $v_{\mathfrak{p}}$ est la valuation $\mathfrak{p}$-adique [69, Chap. XIV].

Lorsque le corps $F$ est totalement réel, nous avons la conjecture de Birch-Tate qui stipule que

$$|K_2(o_F)| = \pm w_2(F) \cdot \zeta_F(-1), \tag{1.7}$$

où de façons plus générale pour un entier $i > 0$, $w_i(F)$ désigne l'ordre du groupe de cohomologie galoisien $H^0(G_F, \mathbf{Q}/\mathbf{Z}(i))$ avec pour coefficients le $G_F$-module $\mathbf{Q}/\mathbf{Z}$ tordu $i$ fois et $G_F$ est le groupe de Galois absolu de $F$. Notons que $w_i(F)$ est défini même si $F$ n'est pas totalement réel. La $p$-partie de $w_i(F)$ pour $p$ un nombre premier, est la puissance maximale $p^m$, telle que l'exposant du groupe de Galois $\mathrm{Gal}(F(\mu_{p^m})/F)$ divise $i$. Si $F$ est totalement réel et $p$ est impair, la dernière condition pour $i = 2$ est équivalente au fait que $F$ contient le sous-corps réel maximal $\mathbf{Q}\left(\mu_{p^m}\right)^+$ de $\mathbf{Q}\left(\mu_{p^m}\right)$.

Comme conséquence de la preuve de la conjecture principale dans la théorie d'Iwasawa, Wiles a prouvé [75, Theorem 1.6] :

**Théorème 1.4.1.** *Soit $F$ un corps de nombres totalement réel et $p$ un nombre premier impair. Pour tout entier pair non-nul $i$,*

$$\zeta_F(1-i) \sim_p \frac{|H^2(o'_F, \mathbf{Z}_p(i))|}{|H^1(o'_F, \mathbf{Z}_p(i))|}.$$

Sous les hypothèses du théorème ci-dessus, $H^1(o'_F, \mathbf{Z}_p(i))$ est fini et isomorphe au groupe de cohomologie galoisien $H^0(G_F, \mathbf{Q}_p/\mathbf{Z}_p(i))$. Ainsi, d'après le paragraphe précédent, $|H^1(o'_F, \mathbf{Z}_p(i))|$ est la partie $p$-primaire de $w_i(F)$. D'autre part, par le calcul de Tate du groupe $K_2$

$$K_2(o_F) \otimes \mathbf{Z}_p \cong H^2(o'_F, \mathbf{Z}/p(2)),$$

qui est un cas particulier de la conjecture de Quillen-Lichtenbaum. Ainsi, à multiplication près par une puissance de 2, nous avons :

$$\zeta_F(1-i) = \pm \prod_{p>2} \frac{|H^2(o'_F, \mathbf{Z}_p(i))|}{|H^1(o'_F, \mathbf{Z}_p(i))|} = \pm \frac{|K_2(o_F)|}{w_i(F)},$$

qui sont des égalités lorsque $F/\mathbf{Q}$ est abélien avec $i = 2$ ([45, Introduction]). En particulier, la conjecture de Birch-Tate est vraie pour les corps totalement réels abéliens sur $\mathbf{Q}$.

# 2 La conjecture de Greenberg

*Dans ce chapitre, nous rappelons la notion de corps de nombres $p$-rationnel et nous fournissons plusieurs équivalences pour qu'un corps de nombres arbitraire soit $p$-rationnel, en accordant une attention particulière au cas où le corps de nombres est totalement réel. En particulier, nous donnons des preuves alternatives pour qu'un corps quadratique soit $p$-rationnel, ce qui nous permet de montrer l'existence d'une part, d'une infinité de corps bi-quadratiques imaginaires $3$-rationnels et d'autre part, d'une infinité de corps quadratiques réels $p$-rationnels pour chaque nombre premier $p$. Nous prouvons pour un corps multi-quadratique réel $p$-rationnel $F$ avec $p > 5$ ne divisant pas l'ordre du noyau modéré $K_2(o_F)$, l'existence d'une infinité d'extensions quadratiques imaginaires $p$-rationnels de $F$. Ensuite pour chaque premier $p$, nous construisons un corps bi-quadratique réel et un corps bi-quadratique imaginaire $p$-rationnels. En utilisant une méthode récente développée par Greenberg, nous déduisons l'existence des extensions galoisiennes de $\mathbf{Q}$ dont les groupes de Galois sont isomorphes à des sous-groupes ouverts de $GL_n(\mathbf{Z}_p)$ pour $n = 4$ et $n = 5$ et au moins pour tout $p \leq 718.328.637$. Notons que la plupart de ces résultats se trouvent dans notre article [12].*

## 2.1 Corps $p$-rationnels

Soit $p$ un nombre premier. Nous allons donner dans cette section, plusieurs caractérisations de la notion de corps de nombres $p$-rationnel (voir [59, 60, 61]).

Soit $F$ un corps de nombres. Notons par $S$ l'ensemble des places au-dessus de $p$ et par $F_S$ la pro-$p$-extension $p$-ramifiée maximale de $F$. On dit que $F$ est $p$-rationnel lorsque le pro-$p$-groupe $G_S(F) := \mathrm{Gal}(F_S/F)$ est libre.

Par la caractéristique d'Euler-Poincaré

$$\chi(G_S(F)) = 1 - d(G_S(F)) + r(G_S(F)) = -r_2,$$

où $r_2$ est le nombre de places complexes de $F$, $d(G_S(F)) = \dim H^1(G_S(F), \mathbf{Z}/p\mathbf{Z})$ le nombre minimal de générateurs ou tout simplement le rang de $G_S(F)$ et $r(G_S(F)) = \dim H^2(G_S(F), \mathbf{Z}/p\mathbf{Z})$ le nombre minimal de relations de $G_S(F)$. Puisque le fait que le pro-$p$-groupe $G_S(F)$ est libre est équivalent à la nullité de $r(G_S(F))$, alors $G_S(F)$ est de rang $r_2+1$ lorsque $F$ est $p$-rationnel et sa $p$-rationalité est équivalente au fait que le groupe abélianisé $X_F := G_S(F)^{ab} = \mathrm{Gal}(F_S^{ab}/F)$, où $F_S^{ab}$ désigne la pro-$p$-extension abélienne $p$-ramifiée maximale de $F$, est un $\mathbf{Z}_p$-module libre de rang $r_2+1$ :

$$X_F \cong \mathbf{Z}_p^{1+r_2}.$$

En d'autres termes, par la formule (1.4), un corps de nombres $F$ est $p$-rationnel précisément lorsque $F$ satisfait la conjecture de Leopoldt en $p$ et que le module de torsion $T_F := \mathrm{Tor}_{\mathbf{Z}_p}(X_F)$ est trivial.

On peut aussi caractériser la $p$-rationalité à l'aide de la notion d'éléments $p$-hyper-primaires. Un élément $\alpha \in F^\times$ est appelé $p$-hyper-primaire si $\alpha o_F = \mathfrak{a}^p$ pour un certain idéal fractionnaire $\mathfrak{a}$ de $F$ et $\alpha \in (F_v^\times)^p$ pour toutes les places $v$ de $F$ au-dessus de $p$. Ici $F_v$ désigne le complété de $F$ en $v$. Soit $\mathscr{H}_p(F)$ l'ensemble des éléments $p$-hyper-primaires de $F$. Alors $F$ est $p$-rationnel précisément lorsque les deux conditions suivantes sont satisfaites :
$(i)$ L'application $\mu_p(F) \longrightarrow \prod_{v|p} \mu_p(F_v)$ est un isomorphisme,
$(ii)$ $\mathscr{H}_p(F) = \left(F^\times\right)^p$.

Une caractérisation un peu particulière est lorsque le corps $F$ contient le groupe des racines $p^{\text{ème}}$ de l'unité. Dans ce cas, $F$ est $p$-rationnel si et seulement si les deux conditions suivantes sont satisfaites :
$(i)$ $F$ contient une seule place au-dessus de $p$,
$(ii)$ La partie $p$-primaire du $p$-groupe de classes $A'_F$ est triviale.

Comme mentionné avant, $G_S(F)$ est libre précisément lorsque $r(G_S(F)) = 0$. Alors en terme de cohomologie, les conditions ci-dessus, sont équivalentes à la nullité du groupe de cohomologie $H^2(G_S(F), \mathbf{Z}/p\mathbf{Z})$. Si $\mathscr{G}_S(F) := \mathrm{Gal}(\Omega_S/F)$ désigne le groupe de Galois de l'extension maximale $\Omega_S$ de $F$ non-ramifiée en dehors des places de $S$, alors nous avons l'isomorphisme suivant [63, Corollary 1] :

$$H^2(G_S(F), \mathbf{Z}/p\mathbf{Z}) \cong H^2(\mathscr{G}_S(F), \mathbf{Z}/p\mathbf{Z}).$$

Ainsi $F$ est $p$-rationnel si et seulement si $H^2(\mathscr{G}_S(F), \mathbf{Z}/p\mathbf{Z})$ est trivial.

Dans certains cas particuliers, la $p$-rationalité est équivalente à la $p$-régularité. Soit $R_2F$ la partie $p$-primaire du "noyau régulier" (voir [29, Sections I & II] et aussi [30, Introduction]). Si

$p$ est impair ou si $F$ n'a pas de plongement réel, alors $R_2F$ est identifié à la partie $p$-primaire du noyau modéré $K_2(o_F)$, alors que lorsque $p = 2$ et $F$ possède un plongement réel, la différence entre la partie 2-primaire de $K_2(o_F)$ et $R_2F$ réside dans le fait que les symboles de Hilbert aux places réelles sont considérés comme modérés. Un corps de nombres $F$ avec $R_2F$ trivial est appelé $p$-régulier par Gras et Jaulent [30]. La terminologie vient du fait que le corps cyclotomique $\mathbf{Q}(\mu_p)$ est $p$-régulier exactement lorsque $p$ est un nombre premier régulier, i.e. $p$ ne divise pas le nombre de classes de $\mathbf{Q}(\mu_p)$. Pour un nombre premier impair $p$, en utilisant le résultat de Tate sur $K_2$ et la cohomologie galoisienne, Soulé a montré [71, Lemme 10] que le caractère de Chern réalise un isomorphisme

$$K_2(o_F)/p \cong H^2(o'_F, \mathbf{Z}/p(2)) \cong H^2(\mathcal{G}_S(F), \mathbf{Z}/p(2)),$$

où $\mathbf{Z}/p(2)$ est le $\mathcal{G}_S(F)$-module $\mathbf{Z}/p$ tordu 2-fois. Ainsi, la $p$-régularité d'un corps de nombres $F$ peut être interprétée par la nullité du $2^{\text{ème}}$ groupe de cohomologie galoisienne $H^2(\mathcal{G}_S(F), \mathbf{Z}/p(2))$.

Par conséquent, les deux notions de $p$-régularité et de $p$-rationalité sont de nature différente puisqu'elles correspondent à des différents tordus à la Tate. Néanmoins, lorsque le sous-corps réel maximal $\mathbf{Q}(\mu_p)^+$ de $\mathbf{Q}(\mu_p)$ est contenu dans $F$, alors la $p$-rationalité de $F$ est équivalente à sa $p$-régularité. En particulier, $\mathbf{Q}(\mu_p)$ est $p$-rationnel précisément lorsque $p$ est régulier. Un autre cas particulier est lorsque $p = 3$, un corps $F$ est 3-rationnel si et seulement si 3 ne divise pas l'ordre du noyau modéré $K_2(o_F)$.

Dans le reste de cette section, nous allons montrer l'existence d'une famille infinie de $p$-extensions cycliques $L/F$ de corps $p$-rationnels contenant $\mu_p$ dans lesquelles l'unique idéal de $F$ au-dessus de $p$ est inerte dans $L$. Commençons tout d'abord, par définir la notion d'ensemble primitif des idéaux premiers qui joue un rôle important dans la monté de la $p$-rationalité :

**Définition 2.1.1.** *([59, Définition 1, page 42]) Un ensemble $S'$ de places de $F$ contenant $S$ est dit primitif pour $(F, p)$ si les Frobenius $\sigma_v(\tilde{F}_1/F)$ attachés aux places $v$ dans $S' \setminus S$ engendrent un $F_p$-sous-espace vectoriel de* $\mathrm{Gal}(\tilde{F}_1/F)$ *de dimension la cardinalité de $S' \setminus S$, où $\tilde{F}_1$ est le composé des premiers étages de $\mathbf{Z}_p$-extensions de $F$.*

**Remarques 2.1.2.** *(1) Si $S'$ est un ensemble primitif, alors le cardinal de $S' \setminus S$ est majoré par le nombre de $\mathbf{Z}_p$-extensions linéairement indépendantes de $F$, i.e. $|S' \setminus S| \leq 1 + r_2 + \delta_F$. En particulier, en cas d'égalité, $S'$ est dit maximal.*
*(2) Le théorème de densité de Čebotarev garantit l'existence d'une infinité d'ensembles primitifs maximaux [50, Theorem 10, Chap. VIII].*

Le théorème suivant donne une condition nécessaire et suffisante pour la montée de la $p$-rationalité dans une $p$-extension.

**Théorème 2.1.3.** *([59, Théorème 2, page 50]) Soit $F/k$ une $p$-extension de corps de nombres. Alors $F$ est $p$-rationnel précisément lorsque $k$ est $p$-rationnel et que l'ensemble $S_k$ de places de $k$ ramifiées dans $F$ ou divisant $p$, est primitif pour $(k,p)$. De plus, si $F$ est $p$-rationnel, alors l'extension $S_F$ de $S_k$ à $F$ reste primitive pour $(F,p)$.*

Soient $F$ un corps $p$-rationnel contenant $\mu_p$ et $\mathfrak{p}$ l'unique idéal de $F$ au-dessus de $p$. D'une part, le sous-corps $\mathbf{Q}(\mu_p)$ est aussi $p$-rationnel et le nombre premier $p$ devrait être un nombre premier régulier. Et d'autre part, dans toute extension $p$-rationnelle de $F$, $\mathfrak{p}$ ne se décompose pas, et il existe au moins une $p$-extension cyclique de $F$ dans laquelle $\mathfrak{p}$ est ramifié. Cela est dû au fait que tous les étages de la $\mathbf{Z}_p$-extension cyclotomique de $F$ sont $p$-rationnels (toute $p$-extension $p$-ramifiée d'un corps $p$-rationnel est aussi $p$-rationnelle) et $p$ se ramifie au moins dans un étage (puisque le corps de classes de Hilbert est une extension finie). En fait, pour un nombre premier régulier $p$, il existe une infinité de $p$-extensions $L/k$ cycliques de corps de nombres $p$-rationnels contenant $\mu_p$ dont lesquelles l'idéal de $k$ au-dessus de $p$ est ramifié dans $L$. Pour cela, il suffit de prendre à chaque fois $k$ égal à un étage de la $\mathbf{Z}_p$-extension cyclotomique de $\mathbf{Q}(\mu_p)$ et appliquer le même raisonnement pour le corps $F$ ci-dessus. Pour le cas où $\mathfrak{p}$ est inerte, nous avons le théorème suivant :

**Théorème 2.1.4.** *Pour chaque nombre premier impair régulier $p$, il existe une infinité de corps $p$-rationnels $F \supset \mu_p$ admettant une $p$-extension cyclique $p$-rationnelle (contenue dans $F_S$) dans laquelle l'idéal de $F$ au-dessus de $p$ est inerte.*

Avant de commencer la démonstration, nous allons rappeler la formule du genre de Chevalley [51, Lemma 4.1 Chap. 13] : soit $F/k$ une extension cyclique de groupe de Galois $G$, $U_k$ le groupe des unités de $k$ et $Cl_F$ le groupe de classes de $F$. Alors :

$$|Cl(F)^G| = \frac{h_k \prod_{\mathfrak{q}} e_{\mathfrak{q}}(F/k)}{[F:k][U_k : U_k \cap N_{F/k}(F^*)]},$$

où le produit est pris sur toutes les places $\mathfrak{q}$ de $k$ qui se ramifient dans $F$ et $e_{\mathfrak{q}}(F/k)$ l'indice de ramification de $\mathfrak{q}$.

*Démonstration.* (du Théorème 2.1.4) Posons $k := \mathbf{Q}(\mu_p)$ qui est $p$-rationnel puisque $p$ est régulier. On considère un ensemble primitif maximal $T := \{\mathfrak{p}, \mathfrak{L}_1, \mathfrak{L}_2, \cdots, \mathfrak{L}_r\}$ pour $(k,p)$, où $r := (p+1)/2$ est le nombre de $\mathbf{Z}_p$-extensions indépendantes de $k$ et $\mathfrak{p} = (\zeta_p - 1)$ est l'idéal $p$-adique premier de $k$ ($\zeta_p \neq 1$ est une racine $p^{\text{ème}}$ de l'unité). Comme mentionné dans la Remarque 2.1.2 ci-dessus, le théorème de densité de Čebotarev garantit l'existence d'une

infinité de tels ensembles primitifs. D'autre part, pour chaque $i = 1, 2, \cdots, r$, il existe un entier naturel non-nul $n_i$ et un entier $\alpha_i$ dans $k$ tel que $\mathfrak{L}_i^{n_i} = (\alpha_i)$. Puisque $p \nmid h_k$, alors chacun des $n_i$ est premier à $p$. Considérons maintenant le corps $F$ obtenu en ajoutant à $k$ une racine $p^{\text{ème}}$ de $a := (\zeta_p - 1)\alpha_1\alpha_2\cdots\alpha_r$, i.e. $F = \mathbf{Q}(\zeta_p, \sqrt[p]{a})$. Alors l'extension cyclique de Kummer $F/k$ est ramifiée exactement aux idéaux de l'ensemble primitif $T$ et non-ramifiée ailleurs ([18, Lemmas 5 and 6, Chap III, section 2]). En résumé, $k$ est $p$-rationnel et l'ensemble des places de $k$ ramifiées dans $F$ ou divisant $p$, est primitif pour $(k, p)$, ainsi, par le Théorème 2.1.3, la $p$-extension $F$ est $p$-rationnelle. Reste à montrer que chacun de ces corps $F$ admet une $p$-extension $p$-rationnelle dans laquelle l'idéal de $F$ au-dessus de $p$ est inerte.

D'après le théorème des unités de Dirichlet appliqué à $k$,

$$U_k \cong (\mathbf{Z}/p\mathbf{Z}) \oplus \mathbf{Z}^{r_2(k)-1},$$

et le fait que $U_k/(U_k \cap N_{F/k}(F^*))$ est un $p$-groupe (pour $x \in U_k$, $x^p = N_{F/k}(x) \in U_k \cap N_{F/k}(F^*)$), alors

$$|U_k/(U_k \cap N_{F/k}(F^*))| = p^t,$$

où $t \leq 1 + r_2(k) - 1 = \dfrac{p-1}{2}$. Ainsi, la formule du genre de Chevalley donne :

$$|Cl(F)^G| = \frac{h_k p^{1+(p+1)/2}}{p p^t} = h_k p^{(p+1)/2-t},$$

où $(p+1)/2 - t \geq 1$.

Par conséquent, $p$ divise le nombre de classes de $F$, et donc il existe une $p$-extension cyclique non-triviale de $F$ (à savoir le $p$-corps de classes de Hilbert de $F$) contenue dans $F_S$ dans laquelle l'idéal premier au-dessus de $p$ est inerte. Sa $p$-rationalité est dû au fait que toute $p$-extension $p$-ramifiée d'un corps $p$-rationnel est aussi $p$-rationnelle. □

**Remarques 2.1.5.** *(1) Un ensemble primitif peut produire un corps $F$ avec les mêmes propriétés dans la preuve ci-dessus si l'indice normique $[U_k : U_k \cap N_{F/k}(F^*)]$ est petit (voir l'exemple ci-dessous).*
*(2) On peut avoir le même résultat si à la place de la formule du genre de Chevalley, on utilise la minoration de Jehne [38, Theorem 4] du $p$-rang du groupe de classes de $F$ : pour un groupe abélien $G$, le $p$-rang de $G$ noté $rk_p(G)$, est la dimension du $p$-groupe abélien élémentaire $G/G^p$ considéré comme $\mathbb{F}_p$-espace vectoriel. Alors :*

$$rk_p(Cl_F) \geq \rho_{F/k} - rk_p(U_k/(U_k \cap N_{F/k}(F^*))) - 1,$$

*où $\rho_{F/k}$ est le nombre de places de k ramifiées dans F.*

**Exemples 2.1.6.** *(1) On peut prendre $p=3$, $k:=\mathbf{Q}(\zeta_3)$ et soient $\mathfrak{L}_7$ et $\mathfrak{L}_{19}$ chacun est l'un des idéaux premiers au-dessus de 7 et de 19 respectivement (les deux nombres premiers 7 et 19 se décomposent dans k). Alors l'ensemble $T=\{\mathfrak{p},\mathfrak{L}_7,\mathfrak{L}_{19}\}$ est un ensemble primitif maximal pour $(k,3)$ (voir [59] en bas de la page 49). Il n'est pas difficile de voir qu'on peut prendre $\mathfrak{L}_7=(\zeta_3-2)$ et $\mathfrak{L}_{19}=(\zeta_3-7)$, et donc*

$$a:=(\zeta_3-1)(\zeta_3-2)(\zeta_3-7)=33\zeta_3-3.$$

*Par conséquent, le corps correspondant $F=\mathbf{Q}\left(\zeta_3,\sqrt[3]{33\zeta_3-3}\right)$ est 3-rationnel et admet une extension cyclique non-ramifiée de degré 3 (dans $F_S$) dans laquelle l'idéal de F au-dessus de 3 est inerte. Ce corps F est obtenu en adjoignant à $\mathbf{Q}$ une racine de $X^6+39X^3+1197$ qui est le polynôme minimal de $\zeta_3\sqrt[3]{33\zeta_3-3}$.*
*(2) On pourrait aussi prendre pour F le "petit" corps $F:=\mathbf{Q}\left(\zeta_3,\sqrt[3]{\zeta_3-7}\right)$, dans lequel seuls les idéaux premiers $\mathfrak{p}=(\zeta_3-1)$ et $\mathfrak{L}_{19}=(\zeta_3-7)$ sont ramifiés et ont les mêmes propriétés : F est à la fois 3-rationnel et admet une extension cyclique non-ramifiée de degré 3 (dans $F_S$) dans laquelle l'idéal de F au-dessus de 3 est inerte. En effet, F est 3-rationnel selon le Théorème 2.1.3 puisque l'ensemble $\{\mathfrak{p},\mathfrak{L}_{19}\}$ est, a fortiori, primitif pour $(k,3)$. D'autre part, soit $\alpha=2+\sqrt[3]{\zeta_3-7}$, il est facile de voir que le polynôme minimal de $\alpha$ sur k est*

$$X^3-6X^2+12X-(\zeta_3+1),$$

*de sorte que $N_{F/k}(\alpha)=1+\zeta_3$. Et donc*

$$N_{F/k}\left(\alpha^2\right)=(1+\zeta_3)^2=\zeta_3,$$

*ainsi chaque unité de k est la norme d'un élément de $F^*$ et donc l'indice normique $[U_k:U_k\cap N_{F/k}(F^*)]$ dans la formule du genre ci-dessus est trivial. Par conséquent, $|Cl(F)^G|=3$ et le nombre de classes de F est divisible par 3. Remarquons également que ce corps F est obtenu en adjoignant à $\mathbf{Q}$ une racine de $X^6+15X^3+57$ qui est le polynôme minimal de $\zeta_3\sqrt[3]{\zeta_3-7}$ (il est irréductible sur $\mathbf{Q}$ puisqu'il vérifie le critère d'Eisenstein pour $p=3$).*

## 2.2 Caractérisations analytiques de la $p$-rationalité

Nous allons commencer par rappeler un résultat de Serre qui va nous aider pour donner des démonstrations alternatives de la $p$-rationalité d'un corps quadratique réel. Tout d'abord, on commence par la définition suivante :

**Définition 2.2.1.** *Soient $K$ un corps complet pour une valuation discrète $v$ et $m$ un entier naturel non nul. On note par $U_v^{(m)}$ le groupe multiplicatif des éléments $x$ de $K$ tels que $v(x-1) \geq m$. Autrement dit :*

$$U_v^{(m)} = 1 + \mathfrak{p}_v^m,$$

*où $\mathfrak{p}_v$ est l'idéal principal associé à $v$.*

**Proposition 2.2.2.** *([69, Proposition 9, page 219]) Soit $K$ un corps complet pour une valuation discrète $v$. On suppose que $K$ est de caractéristique zéro, et que son corps résiduel est de caractéristique $p \neq 0$. Soit $e = v(p)$ l'indice de ramification. Alors pour tout entier $m > \dfrac{e}{p-1}$, l'application :*

$$\begin{array}{ccc} U_v^{(m)} & \to & U_v^{(m+e)} \\ x & \mapsto & x^p \end{array}$$

*est un isomorphisme.*

Pour une extension finie $K$ de $\mathbf{Q}_p$ telle que l'indice de ramification $e < p-1$, les conditions de la proposition ci-dessus sont vérifiées dès que $m \geq 1$ et nous avons le corollaire suivant :

**Corollaire 2.2.3.** *Soit $K/\mathbf{Q}_p$ une extension finie, $e$ l'indice de ramification et $f$ le degré résiduel. Posons $q = p^f$ et soit $\varepsilon$ une unité de $F$. Si $e < p-1$, alors :*

$$\varepsilon^{q-1} \in U_v^{(1+e)} \Leftrightarrow \varepsilon \in (K^\times)^p.$$

*Démonstration.* D'après la proposition ci-dessus appliquée à $m = 1$, l'application

$$\begin{array}{ccc} U_v^{(1)} & \to & U_v^{(1+e)} \\ x & \mapsto & x^p \end{array}$$

est un isomorphisme. Alors dire que $\varepsilon \in (K^\times)^p$ revient à dire que $\varepsilon \in \mu_{q-1} \times U_v^{(1+e)}$ ce qui entraine $\varepsilon^{q-1} \in U_v^{(1+e)}$. L'implication réciproque est évidente puisque dans ce cas $\varepsilon^{q-1} \in (K^\times)^p$ et donc $\varepsilon \in (K^\times)^p$. □

**Remarque 2.2.4.** *Notons que pour que l'unité fondamentale d'un corps quadratique réel, ne soit pas une puissance $p^{ème}$ localement, il est suffisant et nécessaire qu'au moins l'une des unités ne le soit pas.*

Maintenant, nous allons utiliser le Lemme 1.3.1 pour donner une caractérisation de la $p$-rationalité lorsque $p$ est impair, d'un corps quadratique réel $F$. Si $p$ est ramifié dans $F$, il y a

une seule place $\mathfrak{p}$ de $F$ au-dessus de $p$ avec $N(\mathfrak{p}) = p$ et le produit

$$|\mu_{p^\infty} \cap F(\mu_p)| \prod_{\mathfrak{p}|p} (1 - (N(\mathfrak{p}))^{-1})$$

est donc une unité $p$-adique, dans ce cas la formule (1.5) devient :

$$|T_F| \sim_p h_F \frac{R_{p,F}}{\sqrt{p}}.$$

Sinon, $p$ est non-ramifié dans $F$ et le produit $\prod_{\mathfrak{p}|p} (1 - (N(\mathfrak{p}))^{-1})$ est toujours de valuation $p$-adique égale à $-2$, et donc la formule (1.5) devient cette fois-ci :

$$|T_F| \sim_p h_F \frac{R_{p,F}}{p}.$$

En résumé, la formule (1.5) pour un corps quadratique réel $F$ devient

$$|T_F| \sim_p h_F \frac{R_{p,F}}{p^{1/e}}, \tag{2.1}$$

où $e := 2$ ou $1$ selon que $p$ se ramifie dans $F$ ou non.

Désignons par $\varepsilon$ l'unité fondamentale de $F$ de sorte que $R_{p,F} = \log_p(\varepsilon)$, où $\log_p$ est le logarithme $p$-adique. Alors la valuation $p$-adique de $R_{p,F}$ est la même que celle de $(\varepsilon^{q-1} - 1)$, où $q := N(\mathfrak{p}_v)$. En effet, localement $\varepsilon \in \mu_{q-1} \times U_v^{(1)}$, en particulier $(\varepsilon^{q-1} - 1) \in \mathfrak{p}_v$ et donc nous avons :

$$\begin{aligned} (q-1)\log_p(\varepsilon) &= \log_p(\varepsilon^{q-1}) \\ &= \log_p(1 + (\varepsilon^{q-1} - 1)) \end{aligned}$$

puisque $p \nmid (q-1)$, nous en déduisons que

$$v(R_{p,F}) = v(\varepsilon^{q-1} - 1).$$

Par conséquent, d'après la formule (2.1), le corps quadratique réel $F$ est $p$-rationnel précisément lorsque $p$ ne divise pas le nombre de classes de $F$ et $\varepsilon^{q-1} \in U_v^{(1)} \setminus U_v^{(1+e)}$. Or, lorsque $p > 3$ ou $p = 3$ et non-ramifié dans $F$, alors $e < p-1$ et d'après le Corollaire 2.2.3, $\varepsilon^{q-1} \in U_v^{(1+e)}$ précisément quand $\varepsilon^{q-1}$ ou $\varepsilon$ est une puissance $p^{\text{ème}}$ dans le complété $F_v$. Par conséquent, nous avons prouvé la proposition suivante

**Proposition 2.2.5.** *Soient $F$ un corps quadratique réel et $p$ un nombre premier impair. Si*

*$p = 3$, on suppose de plus qu'il est non-ramifié dans $F$. Alors $F$ est $p$-rationnel précisément lorsque $p$ ne divise pas le nombre de classes de $F$ et que l'unité fondamentale de $F$ n'est pas une puissance $p^{ème}$ dans $F_v$.*

Une autre preuve de cette proposition a été donnée dans [31, Proposition 4.1] et nous fournirons une preuve alternative dans la section suivante.

Par la formule (1.6), nous avons l'interprétation de la $p$-rationalité d'un corps totalement réel, en terme du résidu de la fonction zêta $p$-adique :

**Proposition 2.2.6.** *Soit $p$ un nombre premier impair et $F$ un corps de nombres totalement réel. Soit $\mu_{p^m} := \mu_{p^\infty} \cap F(\mu_p)$. Alors $F$ est $p$-rationnel précisément lorsque la valuation $p$-adique du résidu de la fonction zêta $p$-adique de $F$ en 1 est $-m$ :*

$$\lim_{s\to 1}(s-1)\zeta_{F,p}(s) \sim_p p^{-m}.$$

Gardons les notations de la Proposition 2.2.6 ci-dessus. Lorsque le corps de nombres totalement réel $F$ est abélien sur $\mathbf{Q}$ et correspond à un groupe de caractères de Dirichlet $X$, alors [74, Page 71]

$$\lim_{s\to 1}(s-1)\zeta_{F,p}(s) = \lim_{s\to 1}(s-1)L_p(s,\chi_0)\prod_{\chi_0\neq\chi\in X} L_p(1,\chi),$$

où $\chi_0$ est le caractère trivial et $L_p(\ \ ,\chi)$ est la fonction $L$ $p$-adique associée à $\chi$. Puisque le résidu de $L_p(s,\chi_0)$ en $s=1$ est $(1-\frac{1}{p})$, selon la proposition ci-dessus, $F$ est $p$-rationnel précisément lorsque

$$\prod_{\chi_0\neq\chi\in X} L_p(1,\chi) \sim_p p^{-m+1}. \tag{2.2}$$

Pour $p$ un nombre premier et $n$ un entier naturel non-nul, on note par $\mathbf{Q}_n$ le $n^{\text{ème}}$ étage de la $\mathbf{Z}_p$-extension cyclotomique de $\mathbf{Q}$, i.e. $\mathbf{Q}_n$ est l'extension cyclique $p$-ramifiée de $\mathbf{Q}$ de degré $p^n$. La condition $F(\mu_p)\cap\mu_{p^\infty} \subseteq \mu_{p^n}$ peut être traduite par la condition $Q_n \nsubseteq F$. En effet, le fait que $\mathbf{Q}_n \subseteq F$ entraine facilement $\mu_{p^{n+1}} \subset F(\mu_p)$, et réciproquement nous avons

$$\mathbf{Q}_n\mathbf{Q}(\mu_p) = \mathbf{Q}(\mu_{p^{n+1}}) \subseteq F(\mu_p) = F\mathbf{Q}(\mu_p),$$

ainsi en utilisant la définition de la composée de deux extensions de corps, forcément $\mathbf{Q}_n \subseteq F$. En particulier pour $n=1$

$$F(\mu_p)\cap\mu_{p^\infty} = \mu_p \Leftrightarrow \mathbf{Q}_1 \nsubseteq F.$$

D'après cette équivalence et la formule (2.2), nous avons donc la proposition suivante :

**Proposition 2.2.7.** *Soit $F$ un corps totalement réel abélien sur $\mathbf{Q}$ ayant $X$ pour groupe de caractères et tel que $\mathbf{Q}_1 \nsubseteq F$. Alors $F$ est $p$-rationnel si et seulement si $L_p(1,\chi)$ est une unité $p$-adique pour chaque caractère non trivial $\chi \in X$.*

Ainsi, nous avons le cas particulier suivant, qui sera utilisé plus tard pour prouver l'existence d'une infinité de corps quadratiques réels $p$-rationnels.

**Corollaire 2.2.8.** *Soit $p$ un nombre premier impair. Un corps de nombres quadratique réel $F$ est $p$-rationnel précisément lorsque $L_p(1,\chi_F)$ est une unité $p$-adique.*

Soit $F$ un corps multi-quadratique totalement réel ayant $X$ pour groupe de caractères. Par la Proposition 2.2.7, $F$ est $p$-rationnel si et seulement si $L_p(1,\chi)$ est une unité $p$-adique pour chaque $\chi \in X \setminus \{\chi_0\}$. Or, puisque chacun de ces caractères correspond à un sous-corps quadratique de $F$, d'après le corollaire ci-dessus, $F$ est $p$-rationnel précisément lorsqu'il en est de même de tous ses sous-corps quadratiques. Pour un résultat plus général, nous avons :

**Proposition 2.2.9.** *([31, Proposition 3.6]) Si $F$ est une extension abélienne finie de $\mathbf{Q}$ et $[F:\mathbf{Q}]$ n'est pas divisible par $p$, Alors $F$ est $p$-rationnelle si et seulement si toute extension cyclique de $\mathbf{Q}$ contenue dans $F$ est $p$-rationnelle.*

Nous savons que le corps cyclotomique $\mathbf{Q}(\mu_p)$ est $p$-rationnel si et seulement si $p$ est régulier (voir la section précédente). À l'aide de la formule (2.2), nous pouvons aussi montrer la $p$-rationalité de $\mathbf{Q}(\mu_p)^+$ lorsque $p$ est régulier. Plus précisément :

**Proposition 2.2.10.** *Le sous-corps réel maximal $F = \mathbf{Q}(\mu_p)^+$ de $\mathbf{Q}(\mu_p)$ est $p$-rationnel précisément lorsque $p$ est régulier.*

*Démonstration.* D'après la formule (2.2), $F$ est $p$-rationnel précisément quand

$$\prod_{i=1}^{(p-3)/2} L_p(1,\omega^{2i})$$

est une unité $p$-adique avec $\omega$ le caractère de Teichmüller. D'autre part, nous avons :

$$L_p(1,\omega^{2i}) \equiv L_p(1-2i,\omega^{2i}) = -\frac{B_{2i}}{2i} \pmod{p}.$$

où $B_i$ est le $i^{\text{ème}}$ nombre de Bernoulli. Donc $F$ est $p$-rationnel si et seulement si $p$ ne divise pas le numérateur de $B_{2i}$ pour tout $i = 1,2,\ldots,(p-3)/2$, cela revient à dire que $p$ ne divise pas le nombre de classes de $\mathbf{Q}(\mu_p)$ ([74, Theorem 5.34]). □

La Proposition 2.2.7 nous a permis de caractériser la $p$-rationalité dans le cas d'un corps to-

talement réel abélien sur $\mathbf{Q}$ qui ne contient pas $\mathbf{Q}_1$ à l'aide de la fonction $L$ $p$-adique. D'après les relations qui existent entre cette dernière et les fonctions $L$ de Dirichlet, on peut aussi donner une caractérisation de la $p$-rationalité en terme des fonctions $L$ de Dirichlet. Nous aurons besoin tout d'abord, du résultat suivant :

**Lemme 2.2.11.** *Supposons que $p > 2$ et soit $F$ un corps totalement réel abélien sur $\mathbf{Q}$ ayant $X$ pour groupe de caractères. Si*

$$p^{n+1} \nmid f_\chi \quad \textit{pour tout caractère non-trivial } \chi \in X,$$

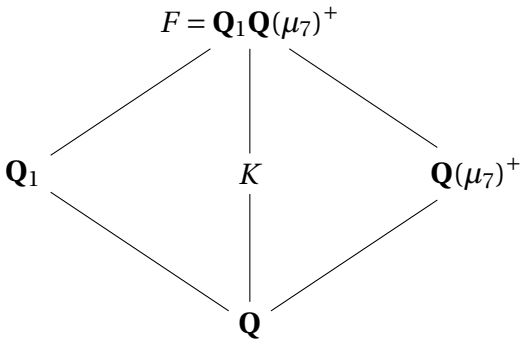
*alors $Q_n \nsubseteq F$.*

*Démonstration.* Supposons que $\mathbf{Q}_n \subseteq F$ et soit

$$Y := \left\{\chi \in X | \chi \text{ est trivial sur le groupe } \mathrm{Gal}(F/\mathbf{Q}_n)\right\}.$$

Alors $Y$ est isomorphe au groupe du caractère de $\mathbf{Q}_n/\mathbf{Q}$ qui est cyclique, d'où l'existence d'un caractère de $X$ qui engendre le groupe $Y$ et dont le conducteur est égal à $p^{n+1}$ (vu que $p^{n+1}$ est le plus petit entier $t$ tel que $\mathbf{Q}_n \subseteq \mathbf{Q}(\mu_t)$). □

Notons aussi que l'implication réciproque du lemme ci-dessus n'est pas vraie en général. En effet, prenons par exemple $p = 3$, $n = 1$ et considérons le diagramme suivant




où $K$ est un sous-corps cubique de $F$ différent de $\mathbf{Q}_1$ et de $\mathbf{Q}(\mu_7)^+$. Un tel corps $K$ est totalement ramifié à la fois en 3 et 7. Puisque 3 est sauvagement ramifié dans $K$, $3^3$ divise son discriminant. D'autre part, le groupe de caractères de $K$ est d'ordre 3, donc engendré par un caractère $\chi$ et par la formule de conducteur-discriminant [74, Theorem 3.11], nous avons :

$$d_K = f_\chi \cdot f_{\chi^2}.$$

Par conséquent, $3^2$ devrait diviser l'un des conducteurs.

En terme des fonctions $L$ de Dirichlet, nous avons donc la caractérisation suivante de la $p$-rationalité :

**Proposition 2.2.12.** *Soient $p$ un nombre premier impair et $F$ un corps totalement réel abélien sur $\mathbf{Q}$ ayant $X$ pour groupe de caractères. Supposons que*

$$p^2 \nmid f_\chi \quad \textit{pour tout caractère non-trivial } \chi \in X.$$

*Alors $F$ est $p$-rationnel si et seulement si*

$$L(2-p,\chi) \quad \textit{est une unité } p\textit{-adique,}$$

*pour chaque caractère $\chi$ non-trivial de $X$.*

*Démonstration.* La condition $p^2 \nmid f_\chi$ pour tout caractère non-trivial $\chi \in X$, entraine d'une part, que $\mathbf{Q}_1 \nsubseteq F$ par le Lemme 2.2.11, et donc d'après la Proposition 2.2.7 $F$ est $p$-rationnel si et seulement si $\prod_{\chi_0 \neq \chi \in X} L_p(1,\chi)$ est une unité $p$-adique, et d'autre part, en appliquant le Lemme 1.1.4

$$L_p(1,\chi) \equiv L_p(2-p,\chi) \pmod{p}.$$

Ensuite, en appliquant la formule (1.1) pour $n = p-1$

$$L_p(2-p,\chi) = (1-\chi(p)p^{p-2})L(2-p,\chi)$$

donc puisque $p > 2$, modulo $p$ nous obtenons

$$L_p(2-p,\chi) \equiv L(2-p,\chi).$$

□

Avec une approche différente, on peut retrouver le même résultat de la Proposition ci-dessus en supposant seulement que $\mathbf{Q}_1 \nsubseteq F$. En effet, dans [5, Section 2], les auteurs ont montré que la $p$-rationalité d'un corps totalement réel $F$ est équivalente à que $w_{p-1}(F)\zeta_F(2-p)$ soit une unité $p$-adique. Alors si $\mathbf{Q}_1 \nsubseteq F$, cela entraine que $w_{p-1}(F)$ est de valuation $p$-adique égale à 1. D'autre part, par le Théorème 1.2.1, nous avons :

$$\zeta_F(2-p) = \zeta(2-p) \prod_{\chi_0 \neq \chi \in X} L(2-p,\chi),$$

avec $\zeta(2-p)$ est de valuation $p$-adique égale à $-1$ par le théorème de Von Staudt et Clausen. Ainsi, $F$ est $p$-rationnel précisément lorsque $\prod_{\chi_0 \neq \chi \in X} L(2-p,\chi)$ est une unité $p$-adique.

**Remarque 2.2.13.** *Notons que cette dernière approche se trouve aussi dans [5, Section 2] avec des hypothèses plus fortes.*

Nous allons finir cette section avec un lemme qui sera utilisé surtout pour montrer l'existence d'une infinité de corps quadratiques réels $p$-rationnels. Fixons un nombre premier $p > 3$ et soit $d \neq (-1)^{\frac{p-1}{2}} p$ un entier sans facteur carré tel que $(-1)^{\frac{p-1}{2}} d > 0$. Introduisons le corps quadratique réel $F := \mathbf{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} pd}\right)$ ainsi que le corps quadratique $K := \mathbf{Q}(\sqrt{d})$. Nous avons alors

**Lemme 2.2.14.**

$$L_p(1,\chi_F) \equiv L(1-\frac{p-1}{2},\chi_K) \pmod{p}.$$

*Démonstration.* Si $p \equiv 1 \pmod 4$, $\frac{p-1}{2}$ est pair et par hypothèse $0 < (-1)^{\frac{p-1}{2}} d = d$, ainsi $\chi_K$ est aussi pair. Maintenant si $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ est impair et encore une fois par hypothèse, $0 < (-1)^{\frac{p-1}{2}} d = -d$, ce qui vaut dire que $d < 0$ et donc $\chi_K$ est aussi impair. Par conséquent, $\chi_K$ et $\frac{p-1}{2}$ sont de même parité, ce qui entraine la non-nullité de $L(1-\frac{p-1}{2},\chi_K)$.

Puisque le conducteur de $\chi_F$ est le discriminant du corps quadratique $F$, les hypothèses du Lemme 1.1.4 sont vérifiées pour $\chi_F$ et nous avons :

$$L_p(1,\chi_F) \equiv L_p(1-\frac{p-1}{2},\chi_F) \pmod{p}.$$

D'autre part, par la définition de la fonction $L$ $p$-adique,

$$L_p(1-\frac{p-1}{2},\chi_F) = \left(1-\chi_F\omega^{-\frac{p-1}{2}}(p)p^{\frac{p-1}{2}-1}\right) L\left(1-\frac{p-1}{2},\chi_F\omega^{-\frac{p-1}{2}}\right).$$

Alors puisque $p > 3$, $\frac{p-1}{2} - 1 > 0$ et modulo $p$, nous avons

$$L_p(1-\frac{p-1}{2},\chi_F) \equiv L\left(1-\frac{p-1}{2},\chi_F\omega^{-\frac{p-1}{2}}\right).$$

Comme $\omega^{-\frac{p-1}{2}}$ est le caractère associé au corps quadratique $\mathbf{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$, le caractère primitif du produit des deux caractères $\chi_F$ et $\omega^{\frac{p-1}{2}}$ est égal à $\chi_K$. □

## 2.3 Caractérisations algébriques de la $p$-rationalité

Dans le coté complètement algébrique, nous avons la proposition suivante remarquée par Nguyen Quang Do.

**Proposition 2.3.1.** *([65, Annexe]) Un corps de nombres $F$ est $p$-rationnel précisément lorsque les trois conditions suivantes sont remplies :*
*(i) le $p$-corps de classes de Hilbert $H_p \subseteq \tilde{F}$ ;*
*(ii) l'application naturelle $\mu_p(F) \to \oplus_{v|p}\mu_p(F_v)$ est un isomorphisme ;*
*(iii) l'application naturelle $U_F/p \to \oplus_{v|p}U_v/p$ est injective.*

*Démonstration.* Par définition, le noyau de Leopoldt $D_F$ est le noyau de l'application diagonale $U_F \to \oplus_{v|p}U_v$ une fois tensorisé avec $\mathbf{Z}_p$ et nous avons une suite exacte à quatre termes fournie par la théorie du corps de classes globale

$$0 \to D_F \to \bar{U}_F \to \oplus_{v|p}\bar{U}_v \to \mathrm{Gal}(F_S^{ab}/H_p) \to 0.$$

Rappelons que la nullité de $D_F$ est l'une des équivalences de la conjecture de Leopoldt. Supposons d'abord que $F$ soit $p$-rationnel. Alors évidemment $H_p \subseteq F_S^{ab} = \tilde{F}$ et $D_F = 0$. Ainsi, nous avons le diagramme commutatif où les applications verticales consistent à élever à la puissance $p$ :

$$\begin{array}{ccccccccc} 0 & \to & \bar{U}_F & \to & \oplus_{v|p}\bar{U}_v & \to & \mathrm{Gal}(F_S^{ab}/H_p) & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle .p} & & \\ 0 & \to & \bar{U}_F & \to & \oplus_{v|p}\bar{U}_v & \to & \mathrm{Gal}(F_S^{ab}/H_p) & \to & 0. \end{array}$$

En appliquant le lemme du serpent

$$0 \to \mu_p(F) \to \oplus_{v|p}\mu_p(F_v) \to \ker(.p) \to U_F/p \to \oplus_{v|p}U_v/p \to \mathrm{coker}(.p) \to 0. \tag{2.3}$$

Or $\mathrm{Gal}(F_S^{ab}/H_p)$ est un sous-groupe de $\mathrm{Gal}(F_S^{ab}/F) \cong \mathbf{Z}_p^{r_2+1}$, donc $\ker(.p) = 0$ et on obtient les deux autres conditions (ii) et (iii). Supposons maintenant que les trois conditions soient remplies. Reconsidérons le même diagramme commutatif ci-dessus en gardant cette fois-ci $D_F$ :

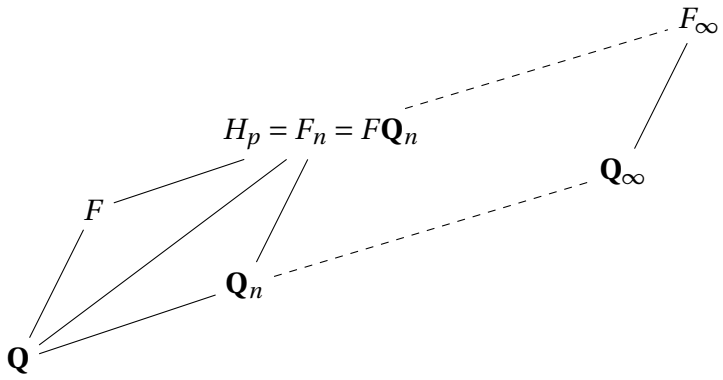
$$\begin{array}{ccccccccc} 0 & \to & D_F & \to \bar{U}_F & \to & \oplus_{v|p}\bar{U}_v & \to & \mathrm{Gal}(F_S^{ab}/H_p) & \to & 0 \\ & & \downarrow & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & D_F & \to \bar{U}_F & \to & \oplus_{v|p}\bar{U}_v & \to & \mathrm{Gal}(F_S^{ab}/H_p) & \to & 0. \end{array}$$

Une chasse dans le diagramme montre que sous la condition (ii), $D_F/p$ est contenu dans le

noyau de $U_F/p \to \oplus_{v|p} U_v/p$. Cette dernière application est, à son tour, injective par l'hypothèse (iii). Par conséquent, $D_F = 0$ et une fois de plus, nous sommes confrontés à la suite exacte (2.3) ci-dessus. Ainsi les deux conditions (ii) et (iii) entraine que $\ker(.p) = 0$ et donc $\mathrm{Gal}(F_S^{ab}/H_p)$ est sans torsion. Par conséquent, $T_F = 0$ par la condition (i) et $F$ est $p$-rationnel.

□

Considérons ici un corps de nombres totalement réel $F$ qui est galoisien sur $\mathbf{Q}$ et satisfaisant à la conjecture de Leopoldt en $p$. Si l'indice de ramification $e$ du nombre premier $p$ dans $F/\mathbf{Q}$ est premier à $p$, alors la condition $(i)$ dans la Proposition ci-dessus 2.3.1 est équivalente à $p \nmid h_F$. En effet, si $p \nmid h_F$, évidement le $p$-corps de classes de Hilbert $H_p$ (qui est trivial) est contenu dans $\tilde{F} = F_\infty$ la $\mathbf{Z}_p$-extension cyclotomique. Inversement, si on suppose que $H_p \subseteq \tilde{F}$ avec $p \mid h_F$, alors $H_p$ correspond à un étage $F_n$ de $F_\infty$ et nous obtiendrons d'après le diagramme suivant




que dans l'extension $H_p/\mathbf{Q}$, $e$ est premier à $p$ dans le tour d'extensions $H_p/F/\mathbf{Q}$, et de l'autre coté, $p^n$ divise $e$ dans le tour $H_p/\mathbf{Q}_n/\mathbf{Q}$ ce qui nous ramène à une contradiction.

Maintenant, si $p-1 \nmid e$, tous les $\mu_p(F_v)$ (pour $v$ divisant $p$) sont triviaux et par la suite, $\mu_p(F)$ est aussi trivial, et la condition $(ii)$ est assurée.

Par conséquent, la $p$-rationalité de $F$ peut être vue à travers le nombre de classes et les unités de la manière suivante :

**Proposition 2.3.2.** *Soit $F$ un corps de nombres totalement réel qui est galoisien sur $\mathbf{Q}$ et qui satisfait la conjecture de Leopoldt en $p$. Supposons que ni $p$ ni $p-1$ ne divisent l'indice de ramification du nombre premier $p$ dans $F/\mathbf{Q}$. Alors $F$ est $p$-rationnel précisément lorsque les deux conditions suivantes sont satisfaites :*
*(i) $p$ ne divise pas le nombre de classes de $F$ ;*
*(ii) l'application naturelle $U_F/p \to \oplus_{v|p} U_v/p$ est injective.*

Considérons maintenant une extension cyclique $F$ de degré premier impair $n$ sur $\mathbf{Q}$. Nous savons qu'une extension galoisienne est ou bien réelle ou bien imaginaire, or puisque le degré est supposé impair, nous avons bien une extension réelle. Si $n = p$, comme expliqué précédemment, $F$ est $p$-rationnel précisément quand (à part $p$ qui peut ou non être ramifié en $F$) au plus une non-$p$-place $\ell \not\equiv 1 \pmod{p^2}$ se ramifie dans $F$. Pour $n \neq p$, le corps cyclique $F$ satisfait les hypothèses de la Proposition 2.3.2 ci-dessus et nous avons

**Corollaire 2.3.3.** *Soit $F$ une extension cyclique de $\mathbf{Q}$ de degré premier impair $n \neq p$. Alors $F$ est $p$-rationnelle précisément lorsque les deux conditions suivantes sont remplies :*
*(i) $p$ ne divise pas le nombre de classes de $F$ ;*
*(ii) l'application naturelle $U_F/p \to \oplus_{v|p} U_v/p$ est injective.*

Lorsque le corps totalement réel $F$ est quadratique, une attention particulière doit être accordée à la condition ci-dessus, $p-1 \nmid e$ lorsque $p = 3$ et est ramifié dans $F$, que nous traiterons un peu plus loin. Dans le cas contraire, les hypothèses de la Proposition 2.3.2 ci-dessus sont satisfaites, ce qui conduit à une preuve alternative de la Proposition 2.2.5.

Si, au contraire, le corps de nombres quadratique $F$ est imaginaire, alors le $p$-corps de classes de Hilbert $H$ est galoisien sur $\mathbf{Q}$, la première condition $H \subseteq \tilde{F}$ dans la Proposition 2.3.1 équivaut à ce que $H$ soit contenu dans la $\mathbf{Z}_p$-extension anticyclotomique de $F$, puisque les étages de la $\mathbf{Z}_p$-extension cyclotomique de $F$ sont nécessairement ramifiées aux places au-dessus de $p$. Par conséquent, nous obtenons également une preuve alternative du corollaire suivant [31, Proposition 4.1].

**Corollaire 2.3.4.** *Soit $F$ un corps de nombres quadratique imaginaire. Supposons que $p \geq 5$ ou $p = 3$ et qu'il soit non-ramifié dans $F/\mathbf{Q}$. Alors $F$ est $p$-rationnel précisément lorsque le $p$-corps de classes de Hilbert de $F$ est contenu dans la $\mathbf{Z}_p$-extension anticyclotomique de $F$. En particulier :*
*(i) Si $p$ ne divise pas le nombre de classes $h_F$, alors $F$ est $p$-rationnel.*
*(ii) Si $F$ est $p$-rationnel, alors $A_F$, la partie $p$-primaire du groupe de classes de $F$, est au plus cyclique.*

Il existe de nombreux exemples où le corps de nombres quadratique imaginaire $F$ est $p$-rationnel avec un $p$-groupe de classes non trivial. Par exemple, $\mathbf{Q}(\sqrt{-23})$, dont le groupe de classes est d'ordre 3, s'avère être 3-rationnel. Un autre exemple est fourni par $\mathbf{Q}(\sqrt{-47})$ qui est 5-rationnel et dont le groupe de classes est d'ordre 5.

Traitons maintenant le cas restant, à savoir lorsque $p = 3$ et est ramifié dans le corps quadratique $F = \mathbf{Q}(\sqrt{d})$ où l'entier $d$ est sans facteur carré et un multiple de 3. Localement, nous

avons $\mathbf{Q}_3(\sqrt{d}) = \mathbf{Q}_3(\sqrt{-3})$, précisément lorsque $-d/3$ est une unité principale dans le corps local $\mathbf{Q}_3$ qui est équivalent à $d \equiv -3 \pmod 9$. Donc, dans ce cas, toujours grâce à la condition (ii) de la Proposition 2.3.1, le corps $F$ est 3-rationnel si et seulement si $F = \mathbf{Q}(\sqrt{-3})$. Si au contraire, $d \not\equiv -3 \pmod 9$, la condition (ii) de la Proposition 2.3.1 est automatiquement valable et nous obtenons le même résultat que précédemment :

**Corollaire 2.3.5.** *Soit $F = \mathbf{Q}(\sqrt{d})$ un corps quadratique avec $d \neq -3$ sans facteur carré et divisible par 3.*
*(i) Si $d \equiv -3 \pmod 9$, alors $F$ n'est pas 3-rationnel.*
*(ii) Si $d \not\equiv -3 \pmod 9$ et $d > 0$, alors $F$ est 3-rationnel précisément quand $3 \nmid h_F$ et l'unité fondamentale de $F$ n'est pas une puissance troisième localement.*
*(iii) Si $d \not\equiv -3 \pmod 9$ et $d < 0$, alors $F$ est 3-rationnel précisément lorsque le 3-corps de classes de Hilbert de $F$ est contenu dans la $\mathbf{Z}_3$-extension anticyclotomique de $F$. En particulier, si 3 ne divise pas le nombre de classes de $F$, alors $F$ est 3-rationnel. De plus, comme précédemment, si $F$ est 3-rationnel alors $A_F$, la partie 3-primaire du groupe de classes de $F$, est au plus cyclique.*

Soit $F = \mathbf{Q}(\sqrt{d})$ un corps quadratique avec $d \neq -3$ sans facteur carré et $F' = \mathbf{Q}(\sqrt{-3d})$. Supposons que $d \not\equiv -3 \pmod 9$ qui est équivaut au fait que 3 ne se décompose pas dans $F'$. Supposons d'abord que $d > 0$, nous avons

$$L_3(1, \chi_F) \equiv L_3(1-1, \chi_F) = (1 - \chi_{F'}(3)) L(1-1, \chi_{F'}) = (1 - \chi_{F'}(3)) \frac{2}{w} h_{F'} \pmod 3,$$

où $w = 2$ sauf quand $d = 3$, auquel cas $w = 4$. Puisque 3 ne se décompose pas dans $F'$, le facteur $(1 - \chi_{F'}(3))$ est non-nul et, par le Corollaire 2.2.8, $F$ est 3-rationnel précisément quand $3 \nmid h_{F'}$ (cette dernière équivalence peut également être vue en utilisant [14, Theorem 2] puisque, comme mentionné précédemment, $F$ est 3-rationnel précisément quand 3 ne divise pas l'ordre du noyau modéré $K_2(o_F)$). Maintenant, si $d < 0$, la 3-rationalité de $F$ est équivalente à la trivialité de $A'_{F'}$, la partie 3-primaire du groupe de classes de $F'$ [25, Théorème 4.1]. Enfin, la non-décomposition de 3 dans $F'$ implique également que $A'_{F'} = A_{F'}$ et nous obtenons la relation intéressante suivante entre la 3-rationalité de $F$ et le nombre de classes de son corps quadratique miroir (voir également [31, Corollaire 4.2] et le paragraphe qui suit).

**Proposition 2.3.6.** *Soit $F = \mathbf{Q}(\sqrt{d})$ un corps quadratique, avec $d \neq -3$ sans facteur carré et $F' = \mathbf{Q}(\sqrt{-3d})$.*
*(i) Si $d \equiv -3 \pmod 9$, alors $F$ n'est pas 3-rationnel.*
*(ii) Si $d \not\equiv -3 \pmod 9$, alors $F$ est 3-rationnel précisément quand $A_{F'} = 0$.*

D'après [76, Theorem A], il existe une infinité de corps quadratiques imaginaires $\mathbf{Q}(\sqrt{-d})$ dans lesquels 3 est inerte et dont les nombres de classes sont premiers à 3. En particulier, ces corps $\mathbf{Q}(\sqrt{-d})$ sont 3-rationnels. Puisque 3 est inerte, alors $3d \not\equiv -3 \pmod 9$ et donc les corps $\mathbf{Q}(\sqrt{3d})$ (et ensuite aussi $\mathbf{Q}(\sqrt{-3},\sqrt{-d})$) sont 3-rationnels par la Proposition 2.3.6. Nous avons donc ce qui suit

**Corollaire 2.3.7.** *Il existe une infinité de corps de nombres bi-quadratiques imaginaires* 3*-rationnels.*

Un corps multi-quadratique est $p$-rationnel précisément lorsque tous ses sous-corps quadratiques le sont (Proposition 2.2.9). D'où en combinant les Corollaire 2.3.4 (i), Corollaire 2.3.5 (iii) et la Proposition 2.3.6, on voit que le degré d'un corps multi-quadratique 3-rationnel qui contient $\sqrt{-3}$ ne peut pas être arbitrairement grand. À savoir :

**Corollaire 2.3.8.** *Soit $F$ un corps multi-quadratique réel* 3*-rationnel. Alors $F(\sqrt{-3})$ est* 3*-rationnel précisément lorsque $F$ ne contient aucun $\sqrt{d}$ avec $d \equiv 1 \pmod 3$. En particulier, un corps multi-quadratique* 3*-rationnel qui contient $\sqrt{-3}$ est au plus bi-quadratique.*

Enfin, pour compléter, traitons brièvement le cas de $p = 2$. En ce qui concerne la 2-rationalité d'un corps quadratique $F$, la situation est complètement différente de celle du cas d'un premier impair. Rappelons tout d'abord que si la racine $p^{\text{ème}}$ de l'unité $\mu_p \subset F$, alors $F$ est $p$-rationnel précisément lorsque $F$ ne contient qu'une seule $p$-place et que la partie $p$-primaire du $p$-groupe de classes $A'_F$ est triviale [61, Théorème et Définition 2.1]. Pour $p = 2$, le groupe de classes au sens restreint $A_F^{'+}$ doit remplacer $A'_F$.

Par conséquent, la $p$-rationalité pour $p = 2$ revient à avoir une place dyadique et à la nullité de la partie 2-primaire du 2-groupe de classes au sens restreint $A_F^{'+}$. Par la formule du genre pour les groupes de classes "à la Chevalley", il devrait être possible de dresser la liste des corps quadratiques 2-rationnels. Mais on en sait beaucoup plus. En fait, pour $p = 2$, les deux conditions ci-dessus sont également équivalentes à la nullité du groupe de cohomologie étale positif $H^2_+(o'_F,\mathbf{Z}_2(i))$ pour tout entier $i \geq 2$ (Voir [6, Proposition 4.8] dont la preuve suit les mêmes idées que celles de la preuve de [44, Proposition 2.6] où le cas des corps de nombres réels est traité). Cette nullité est caractérisée pour les 2-extensions galoisiennes finies de $\mathbf{Q}$ [6, Proposition 6.4] :

**Proposition 2.3.9.** *Soit $F$ une* 2*-extension galoisienne finie de $\mathbf{Q}$ et $i \geq 2$. Alors le groupe de cohomologie étale positif $H^2_+(o'_F,\mathbf{Z}_2(i))$ est nul (en d'autres termes, $F$ est* 2*-rationnelle) exactement quand $F/\mathbf{Q}$ est non-ramifié en dehors de l'ensemble des places $\{2,\infty,\ell\}$ avec $\ell \equiv \pm 3 \pmod 8$.*

Ainsi, les corps quadratiques 2-rationnels sont $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-2})$ et ceux de la forme $\mathbf{Q}(\sqrt{\ell})$, $\mathbf{Q}(\sqrt{2\ell})$, $\mathbf{Q}(\sqrt{-\ell})$ et $\mathbf{Q}(\sqrt{-2\ell})$ où $\ell$ est un nombre premier impair $\equiv \pm 3 \pmod 8$. Par conséquent, il est évident que les seuls corps multi-quadratiques réels 2-rationnels s'avèrent être au plus bi-quadratiques de la forme $\mathbf{Q}(\sqrt{2},\sqrt{\ell})$ avec $\ell \equiv \pm 3 \pmod 8$ et les corps multi-quadratiques imaginaires 2-rationnels sont au plus tri-quadratiques de la forme $\mathbf{Q}(\sqrt{-1},\sqrt{2},\sqrt{\ell})$ avec $\ell \equiv \pm 3 \pmod 8$. Notons que la même liste peut également être obtenue par [29, Corollaire du Théorème 2].

Nous allons finir les caractérisations de la $p$-rationalité des corps quadratiques avec une généralisation de la preuve de Greenberg qui relie la $p$-rationalité de $\mathbf{Q}(\sqrt{5})$ lorsque $p \neq 5$ est un nombre premier impair, aux nombres de Fibonacci sous une forme particulièrement agréable comme il explique dans [31, Corollaire 4.5]. Soit

$$q := \begin{cases} p & \text{if } p \equiv \pm 1 \pmod 5, \\ p^2 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

Alors $\mathbf{Q}(\sqrt{5})$ est $p$-rationnel précisément quand le $q$-ième nombre de Fibonacci $F_q \not\equiv 1 \pmod{p^2}$. Les nombres de Fibonacci sont donnés par la formule de Binet

$$F_q := \frac{\varepsilon_0^q - \bar{\varepsilon}_0^q}{\varepsilon_0 - \bar{\varepsilon}_0},$$

où $\varepsilon_0 := (1+\sqrt{5})/2$ est l'unité fondamentale de $\mathbf{Q}(\sqrt{5})$. La preuve de Greenberg peut être étendue de la même manière pour n'importe quel corps quadratique réel $F$ dans lequel $p$ est non-ramifié. En effet, soit $\varepsilon$ l'unité fondamentale de $F$. Introduisons $q := p^f$, où $f$ est le degré résiduel de $p$ dans $F$. Alors $\varepsilon^{q-1}$ est une unité principale dans le complété $F_v$ en une $p$-place $v$ et est localement une puissance $p^{\text{ème}}$ précisément quand elle appartient à $U_v^{(2)}$ (Corollaire 2.2.3). Par conséquent, $\varepsilon$ est localement une puissance $p^{\text{ème}}$ précisément quand $\varepsilon^q \equiv \varepsilon \pmod{\mathfrak{p}_v^2}$. Il en va de même pour le conjugué $\bar{\varepsilon}$ qui coïncide avec $\varepsilon^{-1}$ ou $-\varepsilon^{-1}$. On note par

$$\mathscr{F}_n := \frac{\varepsilon^n - \bar{\varepsilon}^n}{\varepsilon - \bar{\varepsilon}}$$

les nombres de Fibonacci généralisés définis par la récurrence linéaire à deux termes :

$$\mathscr{F}_{n+2} := (\varepsilon + \bar{\varepsilon})\mathscr{F}_{n+1} - (\varepsilon\bar{\varepsilon})\mathscr{F}_n,$$

avec les termes initiaux $\mathscr{F}_0 = 0$ et $\mathscr{F}_1 = 1$. Par conséquent, il est maintenant clair que nous avons le corollaire suivant qui est une conséquence de la Proposition 2.2.5 et de la discussion ci-dessus inspirée par la preuve de Greenberg de [31, Corollaire 4.5] dans le cas particulier

de $\mathbf{Q}(\sqrt{5})$.

**Corollaire 2.3.10.** *Soit $F = \mathbf{Q}(\sqrt{d})$ un corps quadratique réel ayant pour unité fondamentale $\epsilon = u + t\sqrt{d}$. Soit $p \nmid ut$ un nombre premier impair non-ramifié dans $F$. Notons $q := p^f$ où $f$ est le degré résiduel de $p$ dans $F$. Alors $F$ est $p$-rationnel précisément lorsque les deux conditions suivantes sont remplies :*
*(i) $p$ ne divise pas le nombre de classes de $F$ ;*
*(ii) Le nombre de Fibonacci généralisé $\mathscr{F}_q \not\equiv 1 \pmod{p^2}$.*

Cela fournit un algorithme pour tester la $p$-rationalité d'un corps quadratique réel (et donc aussi d'un corps multi-quadratique réel). En utilisant une caractérisation similaire de la $p$-rationalité des corps quadratiques réels, des exemples de corps multi-quadratiques $p$-rationnels de degrés inférieurs ou égaux à $2^6$ sont obtenus dans [13, Section 3] pour tout nombre premier $p < 1000$.

Maintenant, nous allons énoncer la conjecture suivante de Greenberg pour les nombres premiers impairs $p$, qui a motivé ce travail :

**Conjecture 2.3.11.** *([31, Conjecture 4.8]) Pour chaque nombre premier impair $p$, et chaque entier positif $t$, il existe un corps de nombres $p$-rationnel $F$ qui est galoisien sur $\mathbf{Q}$ avec* $\mathrm{Gal}(F/\mathbf{Q}) \cong (\mathbf{Z}/2)^t$.

Comme l'explique Greenberg [31, Remark 6.8], si la conjecture ci-dessus 2.3.11 est vraie pour les corps multi-quadratiques imaginaires pour un nombre premier impair donné $p$, alors il existerait des représentations galoisiennes continues $\rho : G_{\mathbf{Q}} \to GL_n(\mathbf{Z}_p)$ avec une image ouverte pour tous les degrés $n \geq 4$. Nous y reviendrons dans la dernière section de ce chapitre.

En fait, nous savons quand exactement la $p$-rationalité est héritée par une $p$-extension arbitraire (Théorème 2.1.3) et c'était la stratégie pour obtenir une infinité de corps de nombres non abéliens satisfaisant la conjecture de Leopoldt en $p$. Pour la conjecture ci-dessus 2.3.11, il serait intéressant d'étudier les propriétés de montée de la $p$-rationalité le long des extensions quadratiques (et plus généralement de degrés premiers à $p$).

Remarquons que par la Proposition 2.2.5 et le Corollaire 2.3.5, si la conjecture de Greenberg ci-dessus est vérifiée, alors ces corps quadratiques réels $p$-rationnels fournissent une infinité de corps quadratiques réels dont les nombres de classes sont premiers à $p$. Nous pouvons généraliser cette remarque pour les corps multi-quadratiques réels. D'abord nous avons déjà montré que pour un corps totalement réel $p$-rationnel $F$ qui est galoisien sur $\mathbf{Q}$, le groupe de classes de $F$ est trivial si l'indice de ramification de $p$ dans $F/\mathbf{Q}$ est premier à $p$. En particulier c'est le cas lorsque $F$ est réel $p$-rationnel. Par conséquent, si la conjecture de Greenberg est

vraie pour un nombre premier $p$ impair, alors pour tout entier naturel $t$, il existe une infinité de corps totalement réels ayant comme groupe de Galois $(\mathbf{Z}/2\mathbf{Z})^t$ sur $\mathbf{Q}$ et dont les nombres de classes sont premiers à $p$.

On sait que la conjecture de Leopoldt descend toujours, et sous cette conjecture, pour toute extension $F/k$ de corps de nombres, les homomorphismes de transfert $T_k \longrightarrow T_F$ sont injectifs (voir [27, Theorem IV.2.1]). Alors si $F$ est $p$-rationnel, tous ses sous-corps sont $p$-rationnels. Donc la $p$-rationalité descend. Pour la montée, comme mentionné avant nous savons sous quelles conditions la $p$-rationalité monte dans une $p$-extension. Cependant pour une extension quelconque, il n'existe pas à ce jour une réponse. La proposition suivante donne une condition sous laquelle la $p$-rationalité monte dans le cas d'un corps C.M. Rappelons qu'un corps C.M est une extension quadratique imaginaire d'un corps totalement réel.

**Proposition 2.3.12.** *Soient $p > 2$ et $L$ un corps C.M dont le sous-corps réel maximal $F$ est $p$-rationnel. Supposons que $p \nmid h_L$ et $\mu_p \not\subset L_w$ pour toute $p$-place $w$ de $L$. Alors $L$ est aussi $p$-rationnel.*

*Démonstration.* Puisque $p$ est impair, l'inclusion $U_F \subset U_L$ induit une application naturelle injective $U_F/p \hookrightarrow U_L/p$. Puisque $\mu_p \not\subset L$ par hypothèse, $U_F/p$ et $U_L/p$ ont le même $\mathbf{Z}/p$-rang $[F:\mathbf{Q}]-1$. Par conséquent, l'application naturelle injective ci-dessus est en fait un isomorphisme. En d'autres termes, le groupe de Galois $\mathrm{Gal}(L/F)$ agit trivialement sur $U_L/p$. Considérons maintenant le diagramme commutatif suivant

$$\begin{array}{ccc} U_F/p & \longrightarrow & \oplus_{v|p} U_v/p \\ \downarrow \cong & & \downarrow \\ U_L/p & \longrightarrow & \oplus_{v|p} \oplus_{w|v} U_w/p. \end{array}$$

Puisque $F$ est supposé $p$-rationnel, l'application horizontale supérieure est injective par la Proposition 2.3.1, donc l'application horizontale inférieure est également injective et la $p$-rationalité de $L$ s'en déduit par la même Proposition 2.3.1. □

En fait, la condition $p \nmid h_L$ peut être remplacée par la condition moins restrictive que le $p$-corps de classes de Hilbert de $L$ soit contenu dans $\tilde{L}$. Nous notons également que, pour $p > 3$, si le corps C.M $L$ dans la Proposition ci-dessus 2.3.12 est supposé être multi-quadratique, alors il est $p$-rationnel dès que $p \nmid h_L$, puisque localement, $\mathbf{Q}_p(\mu_p)$ qui est cyclique de degré $p-1 > 3$ sur $\mathbf{Q}_p$, ne peut pas être un sous-corps du complété $L_w$ pour toute place $w$ de $L$ au-dessus de $p$. Le même résultat est valable pour $p = 3$, à condition que $L$ ne contienne pas

$\sqrt{d}$, où $d<0$ et $\equiv -3 \pmod 9$. En effet, $L_w$ contient $\mu_3$ si et seulement si $L$ contient un sous-corps quadratique $\mathbf{Q}(\sqrt{d})$ dont le complété en une place au-dessous de $w$, coïncide avec $\mathbf{Q}_3(\sqrt{-3})$, ce qui équivaut à $d \equiv -3 \pmod 9$. Finalement, $d$ ne peut pas être positif puisque le sous-corps réel maximal de $L$ est 3-rationnel.

Dans le but de généraliser le résultat de Hartung [33] sur l'existence pour chaque nombre premier impair $p$, d'une infinité de corps quadratiques imaginaires dont les nombres de classes sont premiers $p$, Naito [62, Theorem 0] a démontré le théorème suivant :

**Théorème 2.3.13.** *Soient $F$ un corps de nombres totalement réel et $p$ un nombre premier impair tels que $p \nmid w_2(F)\zeta_F(-1)$. Alors il existe une infinité d'extensions quadratiques totalement imaginaires $L/F$ telles que :*
*(i) le nombre de classes relatif de $L$ n'est pas divisible par $p$ ;*
*(ii) chaque idéal premier de $F$ au-dessus de $p$ ne se décompose pas dans $L$.*

Si $L$ est un corps C.M dont le sous-corps réel maximal est $L^+$, alors

$$h_L = h_L^- h_{L^+},$$

où $h_L^-$ est le nombre de classes relatif de $L$. Par conséquent, si $L$ est supposé être multi-quadratique et que $L^+$ est $p$-rationnel avec $p$ impair, alors comme mentionné avant, $p \nmid h_{L^+}$ (ce résultat peut aussi être obtenu en utilisant la condition $(i)$ de la Proposition 2.3.1 et le fait que $p$ se ramifie dans tous les étages de la $\mathbf{Z}_p$-extension cyclotomique de $L^+$). Ainsi, la condition $p \nmid h_L$ est équivalente à $p \nmid h_L^-$.

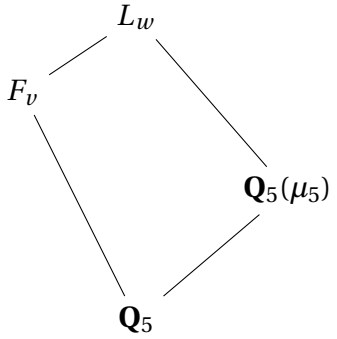
D'après le Théorème 2.3.13 ci-dessus et la Proposition 2.3.12, nous avons le corollaire suivant :

**Corollaire 2.3.14.** *Soit $p \geq 7$ et $F$ un corps multi-quadratique totalement réel $p$-rationnel. Supposons que $p \nmid w_2(F)\zeta_F(-1)$. Alors, il existe une infinité d'extensions quadratiques totalement imaginaires $L/F$ qui sont $p$-rationnelles.*

*Démonstration.* D'après la discussion précédente, $p \nmid h_F$. Alors par Théorème 2.3.13, il existe une infinité d'extensions quadratiques totalement imaginaires $L/F$ dont les nombres de classes sont premiers à $p$. Puisque $p$ est supposé être $\geq 7$, le complété de $L$ en toute $p$-place ne contient pas les racines $p^{\text{ème}}$ de l'unité et le Corollaire découle de la Proposition 2.3.12. □

Le Corollaire 2.3.14 ci-dessus reste valable également pour $p=5$ dès que $F$ ne contient aucun corps quadratique $\mathbf{Q}(\sqrt{d})$, où $d \equiv \pm 5 \pmod{25}$. En effet, d'après la preuve précédente,

il suffit de montrer que les extensions $L$ ne contiennent pas le groupe des racines $5^{\text{ème}}$ de l'unité. Soit $a = p^n u$ un élément de $\mathbf{Q}_p^\times$ avec $u \in \mathbf{Z}_p^\times$ et $n$ un entier naturel. Nous savons que lorsque $p > 2$, $a$ est un carré dans $\mathbf{Q}_p^\times$ si et seulement si $n$ est pair et $u \pmod{p\mathbf{Z}_p}$ est un carré dans $(\mathbf{Z}/p\mathbf{Z})^\times$ (voir par exemple [39, Proposition 2.18]). Supposons que l'une des extensions $L$ contienne $\mu_5$. Soit $v$ une $p$-place de $F$ et $w$ une place de $L$ au-dessus de $v$. Nous avons alors le diagramme suivant




Vu que $F_v$ ne contient pas $\mu_5$ dû au fait que $F$ est 5-rationnel, l'extension $L_w/F_v$ est de degré 2, et par conséquent l'extension $F_v \cap \mathbf{Q}_5(\mu_5)/\mathbf{Q}_5$ est quadratique, ainsi il existe un sous-corps quadratique $\mathbf{Q}(\sqrt{d})$ (avec $d$ sans facteur carré) de $F$ dont le complété en une place au-dessous de $v$ est égal à $\mathbf{Q}_5(\sqrt{5})$, ce qui équivaut à dire que $5d$ est un carré dans $\mathbf{Q}_5^\times$. Alors, $5 \mid d$ et $d/5$ est un carré dans $(\mathbf{Z}/5\mathbf{Z})^\times$, ce qui est équivaut à dire que $5 \mid d$ et $d/5 \equiv \pm 1 \pmod 5$. D'où $d \equiv \pm 5 \pmod{25}$.

Lorsque $F$ est totalement réel et abélien sur $\mathbf{Q}$, alors (voir la section 1.4)

$$w_2(F)\zeta_F(-1) = \pm|K_2(o_F)|.$$

Par conséquent, le Corollaire 2.3.14 s'applique en fait pour tout corps multi-quadratique totalement réel qui est à la fois $p$-rationnel et $p$-régulier.

## 2.4 Le cas $t = 1$ de la conjecture de Greenberg

Il existe une infinité d e corps quadratiques imaginaires dont les nombres de classes ne sont pas divisibles par un nombre premier donné $p$. C'est une conjecture de Chowla prouvée par Hartung [33]. Depuis lors, de nombreux articles ont traité la non-divisibilité par $p$ du nombre de classes des corps quadratiques imaginaires sous différentes conditions. Par exemple, le même résultat est prouvé dans [36] ou dans [35] imposant le comportement du premier $p$ ou un ensemble fini de premiers dans les corps quadratiques imaginaires en question. Dans

[43], les auteurs montrent même l'existence d'une limite inférieure pour le nombre de corps quadratiques imaginaires avec le discriminant $d > -X$ pour un grand entier $X$ ayant des nombres de classes premiers à $p$. Pour des traitements plus récents, voir [76, 10].

Ainsi, selon le Corollaire 2.3.4, pour chaque nombre premier $p$ il y a une infinité de corps quadratiques imaginaires $p$-rationnels. Nous notons également que Stark-Heegner ont montré qu'il y a exactement neuf corps quadratiques imaginaires principaux, plus précisément, $d < 0$ est le discriminant d'un corps quadratique imaginaire dont le nombre de classes égal à 1 si et seulement si :

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Alors, ils sont $p$-rationnels pour chaque nombre premier impair $p$ (en fait, ils sont également 2-rationnels sauf pour $\mathbf{Q}(\sqrt{-7})$) et il serait intéressant de lister les corps de nombres (quadratiques imaginaires) qui sont $p$-rationnels pour tous les nombres premiers impairs $p$.

Ainsi, le cas $t = 1$ est assuré par les corps quadratiques imaginaires. En ce qui concerne le cas réel, nous avons :

**Proposition 2.4.1.** *Pour tout nombre premier $p \neq 3$, le corps quadratique réel $F = \mathbf{Q}\left(\sqrt{p(p+2)}\right)$ est $p$-rationnel. Pour $p = 3$, le corps correspondant $F = \mathbf{Q}(\sqrt{15})$ n'est pas 3-rationnel.*

*Démonstration.* Pour $p = 2$, le corps en question est $\mathbf{Q}(\sqrt{2})$, le premier étage de la $\mathbf{Z}_2$-extension cyclotomique de $\mathbf{Q}$, qui est 2-rationnel. Pour $p = 3$, le corps quadratique $\mathbf{Q}(\sqrt{15})$ n'est pas 3-rationnel (Corollaire 2.3.5). En fait, cela est dû au fait qu'une fois complété en la place 3-adique, il coïncide avec $\mathbf{Q}_3(\sqrt{-3})$, d'où la condition (ii) de la Proposition 2.3.1 n'est pas remplie.

On peut donc supposer $p > 3$. Désignons par $d$ la partie sans facteur carré de $p(p+2)$. Puisque $d \equiv 3 \pmod 4$, l'unité fondamentale est de la forme $x + y\sqrt{d}$, où $x$ et $y$ sont des entiers strictement positifs. Nous affirmons que $\varepsilon := p + 1 + \sqrt{p(p+2)}$ est l'unité fondamentale. Puisque sinon il existerait $n \geq 2$ tel que :

$$2(p+1) = Tr(\varepsilon) = Tr((x + y\sqrt{d})^n) \geq 2x^n + 2x^{n-2}y^2 d,$$

où $Tr := Tr_{F/\mathbf{Q}}$ est l'application trace dans $F/\mathbf{Q}$. Puisque $p \mid d$, nous aurions nécessairement $x = y = 1$ et $d = p$. Mais c'est impossible puisque $x + y\sqrt{d} = 1 + \sqrt{p}$ n'est même pas une unité.

Or, l'unité fondamentale $\varepsilon = p + 1 + \sqrt{p(p+2)}$ est évidemment une unité principale du com-

plété $F_v$ de $F$ en une place $p$-adique $v$ et nous avons

$$\varepsilon \in U_v^{(1)} \setminus U_v^{(2)}.$$

Par conséquent, $\varepsilon \notin F_v^p$ puisque en élevant à la puissance $p$, on obtient un isomorphisme (Proposition 2.2.2) :

$$\begin{array}{ccc} \mu_{p-1}U_v^{(1)} & \longrightarrow & \mu_{p-1}U_v^{(3)} \\ \zeta x & \mapsto & \zeta x^p. \end{array}$$

Reste à montrer que $p$ ne divise pas le nombre de classes $h_F$. Puisque 2 se ramifie dans $F$, d'après le Corollaire 1.2.4

$$L(1,\chi_F) \leq \frac{\log d_F + \kappa_2}{4},$$

où $\kappa_2 < 2$. Pour notre corps quadratique $F$, le discriminant $d_F = 4d$ et $R_F = \log\left(p+1+\sqrt{p(p+2)}\right)$ est le régulateur. Par conséquent, par la formule du nombre de classes (1.3), nous avons successivement :

$$\begin{aligned} h_F &< \frac{\log(4p(p+2))+2}{4} \frac{\sqrt{4p(p+2)}}{2\log\left(p+1+\sqrt{p(p+2)}\right)} \\ &< \frac{\log(4p(p+2))+2}{4} \frac{\sqrt{p(p+2)}}{\log\left(2\sqrt{p(p+2)}\right)} \\ &< \frac{\log(4p(p+2))+2}{2\log(4p(p+2))} \sqrt{p(p+2)} \\ &< (\frac{1}{2}+\frac{1}{3})\sqrt{p(p+2)} \\ &< p. \end{aligned}$$

L'inégalité ci-dessus $h_F < p$ peut également être obtenue en utilisant [67, Corollaire 3]. Ainsi, $p$ ne divise pas $h_F$ et la preuve est complète. □

Le même raisonnement entraine pour $p$ impair, que $\varepsilon = p-1+\sqrt{p(p-2)}$ est l'unité fondamentale de $K = \mathbf{Q}\left(\sqrt{p(p-2)}\right)$, et par la suite $-\varepsilon \in U_v^{(1)} \setminus U_v^{(2)}$. Ainsi pour $p > 3$, $-\varepsilon$ (et donc $\varepsilon$) $\notin K_v^p$ (le cas $p = 3$ est évident). Finalement, le Théorème 1.2.3 entraine directement que $h_K < p$. Par conséquent, $K$ est $p$-rationnel. Notons aussi que ce corps quadratique a été traité dans [16].

De façon plus générale, nous allons montrer à l'aide du théorème suivant et de la Proposition ci-dessus, que pour chaque nombre premier $p > 3$, il existe une infinité de corps quadra-

tiques réels $p$-rationnels. Nous rappelons que pour $p = 3$, nous avons déjà montré l'existence d'une infinité de corps quadratiques réels 3-rationnels dans lesquels 3 se ramifie (Corollaire 2.3.7).

**Théorème 2.4.2.** *([66, Theorem 2]) Soit $p > 3$ un nombre premier, et supposons qu'il y ait un discriminant fondamental $D_0$ premier à $p$ pour lequel*

1. $(-1)^{\frac{p-1}{2}} D_0 > 0$,
2. $|B_{\frac{p-1}{2},\chi_{D_0}}|_p = 1$.

*Alors, il existe une progression arithmétique $r_p \pmod{t_p}$ avec $(r_p, t_r) = 1$ et une constante $\kappa(p)$ telle que pour chaque nombre premier $\ell \equiv r_p \pmod{t_p}$ il existe un entier $1 \leq d_\ell \leq \kappa(p)\ell$, pour lequel*

1. $D_\ell := d_\ell \ell p$ *est un discriminant fondamental,*
2. $h_{\mathbf{Q}(\sqrt{D_\ell})} \not\equiv 0 \pmod{p}$,
3. $|\dfrac{R_{p,D_\ell}}{\sqrt{D_\ell}}|_p = 1$.

Fixons un nombre premier $p > 3$. Remarquons que $p$ se ramifie dans chaque corps quadratique réel $F_{D_\ell} := \mathbf{Q}(\sqrt{D_\ell})$ défini dans le théorème ci-dessus et d'après la formule (2.1) :

$$|T_{F_{D_\ell}}| \sim_p h_{F_{D_\ell}} \frac{R_{p,F_{D_\ell}}}{p^{1/2}} \sim_p 1.$$

Ainsi pour chaque $D_\ell$, $F_{D_\ell}$ est $p$-rationnel.

Il suffit alors de montrer l'existence d'un tel discriminant fondamental $D_0$. Posons $F = \mathbf{Q}(\sqrt{p(p+2)})$. Par la Proposition 2.4.1 et le Corollaire 2.2.8, $L_p(1, \chi_F)$ est une unité $p$-adique. Soit $d$ la partie sans facteur carré de $(-1)^{\frac{p-1}{2}}(p+2)$. Évidement, la condition $(-1)^{\frac{p-1}{2}} d > 0$ est vérifiée et d'après le Lemme 2.2.14, $L(1 - \dfrac{p-1}{2}, \chi_K)$ (et donc aussi $B_{\frac{p-1}{2},\chi_K}$) est une unité $p$-adique où $K = \mathbf{Q}(\sqrt{d})$. Par conséquent, le discriminant fondamental de $K$ vérifie les conditions du théorème ci-dessus. Finalement nous avons prouvé le théorème suivant

**Théorème 2.4.3.** *Pour chaque nombre premier $p > 3$, il existe une infinité de corps quadratiques réels $p$-rationnels dans lesquels $p$ se ramifie.*

**Remarques 2.4.4.** *(1) Dans [5], en utilisant les formes modulaires de poids $1/2$, les auteurs ont montré pour $p = 5$, l'existence d'une infinité de corps quadratiques réels $5$-rationnels.*
*(2) Gras a conjecturé [28, Conjecture 8.11], qu'un corps de nombres $F$ est $p$-rationnel pour tout $p$ sauf pour un nombre fini, ou la version moins faible qui consiste à dire que pour $p$ assez grand, $F$ est $p$-rationnel. Dans ce sens, il a été prouvé que pour tout corps quadratique réel fixe*

*$F$ et tout entier assez grand $X$, la conjecture abc généralisée pour $F$ implique que le nombre de premiers $p \leq X$ pour lesquels $F$ est $p$-rationnel est au moins $c\log(X)$ pour une constante $c > 0$ dépendant de $F$ [54, Corollary].*

## 2.5 Observation pour la 5-rationalité

**Proposition 2.5.1.** *Soit $d \neq 5$ un entier positif sans facteur carré. Alors $\mathbf{Q}(\sqrt{5d})$ est 5-rationnel précisément lorsque $\mathbf{Q}(\sqrt{d})$ est 5-régulier.*

*Démonstration.* Soit $F = \mathbf{Q}(\sqrt{5d})$ et $K = \mathbf{Q}(\sqrt{d})$. Par définition, $K$ est 5-régulier précisément lorsque 5 ne divise pas l'ordre du noyau modéré $K_2(o_K)$. Puisque 2 et 3 sont les seuls diviseurs premiers de $w_2(K)$ et $\zeta_{\mathbf{Q}}(-1) = \dfrac{-1}{12}$, la dernière condition signifie, par l'égalité (1.7), que $\zeta_K(-1)$ ou de façon équivalente $L(-1,\chi_K)$ est une unité 5-adique. Or, d'après le Lemme 2.2.14, la dernière condition est, à son tour, équivalente à $L_5(1,\chi_F)$ étant une unité 5-adique. Enfin, le Corollaire 2.2.8 complète la preuve. □

**Exemple 2.5.2.** *Le corps quadratique $\mathbf{Q}(\sqrt{35})$ est à la fois 5-rationnel (Proposition 2.4.1) et 5-régulier (Proposition 2.5.1). Ainsi, par la discussion qui suit la preuve du Corollaire 2.3.14, il existe une infinité de corps imaginaires 5-rationnels de degré 4 sur $\mathbf{Q}$ contenant $\mathbf{Q}(\sqrt{35})$.*

Soit $F/k$ une extension bi-quadratique de corps de nombres totalement réels avec des sous-corps quadratiques $k_1$, $k_2$ et $k_3$, de sorte que $F/\mathbf{Q}$ est abélien. Nous avons la relation de Brauer suivante pour l'ordre des noyaux modérés [46, Proposition 1.1]

$$|K_2(o_k)|^2|K_2(o_F)| = |K_2(o_{k_1})||K_2(o_{k_2})||K_2(o_{k_3})|. \tag{2.4}$$

Comme conséquence, nous pouvons montrer la proposition suivante :

**Proposition 2.5.3.** *Soit $F$ un corps multi-quadratique réel de degré $n$. Alors*

$$2^{n-2}|K_2(o_F)| = \prod_k |K_2(o_k)|,$$

*où le produit est pris sur tous les sous-corps quadratiques $k$ de $F$.*

*Démonstration.* Posons $n = 2^m$. Nous allons montrer ce résultat par récurrence sur $m$. Considérons la suite $(U_l)$ définie par

$$U_l = 2^{2^l-2}, \quad l \geq 1.$$

Montrons que

$$U_m\,|K_2(o_F)| = \prod_k |K_2(o_k)|. \tag{2.5}$$

Pour $m = 1$, $F$ est quadratique et $U_1 = 1$, donc la formule est vraie. Pour $m = 2$, $U_2 = 4$ et puisque $F$ est bi-quadratique, nous avons dans la formule (2.4), $o_k = \mathbf{Z}$ et le noyau modéré $K_2(\mathbf{Z})$ de $\mathbf{Q}$ est d'ordre 2 [56, Corollaire 10.2]. Donc $2^2 = U_2$.
Soit $m > 1$ un entier et supposons que la formule est vraie pour tout entier inférieur ou égal à $m$. Soit $n = m+1$ et prenons un sous-corps $k$ de $F$ de degré $m-1$, on note par $k_1, k_2$ et $k_3$ les sous-corps intermédiaires entre $k$ et $F$, ils sont de degré $m$. Alors la formule (2.5) s'applique pour $k, k_1, k_2$ et $k_3$ et d'après la formule (2.4) nous avons

$$\left(\frac{\prod_{k^i} |K_2(o_{k^i})|}{U_{m-1}}\right)^2 |K_2(o_F)| = \left(\frac{\prod_{k_1^i} |K_2(o_{k_1^i})|}{U_m}\right)\left(\frac{\prod_{k_2^i} |K_2(o_{k_2^i})|}{U_m}\right)\left(\frac{\prod_{k_3^i} |K_2(o_{k_3^i})|}{U_m}\right),$$

où les $k^i$ (resp. $k_j^i$) sont les sous-corps quadratiques de $k$ (resp. $k_j$). Dans chaque sous-corps $k_j$, il y a les $2^{m-1}$ sous-corps quadratiques $k^i$ de $k$. Après simplification, nous obtenons

$$\frac{U_m^3}{U_{m-1}^2}|K_2(o_F)| = \prod_{F_i} |K_2(o_{F_i})|,$$

où le produit est pris sur tous les sous-corps quadratiques $F_i$ de $F$. Reste à montrer que $\dfrac{U_m^3}{U_{m-1}^2} = U_{m+1}$. En effet

$$\frac{U_m}{U_{m-1}} = \frac{2^{2^m-2}}{2^{2^{m-1}-2}} = 2^{2^{m-1}}.$$

Donc

$$\frac{U_m^3}{U_{m-1}^2} = \left(2^{2^{m-1}}\right)^2 2^{2^m-2} = 2^{2^m} 2^{2^m-2} = 2^{2^{m+1}-2} = U_{m+1}.$$

□

Comme conséquence de cette proposition, le corps multi-quadratique réel $F$ est $p$-régulier pour un nombre premier impair $p$ précisément quand c'est le cas de tous ses sous-corps quadratiques. Nous avons alors le corollaire suivant :

**Corollaire 2.5.4.** *Soit $F$ un corps multi-quadratique réel. Alors $F$ est à la fois* 5*-rationnel et* 5*-régulier si et seulement si $F(\sqrt{5})$ est* 5*-rationnel (et* 5*-régulier).*

*Démonstration.* L'équivalence est évidente si $F$ contient $\sqrt{5}$, puisque dans ce cas, $F$ contient le sous-corps réel maximal de $\mathbf{Q}(\mu_5)$ et donc la 5-rationalité de $F$ est équivalente à la 5-régularité de $F$. Supposons alors que $\sqrt{5} \notin F$. La 5-régularité de $F$ entraine que chacun de ses

sous-corps quadratiques $\mathbf{Q}(\sqrt{d})$ est 5-régulier. Par la Proposition 2.5.1, chaque corps quadratique $\mathbf{Q}(\sqrt{5d})$ est 5-rationnel, et de plus, on sait que $\mathbf{Q}(\sqrt{5})$ est aussi 5-rationnel, ainsi tous les sous-corps quadratiques de $F(\sqrt{5})$ sont 5-rationnels. D'où, $F(\sqrt{5})$ l'est aussi.
Inversement, $F(\sqrt{5})$ est 5-rationnel revient à dire que chacun de ses sous-corps quadratiques est 5-rationnel. D'après la Proposition 2.5.1 appliquée à chaque sous-corps quadratique sauf $K = \mathbf{Q}(\sqrt{5})$, et le fait que aussi $K$ est 5-régulier (pour le voir, un calcul facile montre que la 5-partie de $w_2(K)\zeta_K(-1)$ est triviale) entrainent que tous ses sous-corps quadratiques sont 5-réguliers, ainsi nous avons l'implication réciproque. □

## 2.6 Le cas $t = 2$ de la conjecture de Greenberg

Tout d'abord, on commence par le cas de corps bi-quadratique imaginaire.

**Proposition 2.6.1.** *Pour tout nombre premier $p$, les corps quadratiques imaginaires $F = \mathbf{Q}(\sqrt{-p})$ et $K = \mathbf{Q}(\sqrt{-(p+2)})$ sont $p$-rationnels.*

*Démonstration.* Pour $p = 2$, $F = \mathbf{Q}(\sqrt{-2})$ et $K = \mathbf{Q}(\sqrt{-1})$ sont 2-rationnels (voir le paragraphe au-dessous de la Proposition 2.3.9).
Pour $p = 3$, $F = \mathbf{Q}(\sqrt{-3})$ est 3-rationnel et pour $p > 3$, nous avons déjà montré dans la Section 1.2, que le nombre de classes de $F$ est toujours strictement inférieur à $p$, d'où par le Corollaire 2.3.4, $F$ est $p$-rationnel.
Soit $p \geq 3$. Si $p+2$ ou $(p+2)/3$ est un carré, $K = \mathbf{Q}(\sqrt{-1})$ ou $\mathbf{Q}(\sqrt{-3})$ et le groupe de classes de chacun de ces corps est trivial. Sinon, par le Théorème 1.2.2 et le même raisonnement appliqué à $F$ (voir Section 1.2), on montre que le nombre de classes de $K$ est strictement inférieur à $p$. Ainsi dans tous les cas, $K$ est $p$-rationnel par le Corollaire 2.3.4. □

D'après la $p$-rationalité de $\mathbf{Q}(\sqrt{p(p+2)})$ pour $p \neq 3$ (Proposition 2.4.1) et la Proposition ci-dessus, nous avons le résultat suivant :

**Proposition 2.6.2.** *Pour tout nombre premier $p \neq 3$, le corps bi-quadratique imaginaire $\mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{-p}\right)$ est $p$-rationnel.*

Comme indiqué dans la section 2.4, pour $p > 2$, $\mathbf{Q}\left(\sqrt{p(p-2)}\right)$ est $p$-rationnel et puisque $p$ ne divise pas le nombre de classes de $\mathbf{Q}\left(\sqrt{-p+2}\right)$ (par la même méthode de la Proposition 2.6.1 et le Théorème 1.2.2) alors $\mathbf{Q}\left(\sqrt{p(p-2)}, \sqrt{-p}\right)$ est aussi $p$-rationnel. Notons aussi que dans [8, Theorem 2.4], les auteurs ont montré que pour tout nombre premier $p$, le corps bi-quadratique imaginaire $\mathbf{Q}\left(\sqrt{-(p-1)}, \sqrt{-(p+1)}\right)$ est $p$-rationnel.

Pour le cas bi-quadratique réel, nous avons la proposition suivante :

**Proposition 2.6.3.** *Pour chaque nombre premier $p > 3$, le corps bi-quadratique réel $\mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{p(p-2)}\right)$ est $p$-rationnel.*

*Démonstration.* La différence $p^2 - 4$ ne peut jamais être un carré, donc nous avons bien un corps bi-quadratique. D'après la Proposition 2.4.1 et le paragraphe qui suit, la $p$-rationalité de $\mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{p(p-2)}\right)$ est équivalente à celle du sous-corps quadratique $k := \mathbf{Q}\left(\sqrt{p^2-4}\right)$. Montrons alors la $p$-rationalité de $k$. Posons :

$$q := \begin{cases} p & \text{si } p \equiv 1 \pmod 4, \\ p^2 & \text{si } p \equiv 3 \pmod 4, \end{cases}$$

et $\varepsilon := \dfrac{1}{2}\left(p + \sqrt{p^2-4}\right)$. Alors, il est clair que $\varepsilon$ est une unité de $k$ et nous avons :

$$\begin{aligned} (2\varepsilon)^{q-1} &= \left(p + \sqrt{p^2-4}\right)^{q-1} \\ &\equiv (p^2-4)^{\frac{q-1}{2}} + p(q-1)(p^2-4)^{\frac{q-3}{2}}\sqrt{p^2-4} \pmod{p^2 o_k} \\ &\equiv (-4)^{\frac{q-1}{2}} - (-4)^{\frac{q-3}{2}} p\sqrt{p^2-4} \pmod{p^2 o_k} \\ &\equiv 2^{q-1} + 2^{q-3} p\sqrt{p^2-4} \pmod{p^2 o_k}. \end{aligned}$$

Ainsi

$$\varepsilon^{q-1} \equiv 1 + \frac{1}{4} p\sqrt{p^2-4} \pmod{p^2 o_k},$$

et par conséquent, $\varepsilon^{q-1} \notin U_v^{(2)}$. Cela garantit le fait que notre unité $\varepsilon$ (et donc également l'unité fondamentale) n'est pas une puissance $p^{\text{ème}}$ localement. Examinons maintenant la non-divisibilité du nombre de classes $h_k$ par $p$. Il est possible de prouver que $h_k < p$ en utilisant à nouveau [52, Corollaire 2] mais ici nous avons une meilleure majoration. À savoir, par Théorème 1.2.3 ou [67, Corollary 2], on a les inégalités suivantes

$$h_k \leq \frac{1}{2}\sqrt{d_k} \leq \frac{1}{2} p.$$

Ainsi, $p$ ne divise pas $h_F$ et le corps $k$ est $p$-rationnel par La Proposition 2.2.5. La preuve est complète. □

Pour $p = 3$, le corps bi-quadratique correspondant ci-dessus $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ n'est pas 3-rationnel puisque comme indiqué précédemment $\mathbf{Q}(\sqrt{15})$ n'est pas 3-rationnel. Le corps $\mathbf{Q}(\sqrt{2}, \sqrt{5})$ est à la fois 2 et 3-rationnel (Propositions 2.3.9 et 2.2.5).

Notons que les mêmes arguments de la Proposition ci-dessus et de celles de la Proposition 2.4.1 entrainent que pour $p \neq 3$, le corps bi-quadratique réel $\mathbf{Q}\left(\sqrt{p(p+1)}, \sqrt{p(p-1)}\right)$ est $p$-rationnel. Pour $p = 3$, ce corps est $\mathbf{Q}(\sqrt{3}, \sqrt{6})$ qui n'est pas 3-rationnel puisque $\mathbf{Q}(\sqrt{6})$ ne l'est pas ($6 \equiv -3 \pmod 9$).

**Exemple 2.6.4.** *Par la Proposition ci-dessus 2.6.3, le corps bi-quadratique* $\mathbf{Q}(\sqrt{15}, \sqrt{35})$ *est* 5*-rationnel. D'autre part, les trois sous-corps quadratiques* $\mathbf{Q}(\sqrt{15})$, $\mathbf{Q}(\sqrt{21})$ *et* $\mathbf{Q}(\sqrt{35})$ *sont* 5*-réguliers par la Proposition 2.5.1, donc* $\mathbf{Q}(\sqrt{15}, \sqrt{35})$ *est aussi* 5*-régulier (voir paragraphe qui suit la Proposition 2.5.3). Par conséquent, d'après la discussion à la fin de la section 3.3, il existe une infinité de corps C.M* 5*-rationnels ayant le même sous-corps réel maximal* $\mathbf{Q}(\sqrt{15}, \sqrt{35})$.

Soit $p > 3$ un nombre premier et $\alpha$ un entier naturel premier à $p$. Considérons le corps bi-quadratique réel

$$K_\alpha := \mathbf{Q}\left(\sqrt{\alpha p(\alpha p+2)}, \sqrt{\alpha p(\alpha p-2)}\right).$$

Pour $\alpha = 1$, on retrouve le corps bi-quadratique de la Proposition 2.6.3. Dans chacun des sous-corps quadratiques $k_1 := \mathbf{Q}\left(\sqrt{\alpha p(\alpha p+2)}\right)$, $k_2 := \mathbf{Q}\left(\sqrt{\alpha p(\alpha p-2)}\right)$ et $k_3 := \mathbf{Q}\left(\sqrt{\alpha^2 p^2-4}\right)$ respectivement, $\epsilon_1 := 1+\alpha p+\sqrt{\alpha p(\alpha p+2)}$, $\epsilon_2 := 1-\alpha p+\sqrt{\alpha p(\alpha p-2)}$ et $\epsilon_3 := \dfrac{\alpha p+\sqrt{\alpha^2 p^2-4}}{2}$ est une unité. Puisque $\alpha$ est premier à $p$, on peut montrer par le même raisonnement que celui de la Proposition 2.4.1, que $\epsilon_1$ (resp. $\epsilon_2$) n'est pas une puissance $p^{\text{ème}}$ localement dans $k_1$ (resp. $k_2$). Le même résultat peut être démontré pour $\epsilon_3$ en appliquant les arguments de la preuve de la Proposition 2.6.3. Ainsi $K_\alpha$ est $p$-rationnel dès que $p$ ne divise pas le nombre de classes de chacun des sous-corps $k_i$, où autrement dit, $p \nmid h_{K_\alpha}$ puisque $h_{K_\alpha}$ est le produit de $h_{k_i}$ par une puissance de 2.
Notons qu'il existe $\alpha$ tel que $p \mid h_{K_\alpha}$, par exemple pour $p = 5$ et $\alpha = 17$ et à l'aide de PARI/GP, le nombre de classes de chacun des sous-corps $k_1$, $k_2$ et $k_3$ est respectivement 16, 12 et 10. Ainsi $p \mid h_{k_3}$. Il serait intéressant de trouver une famille infinie d'entiers $\alpha$ pour lesquels $p \nmid h_{K_\alpha}$.

## 2.7 Le cas $t = 3$ de la conjecture de Greenberg

Ayant en main le corps bi-quadratique réel $p$-rationnel $F = \mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{p(p-2)}\right)$ avec $p > 3$, la première question qui vient à l'esprit est de savoir comment ajouter une racine carrée imaginaire afin d'obtenir un corps tri-quadratique $p$-rationnel puisque dans ce cas, et plus généralement pour tout corps multi-quadratique imaginaire $p$-rationnel de degré $\geq 8$, Greenberg a construit dans son article [31] des représentations galoisiennes continues à valeur dans $GL_n(\mathbf{Z}_p)$ avec image ouverte. Plus précisément, nous avons d'une part la proposition suivante :

**Proposition 2.7.1.** *([31, Proposition 6.7]) Soit p un nombre premier impair et supposons que F est un corps multi-quadratique imaginaire p-rationnel de degré $2^t$ où $t \geq 4$. Alors il existe des représentations continues*

$$\rho : G_{\mathbf{Q}} \to GL_n(\mathbf{Z}_p)$$

*du groupe de Galois absolu $G_{\mathbf{Q}}$ de $\mathbf{Q}$ avec image ouverte pour tout $4 \leq n \leq 2^{t-1} - 3$.*

Et d'autre part, par la remarque ([31, Remark 6.8]) qui garantit, pour tout $t \geq 3$, l'existence des représentations dans la proposition ci-dessus pour $n = 2^{t-1}$ et $n = 2^{t-1} + 1$.

Revenons maintenant à notre corps $F$. Puisque les corps quadratiques imaginaires $\mathbf{Q}(\sqrt{-p})$, $\mathbf{Q}\left(\sqrt{-p-2}\right)$ et $\mathbf{Q}\left(\sqrt{-p+2}\right)$ sont $p$-rationnels, la Proposition 2.6.3 entraine que le corps de nombres tri-quadratique

$$L := F(\sqrt{-p}) = \mathbf{Q}\left(\sqrt{-p-2}, \sqrt{-p}, \sqrt{-p+2}\right)$$

est $p$-rationnel précisément lorsque le corps quadratique imaginaire $K := \mathbf{Q}\left(\sqrt{-p(p^2-4)}\right)$ est $p$-rationnel. En utilisant PARI/GP, le plus petit nombre premier inférieur ou égal à $p_0 :=$ 718.328.637 et divisant son nombre de classes est $p_1 :=$ 192.699.943 (pour $p = p_1$, le nombre de classes de $K$ est égal à $2^{10}p_1$). Alors pour tout premier $p \neq p_1$ et $\leq p_0$, le corps $L$ ci-dessus est $p$-rationnel. Il est aussi possible de vérifier en utilisant l'algorithme pour tester la $p$-rationalité mentionné dans [26, section 3.1] (voir le programme ci-dessous) que même pour $p = p_1$, le corps K est $p$-rationnel, ce qui vaut dire que pour tout $p \leq p_0$, le corps $L$ est $p$-rationnel. Il serait intéressant d'étudier sa $p$-rationalité pour un nombre premier arbitraire $p$.

**Programme pour tester la $p$-rationalité pour $p = p_1$ de $\mathbf{Q}\left(\sqrt{-p(p^2-4)}\right)$ :**

```
p=192699943;
K=bnfinit(x^2+p*(p^2-4));
r=K.sign[2];
H=bnrinit(K,p^2);
c=H.cyc;
R=sum(i=1,#c,c[i]%p==0);
if(R==r+1, print("K est ",p,"-rationnel"));
if(R>r+1, print("K n'est pas ",p,"-rationnel"))
```

Par conséquent, l'existence du corps tri-quadratique $p$-rationnel ci-dessus entraine l'exis-

tence de représentations continues

$$\rho : G_{\mathbf{Q}} \to GL_n(\mathbf{Z}_p)$$

avec image ouverte à la fois pour $n = 4$ et $n = 5$ et au moins pour tout $p \leq p_0$.

Un autre choix naturel consiste à ajouter la racine carrée de $-1$ au corps bi-quadratique réel $p$-rationnel $F$. Alors la $p$-rationalité du corps tri-quadratique

$$M_p := \mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{p(p-2)}, \sqrt{-1}\right)$$

est équivalente à celle des trois sous-corps quadratiques imaginaires autres que $\mathbf{Q}(\sqrt{-1})$, ce qui est également intéressant à étudier. Ce corps tri-quadratique à été traité récemment dans [47] où l'auteur se base sur un résultat analytique [47, Proposition 4.1] qui assure l'existence pour $A > 0$, d'une infinité de nombres premiers $p$ tels que $p-2$ et $p+2$ ont des facteurs carrés supérieurs à $(\log p)^A$. Ce résultat lui a permis de montrer pour $A = 2$ et en utilisant la majoration du nombre de classes donnée dans [53, Proposition 2], que pour ces nombres premiers $p$, les trois sous-corps quadratiques imaginaires de $M_p$ autre que $\mathbf{Q}(\sqrt{-1})$, ont des nombres de classes strictement inférieurs à $p$. Par conséquent, Il existe une infinité de nombres premiers $p$ pour lequel $\mathbf{Q}\left(\sqrt{p(p+2)}, \sqrt{p(p-2)}, \sqrt{-1}\right)$ est $p$-rationnel [47, Theorem 3.1], ce qui garantit l'existence des représentations ci-dessus pour une infinité de nombres premiers et à la fois pour $n = 4$ et $n = 5$.

Dans tous les cas, nous pensons que pour chaque premier impair $p > 3$, il existe un entier positif sans facteur carré $d_p$ tel que le nombre de classes relatif de

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

n'est pas divisible par $p$. Un tel corps tri-quadratique est alors $p$-rationnel par les Propositions 2.6.3 et 2.3.12. Par conséquent, nous aurions les représentations ci-dessus

$$\rho : G_{\mathbf{Q}} \to GL_n(\mathbf{Z}_p),$$

pour tout $p > 3$ et à la fois pour $n = 4$ et $n = 5$.

# 3 Le lien entre la $p$-rationalité et les conjectures AAC et de Mordell

Dans tout ce chapitre, le $p$ désigne un nombre premier impair.

*Nous donnons une caractérisation de la $p$-rationalité de $\mathbf{Q}(\sqrt{p})$ qui nous permet ensuite, d'interpréter la conjecture AAC et la conjecture de Mordell concernant l'unité fondamentale de $\mathbf{Q}(\sqrt{p})$, en terme de la $p$-rationalité. Enfin, pour $p \equiv 1 \pmod 4$, nous donnons une condition nécessaire et suffisante pour la montée de la $p$-rationalité en rajoutant $\sqrt{p}$ à un corps multiquadratique réel. Ce chapitre fait l'objet d'un article soumis à publication [11].*

## 3.1 Conjectures AAC et de Mordell et la $p$-rationalité

Soient $t$ et $u$ deux entiers positifs tels que

$$\epsilon_p := \frac{t + u\sqrt{p}}{\alpha} > 1,$$

est l'unité fondamentale de $\mathbf{Q}(\sqrt{p})$, où $\alpha = 2$ si $p \equiv 1 \pmod 4$, sinon $\alpha = 1$.

En 1952, Ankeny, Artin et Chowla [2, page 480] ont demandé si pour $p \equiv 1 \pmod 4$, $\epsilon_p$ avait toujours la propriété que $u \not\equiv 0 \pmod p$. La conjecture selon laquelle la réponse à cette question est affirmative est connue sous le nom de la conjecture de Ankeny-Artin-Chowla (AAC), et n'est toujours pas résolue. Dans un article de 1961, Mordell [58, page 283] a mentionné la conjecture analogue pour le cas où $p \equiv 3 \pmod 4$.

Dans [57, Theorem I], Mordell a prouvé la conjecture AAC pour tout nombre premier régulier. Il a été conjecturé qu'il existe une infinité de nombres premiers réguliers. En fait, en 1964, Siegel [70] a conjecturé que les nombres premiers réguliers ont une densité relative de $1/\sqrt{e}$ (à peu près 60.65%) comme sous-ensemble de tous les nombres premiers. Numériquement, la conjecture AAC a été vérifiée pour les nombres premiers $p < 10^{11}$ par Van Der Poorten, Te

Riele et Williams dans [72]. Dans un rectificatif à [72], les auteurs ont signalé la vérification pour tous les nombres premiers $p < 2 \times 10^{11}$ dans [73].

Pour les deux conjectures (AAC et Mordell), des conditions équivalentes à la non congruence $u \not\equiv 0 \pmod{p}$ peuvent être trouvées dans la littérature. Les articles [19, 21, 32, 34] sont quelques exemples. Par exemple, Hashimoto [34] avait lié la conjecture AAC à la fraction continue de $(1+\sqrt{p})/2$ montrant que la conjecture est vraie pour des $p$ non "petits" dans un certain sens. Ou, plus récemment, Chakraborty et Saikia [19] ont lié la conjecture de Mordell avec la fraction continue de $\sqrt{p}$ montrant l'existence d'un nombre conjecturalement infini de nombres premiers $p$ pour lesquels la conjecture est vraie. Un autre résultat notable concernant la conjecture AAC est celui de Cohen et Thorne [21, Corollaire 9.3]. Ils ont montré que la conjecture AAC est vraie pour un nombre premier $p \equiv 1 \pmod{4}$, si et seulement s'il n'existe pas d'extension galoisienne $N/\mathbf{Q}$ avec $\mathrm{Gal}(N/\mathbf{Q}) \cong D_p$, le groupe diédral d'ordre $2p$, où $p$ est le seul nombre premier ramifié.

De notre côté, nous donnerons une nouvelle condition équivalente pour les deux conjectures qui est basée sur la notion de $p$-rationalité. En particulier, le résultat de Mordell mentionné ci-dessus concernant la validité de la conjecture AAC pour les nombres premiers réguliers serait facilement vu à travers cette nouvelle caractérisation. Cette nouvelle condition équivalente nous permet également de donner une preuve alternative du résultat ci-dessus de Cohen et Thorne et, en outre, conduit à un résultat similaire pour la conjecture de Mordell.

D'abord, nous avons montré dans le chapitre précédent, la $p$-rationalité des corps quadratiques réels $\mathbf{Q}(\sqrt{p(p+2)})$ et $\mathbf{Q}(\sqrt{p(p-2)})$ pour tous $p$, ce qui implique que $\mathbf{Q}(\sqrt{p})$ est $p$-rationnel lorsque $p+2$ ou $p-2$ est un carré. Nous avons aussi fait remarquer qu'il en va de même lorsque $p-1$ ou $p-4$ est un carré. On note également que, puisque le corps cyclotomique $\mathbf{Q}(\mu_p)$ est $p$-rationnel pour un premier régulier, c'est également le cas de tous ses sous-corps, en particulier $\mathbf{Q}(\sqrt{p})$ lorsque $p \equiv 1 \pmod{4}$. Il est alors évident de poser la question suivante :

**Question 3.1.1.** *Est-ce que* $\mathbf{Q}(\sqrt{p})$ *est toujours* $p$*-rationnel?*

Nous ne savons pas l'existence d'un premier $p$ pour lequel $\mathbf{Q}(\sqrt{p})$ n'est pas $p$-rationnel et si un tel premier existe, il est soit irrégulier soit $\equiv 3 \pmod{4}$. Selon la caractérisation de la $p$-rationalité des corps quadratiques réels donnée par la Proposition 2.2.5, la question ne concerne que l'unité fondamentale puisque, $p$ ne divise pas le nombre de classes de $\mathbf{Q}(\sqrt{p})$ (voir Théorème 1.2.3). Autrement dit, $\mathbf{Q}(\sqrt{p})$ est $p$-rationnel si et seulement si l'unité fondamentale $\epsilon_p$ n'est pas une puissance $p^{\text{ème}}$ localement. En utilisant le Corollaire 2.2.8, nous

allons montrer que la $p$-rationalité de $\mathbf{Q}(\sqrt{p})$ peut être vérifiée à travers les nombres de Bernoulli ordinaires ou généralisés. Plus précisément, nous avons la proposition suivante :

**Proposition 3.1.2.** *Le corps quadratique $\mathbf{Q}(\sqrt{p})$ est $p$-rationnel précisément lorsque*
*(i) soit $p \equiv 1 \pmod 4$ et le nombre de Bernoulli ordinaire $B_{\frac{p-1}{2}}$ est une unité $p$-adique;*
*(ii) ou $p \equiv 3 \pmod 4$ et le nombre de Bernoulli généralisé $B_{\frac{p-1}{2},\chi_{\mathbf{Q}(\sqrt{-1})}}$ est une unité $p$-adique.*

*Démonstration.* (i) Par [74, Chapitre 5], nous avons

$$L_p(1,\omega^{\frac{p-1}{2}}) \equiv L_p(0,\omega^{\frac{p-1}{2}}) = -B_{1,\omega^{\frac{p-1}{2}-1}} \equiv -\frac{B_{\frac{p-1}{2}}}{\frac{p-1}{2}} \pmod p.$$

Le Corollaire 2.2.8 complète maintenant la preuve dans ce cas.
(ii) Nous supposons $p > 3$ puisque le cas de $p = 3$ est évident. En appliquant le Lemme 2.2.14 au cas où $d = -1$, $K = \mathbf{Q}(\sqrt{-1})$ et $F = \mathbf{Q}(\sqrt{p})$, on obtient

$$L_p(1,\chi_F) \equiv L(1-\frac{p-1}{2},\chi_K) = -\frac{B_{\frac{p-1}{2}},\chi_K}{\frac{p-1}{2}} \equiv 2B_{\frac{p-1}{2},\chi_K} \pmod p, \tag{3.1}$$

et il suffit d'appliquer à nouveau le Corollaire 2.2.8 pour compléter la preuve. □

Il est facile de remarquer d'après le Théorème 1.1.1, que pour $p \equiv 1 \pmod 4$ (resp. $p \equiv 3 \pmod 4$) et $i = (p-1)/2$, $\mathbf{Q}(\sqrt{p})$ est $p$-rationnel si et seulement si $\zeta(1-i)$ (resp. $L(1-i,\chi_K)$ où $K = \mathbf{Q}(\sqrt{-1})$) est une unité $p$-adique.

Nous allons maintenant relier la proposition ci-dessus aux deux conjectures concernant le corps quadratique $F = \mathbf{Q}(\sqrt{p})$. Supposons d'abord $p \equiv 1 \pmod 4$. Soit $(t+u\sqrt{p})/2 > 1$ l'unité fondamentale de $F$. En 1948, la congruence remarquable suivante a été prouvée pour la première fois par Kiselev [41], puis de façon indépendante par Ankeny et Chowla [3] :

$$\frac{u}{t}h_F \equiv B_{\frac{p-1}{2}} \pmod p.$$

Évidemment $p \nmid t$ et puisque $p \nmid h_F$ non plus, cette conjecture se vérifie précisément lorsque $B_{\frac{p-1}{2}}$ est une unité $p$-adique.

Si au contraire $p \equiv 3 \pmod 4$, Notons par $t+u\sqrt{p} > 1$ l'unité fondamentale de $F$. Nous pouvons supposer que $p > 3$ puisque le cas $p = 3$ est évident. En imitant la preuve de [74, Theorem 5.37], nous avons le même type de congruence que dans le cas précédent. À savoir, par

la formule du nombre de classes $p$-adique

$$L_p(1,\chi_F) = 2h_F \log_p(t+u\sqrt{p})/\sqrt{4p}$$

et

$$\log_p(t+u\sqrt{p}) = \log_p(t) + \log_p(1+\frac{u}{t}\sqrt{p}) \equiv \log_p(1+\frac{u}{t}\sqrt{p}) \equiv \frac{u}{t}\sqrt{p} \pmod{p},$$

puisque le logarithme $p$-adique d'un entier est congru à 0 (mod $p$) et $p \nmid t$. Par conséquent, en combinant avec les congruences (3.1), On en déduit

$$\frac{u}{t}h_F \equiv 2B_{\frac{p-1}{2},\chi_K} \pmod{p},$$

où $K = \mathbf{Q}(\sqrt{-1})$.

Comme dans le cas précédent, cette conjecture se vérifie précisément lorsque $B_{\frac{p-1}{2},\chi_K}$ est une unité $p$-adique.

Maintenant, comme conséquence directe de la Proposition 3.1.2 ci-dessus, nous voyons que les deux conjectures sont vraies précisément lorsque la Question 3.1.1 a une réponse affirmative.

**Corollaire 3.1.3.** *La conjecture d'Ankeny-Artin-Chowla (resp. Mordell) est vraie pour le premier $p \equiv 1 \pmod 4$ (resp. $p \equiv 3 \pmod 4$) précisément lorsque $\mathbf{Q}(\sqrt{p})$ est $p$-rationnel. C'est-à-dire lorsque les seules $p$-extensions $p$-ramifiées de $\mathbf{Q}(\sqrt{p})$ sont les étages de la $\mathbf{Z}_p$-extension cyclotomique de $\mathbf{Q}(\sqrt{p})$.*

Par le paragraphe précédent la Question 3.1.1, La conjecture AAC (resp. Mordell) est vraie pour le premier $p$ tel que $p-1$ ou $p-4$ (resp. $p-2$ ou $p+2$) est un carré (remarquons que l'existence d'une infinité de premiers $p$ dans chaque cas, est conjecturée par Bouniakowsky). Ceci peut également être vu à travers l'unité fondamentale, par exemple, si nous supposons que $p+2 = n^2$, alors l'unité fondamentale de $\mathbf{Q}(\sqrt{p})$ est de la forme $\epsilon_p = p+1+n\sqrt{p}$. La conjecture de Mordell a été vérifiée pour tous les nombres premiers $p < 10^7$ dans [9]. Quelques exemples de $p > 10^7$ vérifiant cette conjecture peuvent également être trouvés dans [19]. Comme conséquence du Corollaire 3.1.3 ci-dessus, nous avons vérifié qu'elle est également vraie pour tous les nombres premiers $p < 1.6 \times 10^9$ en utilisant le programme PARI/GP ci-dessous qui teste la $p$-rationalité (le programme original et général pour tester la $p$-rationalité dû à G. Gras se trouve dans [26, section 3.1]) :

```
forprime(p=3, 1.6*10^9,{
    F=bnfinit(x^2-p);
```

```
    r=F.sign[2];
    H=bnrinit(F,p^2);
    c=H.cyc;
    R=sum(i=1,#c,c[i]%p==0);
    if(R==r+1, print("F est ",p,"-rationnel"));
    if(R>r+1, print("F n'est pas ",p,"-rationnel"))}
)
```

Mentionnons brièvement maintenant le lien avec les extensions diédrales de $\mathbf{Q}$ remarqué par Cohen et Thorne. Soit $L/\mathbf{Q}$ une extension de degré $p$. Soit $N$ la clôture galoisienne de $L/\mathbf{Q}$ et supposons que le groupe galoisien $\mathrm{Gal}(N/\mathbf{Q})$ est isomorphe au groupe diédral $D_p$ d'ordre $2p$. Nous appellerons une telle extension $L/\mathbf{Q}$, une $D_p$-extension, comme ils l'ont fait. Avec une approche différente, notre Corollaire 3.1.3 conduit à leur résultat suivant.

**Proposition 3.1.4.** *([21, Corollaire 9.3]) La conjecture AAC est vraie pour un nombre premier $p \equiv 1 \pmod 4$, si et seulement s'il n'existe pas de $D_p$-extension de $\mathbf{Q}$ où $p$ est le seul nombre premier ramifié.*

*Démonstration.* Supposons d'abord qu'il existe une $D_p$-extension qui est ramifiée seulement en $p$ avec $N$ sa clôture galoisienne. Alors $N/\mathbf{Q}$ est aussi ramifiée seulement en $p$ et puisque $p \equiv 1 \pmod 4$, le sous-corps quadratique de $N$ ne peut être que $F = \mathbf{Q}(\sqrt{p})$. Ainsi, $N/F$ est une extension galoisienne de degré $p$ qui est non-ramifiée en dehors de $p$. Le corps $N$ n'étant pas abélien sur $\mathbf{Q}$ n'est pas contenu dans la $\mathbf{Z}_p$-extension cyclotomique de $F$ et donc $F$ n'est pas $p$-rationnel ce qui, selon le Corollaire 3.1.3, signifie que la conjecture AAC n'est pa vraie pour le premier $p$. Inversement, supposons que le corps quadratique $F = \mathbf{Q}(\sqrt{p})$ n'est pas $p$-rationnel. Introduisons la $p$-extension élémentaire maximale $E$ de $F$ qui est non-ramifiée en dehors des places de $F$ au-dessus de $p$ et considérons l'action naturelle (par conjugaison) de $\mathrm{Gal}(F/\mathbf{Q})$ sur $\mathrm{Gal}(E/F)$. Puisque le corps quadratique réel $F$ est supposé n'est pas $p$-rationnel, cette action n'est pas triviale sur le groupe de Galois $\mathrm{Gal}(E/F)$ et nous avons :

$$\mathrm{Gal}(E/F) \neq \mathrm{Gal}(E/F)^+ := \{\sigma \in \mathrm{Gal}(E/F) \ : \sigma^\tau = \tau\sigma\tau^{-1} = \sigma\}$$

où $\tau$ désigne l'élément non trivial de $\mathrm{Gal}(F/\mathbf{Q})$. Soit $H$ un sous-groupe maximal de $\mathrm{Gal}(E/F)$ contenant $\mathrm{Gal}(E/F)^+$ et désignons par $N$ le corps correspondant dans $E$. Alors $\tau$ induit sur $\mathrm{Gal}(N/F) \cong \mathrm{Gal}(E/F)/H$ l'automorphisme $x \mapsto x^{-1}$ [55, Corollaire 3.2]. Par conséquent, $N/\mathbf{Q}$ est galoisienne et son groupe de Galois est isomorphe à $D_p$. Ainsi, il existe une $D_p$-extension de $\mathbf{Q}$ où $p$ est le seul nombre premier ramifié. □

En ce qui concerne la conjecture de Mordell, notre Corollaire 3.1.3 conduit également à un résultat similaire

**Proposition 3.1.5.** *Étant donné un nombre premier $p \equiv 3 \pmod 4$, les deux conditions suivantes sont équivalentes :*
*(a) La conjecture de Mordell est fausse pour $p$ ;*
*(b) Il existe une $D_p$-extension $L/\mathbf{Q}$ où 2 et $p$ sont les seuls nombres premiers ramifiés, où l'indice de ramification de chaque nombre premier dyadique est au plus égal à 2 et où la valuation 2-adique du discriminant de $L/\mathbf{Q}$ est paire.*

*Démonstration.* Supposons d'abord qu'il existe une telle $D_p$-extension $L/\mathbf{Q}$ avec $N$ sa clôture galoisienne. Soit $\alpha$ tel que $L = \mathbf{Q}(\alpha)$ et désignons par $\varphi(X)$ son polynôme minimal sur $\mathbf{Q}$. Puisque $p \equiv 3 \pmod 4$, le groupe diédral $\mathrm{Gal}(N/\mathbf{Q}) \cong D_p$ considéré comme un groupe de permutation des conjugués de $\alpha$ est impair. En particulier, le sous-corps quadratique de $N$ est égal à $\mathbf{Q}(\sqrt{D_\varphi}) = \mathbf{Q}(\sqrt{D_{L/\mathbf{Q}}})$ où $D_\varphi$ (resp. $D_{L/\mathbf{Q}}$) est le discriminant de $\varphi$ (resp. de l'extension $L/\mathbf{Q}$). Par hypothèse, le seul nombre premier intervenant dans la partie sans facteur carré du discriminant $D_{L/\mathbf{Q}}$ est $p$. Par conséquent, le sous-corps quadratique $F = \mathbf{Q}(\sqrt{D_{L/\mathbf{Q}}})$ de $N$ soit $\mathbf{Q}(\sqrt{p})$ ou bien $\mathbf{Q}(\sqrt{-p})$. De nouveau, par hypothèse, 2 ne peut pas se ramifier dans $N/F$ puisque sinon l'indice de ramification de 2 dans $N/\mathbf{Q}$ serait supérieur à 2. Par conséquent, 2 doit se ramifier dans $F/\mathbf{Q}$ de sorte que $F = \mathbf{Q}(\sqrt{p})$. Le corps $N$ n'étant pas abélien sur $\mathbf{Q}$ n'est pas contenu dans la $\mathbf{Z}_p$-extension cyclotomique de $F$ et donc $F$ n'est pas $p$-rationnel ce qui, selon le Corollaire 3.1.3, signifie que la conjecture de Mordell n'est pas vraie pour le premier correspondant $p$. La réciproque est prouvée de la même manière que dans la proposition 3.1.4 ci-dessus. □

## 3.2 La montée de la $p$-rationalité en rajoutant $\sqrt{p}$

Puisque le corps des nombres rationnels est $p$-rationnel, compte tenu du Corollaire 3.1.3, il est important de savoir sous quelles conditions $F(\sqrt{p})$ est $p$-rationnel si c'est déjà le cas pour le corps de nombres $F$. Dans le Corollaire 2.5.4, nous avons donné une condition nécessaire et suffisante pour qu'un corps multi-quadratique réel reste 5-rationnel en rajoutant $\sqrt{5}$. Dans cette section, nous généralisons ce résultat en remplaçant le nombre premier 5 par tout nombre premier $p \equiv 1 \pmod 4$ en utilisant la Proposition 3.1.2.

Commençons par la définition suivante :

**Définition 3.2.1.** *([4, Définition 1.1]) Soit $i$ un entier. Un corps de nombres $F$ est dit $(p,i)$-régulier lorsque le groupe de cohomologie étale $H^2(o'_F, \mathbf{Z}/p(i)) = 0$.*

Puisque $p$ est supposé impair, la $(p,i)$-régularité de $F$ est équivalente à la nullité de $H^2(o'_F, \mathbf{Z}_p(i))$. Pour $i \geq 2$, un corps de nombres $F$ est $(p,i)$-régulier presque pour tous les nombres premiers $p$ [45, Corollary 2.5]. Le cas $i = 0$ correspond à la $p$-rationalité, tandis que le cas $i = 2$ correspond à la $p$-régularité. Si $\delta$ désigne le degré de l'extension $F(\mu_p)/F$, alors pour deux entiers $i \equiv j \pmod{\delta}$ :

$$H^2(o'_F, \mathbf{Z}/p(i)) \cong H^2(o'_F, \mathbf{Z}/p(j)). \tag{3.2}$$

Considérons un corps de nombres totalement réel $F$ et un entier pair $i \geq 2$. D'après le théorème de Wiles (Théorème 1.4.1) et la discussion dans la section 1.4,

$$w_i(F)\zeta_F(1-i) \sim_p |H^2(o'_F, \mathbf{Z}_p(i))|.$$

Par conséquent, $F$ est $(p,i)$-régulier pour un entier pair $i \geq 2$, précisément lorsque

$$w_i(F)\zeta_F(1-i) \quad \text{est une unité } p\text{-adique.} \tag{3.3}$$

Pour tout le reste de ce chapitre $i := (p-1)/2$. Rappelons que la $p$-partie de $w_i(F)$ d'un corps de nombres $F$, est la puissance maximale $p^m$ telle que l'exposant du groupe de Galois $\mathrm{Gal}(F(\mu_{p^m})/F)$ divise $i$, on la note ainsi $w_i^{(p)}(F)$. Alors nous avons le lemme suivant :

**Lemme 3.2.2.** *Soient $F$ un corps multi-quadratique et $K = \mathbf{Q}\left(\sqrt{(-1)^i p}\right)$. Alors :*
*(a) Si $K \subseteq F$, $w_i^{(p)}(F) = p$,*
*(b) Sinon, $w_i^{(p)}(F) = 1$.*

*Démonstration.* Rappelons tout d'abord, que l'exposant d'un groupe cyclique est égal à son ordre. Commençons par $(a)$. Dans ce cas, le groupe de Galois $\mathrm{Gal}(F(\mu_{p^m})/F)$ est identifié au groupe $\mathrm{Gal}(\mathbf{Q}(\mu_{p^m})/K)$ qui est cyclique d'ordre $p^{m-1}\dfrac{p-1}{2}$. Ainsi $m$ est forcément égal à 1.
Pour la deuxième assertion $(b)$, si $m \geq 1$, le groupe de Galois $\mathrm{Gal}(F(\mu_{p^m})/F)$ est identifié au groupe $\mathrm{Gal}(\mathbf{Q}(\mu_{p^m})/\mathbf{Q})$ qui est cyclique d'ordre $p^{m-1}(p-1)$. Ainsi son exposant ne peut pas diviser $i$. Par conséquent, $m = 0$. □

Soit $F$ un corps de nombres contenant le sous-corps quadratique de $\mathbf{Q}(\mu_p)$. Alors le groupe de Galois $\mathrm{Gal}(F(\mu_p)/F)$ est isomorphe au groupe $\mathrm{Gal}(\mathbf{Q}(\mu_p)/F \cap \mathbf{Q}(\mu_p))$, ainsi $\delta = [F(\mu_p) : F]$ divise $i$. Par conséquent, la formule (3.2) entraine l'isomorphisme :

$$H^2(o'_F, \mathbf{Z}/p) \cong H^2(o'_F, \mathbf{Z}/p(i)).$$

Nous avons donc le corollaire suivant :

**Corollaire 3.2.3.** *Soit $F$ un corps de nombres contenant le sous-corps quadratique de $\mathbf{Q}(\mu_p)$. Alors $F$ est $p$-rationnel précisément lorsqu'il est $(p,i)$-régulier.*

Comme conséquence, en prenant $F = \mathbf{Q}(\sqrt{p})$ dans le corollaire ci-dessus et en utilisant le corollaire 3.1.3, nous pouvons également exprimer les conjectures AAC et de Mordell en termes de $(p,i)$-régularité :

**Proposition 3.2.4.** *La conjecture AAC (resp. Mordell) est vraie pour $p \equiv 1 \pmod 4$ (resp. $p \equiv 3 \pmod 4$) si et seulement si $\mathbf{Q}(\sqrt{p})$ est $(p,i)$-régulier.*

**Remarque 3.2.5.** *Pour $F = \mathbf{Q}(\sqrt{p})$, on a $w_i^{(p)}(F) = p$ par le Lemme 3.2.2. Ainsi, selon les propositions 3.1.2 et 3.2.4 et la caractérisation (3.3)*

$$L(1-i,\chi_F) \sim p^{-1},$$

*pour $p \equiv 1 \pmod 4$ (voir aussi [17, Theorem 3]).*

Nous avons vu dans le chapitre précédent, que pour $d \neq 5$ un entier positif sans facteur carré, la 5-rationalité de $\mathbf{Q}(\sqrt{d})$ se lit à travers la 5-régularité de $\mathbf{Q}(\sqrt{5d})$. Nous avons alors la généralisation suivante :

**Proposition 3.2.6.** *Soient $p \equiv 1 \pmod 4$ et $d \neq p$ un entier positif sans facteur carré. Alors les deux conditions suivantes sont équivalentes :*
*(a) $\mathbf{Q}(\sqrt{d})$ et $\mathbf{Q}(\sqrt{p})$ sont $p$-rationnels,*
*(b) $K = \mathbf{Q}(\sqrt{pd})$ est $(p,i)$-régulier.*

*Démonstration.* L'équivalence est déjà établie lorsque $d = 1$. Supposons que $d > 1$ et $K$ est $(p,i)$-régulier. Puisque $K \neq \mathbf{Q}(\sqrt{p})$, d'après le Lemme 3.2.2 $p$ ne divise pas $w_i(F)$. Par conséquent,

$$\zeta_K(1-i) = \zeta(1-i)L(1-i,\chi_K)$$

est une unité $p$-adique. Ainsi, chaque facteur est une unité $p$-adique, puisqu'ils sont tous les deux des entiers $p$-adiques. Cela revient à dire que $\mathbf{Q}(\sqrt{p})$ est $p$-rationnel (voir le paragraphe qui suit la preuve de la Proposition 3.1.2) et $\mathbf{Q}(\sqrt{d})$ est $p$-rationnel par le Lemme 2.2.14 et le Corollaire 2.2.8. □

Une conséquence immédiate de cette proposition est que l'existence d'un corps quadratique réel $(p,i)$-régulier entraine que la conjecture AAC est vraie pour $p$.

Nous avons également le résultat suivant concernant la $(p,i)$-régularité qui est un résultat similaire à la Proposition 2.2.9 dans le cas d'un corps réel multi-quadratique.

**Lemme 3.2.7.** *Soit $p \equiv 1 \pmod 4$ et $i := (p-1)/2$. Un corps réel multi-quadratique $F$ est $(p,i)$-régulier précisément lorsqu'il est le cas de tous ses sous-corps quadratiques.*

*Démonstration.* Remarquons d'abord que $w_i^{(p)}(F) = \prod_k w_i^{(p)}(k)$ où $k$ parcourt l'ensemble des sous-corps quadratiques de $F$ (Lemme 3.2.2). Donc par la caractérisation (3.3),

$$\begin{aligned} F \text{ is } (p,i)-\text{regular} &\iff w_i^{(p)}(F)\zeta_F(1-i) \sim 1 \\ &\iff \zeta(1-i)\prod_k w_i^{(p)}(k)L(1-i,\chi_k) \sim 1 \end{aligned}$$

Puisque chaque facteur est un entier $p$-adique (à moins que $\sqrt{p} \in F$, auquel cas $L(1-i,\chi_{\mathbf{Q}(\sqrt{p})}) \sim p^{-1}$ par la Remarque 3.2.5 qui est compensé par $w_i^{(p)}(\mathbf{Q}(\sqrt{p})) = p$), la dernière condition est équivalente à

$$w_i^{(p)}(k)\zeta_k(1-i) \sim 1$$

pour tous les sous-corps quadratiques $k$ de $F$, ce qui signifie à son tour que tous les sous-corps quadratiques de $F$ sont $(p,i)$-réguliers. □

Finalement, nous arrivons à la généralisation du Corollaire 2.5.4.

**Proposition 3.2.8.** *Soit $p \equiv 1 \pmod 4$ et $F$ un corps multi-quadratique réel. Alors $F$ est à la fois $p$-rationnel et $(p,i)$-régulier précisément lorsque $F(\sqrt{p})$ est $p$-rationnel.*

*Démonstration.* Lorsque $\sqrt{p} \in F$, l'équivalence est établie par le Corollaire 3.2.3. Supposons alors que $\sqrt{p} \notin F$ qui entraine que $p$ ne divise pas $w_i(F)$. D'après le Théorème 1.2.1

$$\zeta_F(1-i) = \zeta(1-i) \prod_{\chi \neq \chi_0} L(1-i,\chi),$$

où $\chi$ parcourt l'ensemble des caractères associés aux sous-corps quadratiques $\mathbf{Q}\left(\sqrt{d}\right)$ de $F$. Puisque chacun des $d \neq p$, les facteurs ci-dessus sont des entiers $p$-adiques. Ainsi la Proposition 3.2.6, montre que $\mathbf{Q}\left(\sqrt{d}\right)$ est $(p,i)$-régulier si et seulement si $\mathbf{Q}\left(\sqrt{p}\right)$ et $\mathbf{Q}\left(\sqrt{pd}\right)$ sont $p$-rationnels. Pour terminer la preuve, il suffit d'appliquer la Proposition 2.2.9 pour la $p$-rationalité et le lemme 3.2.7 pour la $(p,i)$-régularité. □

Puisque $\mathbf{Q}$ est $p$-rationnel pour tout nombre premier $p$, la Proposition ci-dessus montre que, pour $p \equiv 1 \pmod 4$, $\mathbf{Q}(\sqrt{p})$ est $p$-rationnel précisément lorsque $\mathbf{Q}$ est $(p,i)$-régulier. Cette

équivalence peut également être obtenue en combinant la caractérisation (3.3) et le paragraphe qui suit la Proposition 3.1.2.

# *Glossaire*

| | |
|---|---|
| $p$ | un nombre premier ; |
| $F$ | un corps de nombres ; |
| $o_F$ | l'anneau des entiers de $F$ ; |
| $o'_F = o_F[1/p]$ | l'anneau des $p$-entiers de $F$ ; |
| $d_F$ | le discriminant de $F/\mathbf{Q}$ ; |
| $h_F$ | le nombre de classes de $F$ ; |
| $r_1$ (resp. $r_2$) | le nombre de places réelles (resp. complexes) de $F$ ; |
| $\zeta_F$ | la fonction zêta de Dedekind de $F$ ; |
| $\mu_n$ | le groupe des racines $n^{\text{ème}}$ de l'unité ; |
| $\mu_{p^\infty}$ | le groupe de tous les éléments dont l'ordre est une puissance de $p$ ; |
| $\mu_p(F) = \mu_p \cap F$ | le groupe des racines $p^{\text{ème}}$ de l'unité dans $F$ ; |
| $U_F$ | le groupe des unités de $F$ ; |
| $\bar{U}_F = \varprojlim(U_F/p^m)$ | le pro-$p$-complété de $U_F$ ; |
| $F_v$ | le complété de $F$ en une place $v$ de $F$ ; |
| $U_v$ | le groupe des unités locales de $F_v$ ; |
| $\bar{U}_v = \varprojlim(U_v/p^m)$ | le pro-$p$-complété de $U_v$ ; |
| $S$ | l'ensemble des places de $F$ au-dessus de $p$ ; |
| $A_F$ | la partie $p$-primaire du groupe de classes de $F$ ; |
| $A'_F$ | la partie $p$-primaire du $(p)$-groupe de classes de $F$ ; |
| $F_S$ | la pro-$p$-extension $S$-ramifiée maximale de $F$ ; |
| $F_S^{ab}$ | la pro-$p$-extension abélienne $S$-ramifiée maximale de $F$ ; |
| $\tilde{F}$ | le composé de toutes les $\mathbf{Z}_p$-extensions de $F$ ; |
| $G_S(F) := \mathrm{Gal}(F_S/F)$ | le groupe de Galois de l'extension $F_S/F$ ; |
| $\mathcal{G}_S(F) := \mathrm{Gal}(\Omega_S/F)$ | le groupe de Galois de l'extension $S$-ramifiée maximale $\Omega_S$ de $F$ ; |
| $X_F := \mathrm{Gal}(F_S^{ab}/F)$ | le groupe de Galois de l'extension $F_S^{ab}/F$ ; |
| $T_F := \mathrm{Tor}_{\mathbf{Z}_p}(X_F)$ | le groupe de torsion de $X_F$. |

# *Bibliographie*


[1] T. Agoh, 'Congruences related to the Ankeny-Artin-Chowla conjecture', *Integers 16* (2016), no. A12, 30 pp.

[2] N. C. Ankeny, E. Artin and S. Chowla, 'The class-number of real quadratic number fields', *Ann. of Math.* (2) 56 (1952), 479–493.

[3] N. C. Ankeny and S. Chowla, 'A further note on the class number of real quadratic fields', *Acta Arith.* 7 (1962), 271–272.

[4] J. Assim, 'Codescente en $K$-théorie étale et corps de nombres', *Manuscripta Math.* 86 (1995), no. 4, 499–518.

[5] J. Assim and Z. Bouazzaoui, 'Half-integral weight modular forms and real quadratic $p$-rational fields', *Funct. Approx. Comment. Math.* 63 (2020), no. 2, 201–213.

[6] J. Assim and A. Movahhedi, 'Galois codescent for motivic tame kernels', Preprint, https ://arxiv.org/abs/1901.07219.

[7] J. Ax, 'On the units of an algebraic number field', *Illinois J. Math.* 9 (1965), 584–589.

[8] R. Barbulescu and J. Ray, 'Numerical verification of the Cohen-Lenstra-Martinet heuristics and of Greenberg's $p$-rationality conjecture', *J. Théor. Nombres Bordeaux* 32 (2020), no. 1, 159–177.

[9] B. D. Beach, H. C. Williams and C. R. Zarnke, 'Some computer results on units in quadratic and cubic fields', Proc. 25th Summer Meeting Can. Math. Congress, Lakehead Univ. (1971), 609–648.

[10] O. Beckwith, 'Indivisibility of class numbers of imaginary quadratic fields', *Res. Math. Sci.* 4 (2017), no. 20, 11 pp.

[11] Y. Benmerieme and A. Movahhedi, 'Ankeny-Artin-Chowla and Mordell conjectures in terms of $p$-rationality'. Soumis, 2021.

[12] Y. Benmerieme and A. Movahhedi, 'Multi-quadratic $p$-rational number fields'. *J. Pure Appl. Algebra* 225 (2021), no. 9, 106657, 17 pp.

[13] Z. Bouazzaoui, 'Fibonacci numbers and real quadratic $p$-rational fields'. *Period. Math. Hungar.* 81 (2020), no. 1, 123–133.

[14] J. Browkin, 'On the divisibility by 3 of $\#K_2O_F$ for real quadratic fields $F$', *Demonstratio Math.* 18 (1985), no. 1, 153–159.

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

[16] D. Byeon, 'Existence of certain fundamental discriminants and class numbers of real quadratic fields', *J. Number Theory* 98 (2003), no. 2, 432–437.

[17] L. Carlitz, 'Arithmetic properties of generalized Bernoulli numbers'. *J. Reine Angew. Math.* 202 (1959), 174–182.

[18] J. W. S. Cassels and A. Fröhlich, 'Algebraic Number Theory', Academic Press, London, Thompson Book Co., Inc., Washington, D.C. (1967).

[19] D. Chakraborty and A. Saikia, 'On a conjecture of Mordell', *Rocky Mountain J. Math.* 49 (8)2545–2556, 2019.

[20] J. Coates, '$p$-adic $L$-functions and Iwasawa's theory', *Algebraic number fields : L-functions and Galois properties*, (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 269–353. Academic Press, London, 1977.

[21] H. Cohen and F. Thorne, 'On $D_l$-extensions of odd prime degree $l$'. *Proc. Lond. Math. Soc.* (3) 121 (2020), no. 5, 1171–1206.

[22] P. Colmez, 'Arithmétique de la fonction zêta', 37–164, Ed. Éc. Polytech., Palaiseau, 2003.

[23] P. Colmez, 'Résidu en $s = 1$ des fonctions zêta $p$-adiques', *Invent. Math.* 91 (1988), no. 2, 371–389.

[24] C. Cornut and J. Ray , 'Generators of the pro-$p$ Iwahori and Galois representations', *Int. J. Number Theory* 14 (2018), no. 1, 37–53.

[25] S. Fujii, 'On the maximal pro-$p$ extension unramified outside $p$ of an imaginary quadratic field', *Osaka J. Math.* 45 (2008), no. 1, 41–60.

[26] G. Gras, 'On $p$-rationality of number fields. Applications ? PARI/GP programs', Publications Mathématiques de Besançon - Algèbre et Théorie des Nombres, no. 2 (2019), pp. 29–51.

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

[28] G. Gras, 'Les $\theta$-régulateurs locaux d'un nombre algébrique : Conjectures $p$-adiques', *Canadian J. of Math.* 68(3) (2016), 571–624.

[29] G. Gras, 'Remarks on $K2$ of number fields', *J. Number Theory* 23 (1986), no. 3, 322–335.

[30] G. Gras and J.F. Jaulent, 'Sur les corps de nombres réguliers', *Math. Z.* 202 (1989), no. 3, 343–365.

[31] R. Greenberg, 'Galois representation with open image', *Ann. Math. Qué.* 40 (2016), no. 1, 83–119.

[32] J. Harrington and L. Jones, 'A new condition equivalent to the Ankeny-Artin-Chowla conjecture', *J. Number Theory* 192 (2018), 240–250.

[33] P. Hartung, 'Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3', *J. Number Theory* 6 (1974) 276–278.

[34] R. Hashimoto, 'Ankeny-Artin-Chowla Conjecture and Continued Fraction Expansion', *J. Number Theory* 90 (2001), no. 1, 143–153.

[35] K. Horie, 'Trace formulae and imaginary quadratic fields', *Math. Ann.* 288 (1990), no. 4, 605–612.

[36] K. Horie and Y. Onishi, 'The existence of certain infinite families of imaginary quadratic fields', *J. Reine Angew. Math.* 390 (1988), 97–113.

[37] K. Iwasawa, 'Lectures on $p$-adic $L$-functions', *Annals of Mathematics Studies*, No. 74. Princeton University Press, Princeton, N.J ; University of Tokyo Press, Tokyo, 1972. vii+106 pp.

[38] W. Jehne, 'On knots in algebraic number theory', *J. Reine Angew. Math.* 311(312) (1979), 215–254.

[39] K. Kato, N. Kurokawa and T. Saito, 'Number Theory I. Fermat's Dream', Transl. Math. Monogr., Iwanami Series in Modern Mathematics 186 AMS, Providence (2000)

[40] N. M. Katz, 'A note on Galois representations with big image', *Enseign. Math.* 65 (2019) no. 3-4, 271–301.

[41] A. A. Kiselev, 'An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers', Dokl. Akad. Nauk SSSR (N.S.), 61 (1948), 777–779.

[42] H. Koch, 'Algebraic number theory', Springer-Verlag, Berlin, 1997.

[43] W. Kohnen and K. Ono, 'Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication', *Invent. Math.* 135 (1999), no. 2, 387–398.

[44] M. Kolster, 'Higher relative class number formulae', *Math. Ann.* 323 (2002), no. 4, 667–692.

[45] M. Kolster, '$K$-theory and arithmetic', *Contemporary developments in algebraic $K$-theory*, 191–258 (electronic), ICTP Lect. Notes, XV, Abdus Salam Int. Cent. Theoret. Phys., Trieste, 2004.

[46] M. Kolster and A. Movahhedi, 'Bi-quadratic number fields with trivial 2-primary Hilbert kernels', *Proc. London Math. Soc.* (3) 87 (2003), no. 1, 109–136.

[47] J. Koperecz, 'Triquadratic $p$-Rational Fields', Preprint, arXiv :2103.15648.

[48] E. Landau, 'Elementary number theory' , Translated by J. E. Goodman. Chelsea Publishing Co., New York, N.Y., 1958. 256 pp.

[49] Mao Hua Le, 'Upper bounds for class numbers of real quadratic fields', *Acta Arith.* 68 (1994), no. 2, 141–144.

[50] S. Lang, 'Algebraic number theory', 2nd ed., Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994. xiv+357 pp.

[51] S. Lang, 'Cyclotomic fields II', Graduate Texts in Mathematics, 69. Springer-Verlag, New York-Berlin, 1980. xi+164 pp.

[52] S. R. Louboutin, 'Explicit upper bounds for values at $s = 1$ of Dirichlet $L$-series associated with primitive even characters', *J. Number Theory.* 104 (2004), no. 1, 118–131.

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

[54] C. Maire and M. Rougnant, 'A note on $p$-rational fields and the $abc$-conjecture', *Proc. Amer. Math. Soc.* 148 (2020), no. 8, 3263–3271.

[55] B. Mazur and K. Rubin, 'Growth of Selmer rank in nonabelian extensions of number fields', *Duke Math. J.* 143 (2008) 437–461.

[56] J. Milnor, 'Introduction to algebraic K-theory, Annals of Mathematics Studies, No. 72. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971. xiii+184 pp.

[57] L. J. Mordell, 'On a pellian equation conjecture', *Acta Arith.* 6 (1960), 137–144.

[58] L. J. Mordell, 'On a Pellian equation conjecture. II', *J. London Math. Soc.* 36 (1961), 282–288.

[59] A. Movahhedi, 'Sur les $p$-extensions des corps $p$-rationnels', Thèse de doctorat en Mathématiques. Paris VII (1988).

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

[61] A. Movahhedi and T. Nguyen Quang Do, 'Sur l'arithmétique des corps de nombres $p$-rationnels', in Séminaire de Théorie des nombres, Paris 1987-88, 155–200, Progr. Math., 81, Birkhäuser, Boston, Boston, MA, 1990.

[62] H. Naito, 'Indivisibility of class numbers of totally imaginary quadratic extensions and their Iwasawa invariants', *J. Math. Soc.* Japan 43 (1991), no. 1, 185–194.

[63] O. Neumann, 'On $p$-closed algebraic number fields with restricted ramification', Izv. Akad. Nauk SSSR Ser. Mat., 39 :2 (1975) ; Math. USSR-Izv., 9 :2 (1975), 243–254.

[64] T. Nguyen Quang Do, 'Sur la $\mathbf{Z}_p$-torsion de certains modules galoisiens', *Ann. Inst. Fourier (Grenoble)*. 36 (1986), no. 2, 27–46.

[65] T. Nguyen Quang Do, 'On Greenberg's generalized conjecture for families of number fields', Preprint.

[66] K. Ono, 'Indivisibility of class numbers of real quadratic fields', *Compositio Math.* 119 (1999), no. 2, 1–11.

[67] O. Ramaré, 'Approximate formulae for $L(1,\chi)$', *Acta Arith.* 100 (2001), no. 3, 245–266.

[68] P. Ribenboim, 'Classical Theory of Algebraic Numbers', UTX, Springer-Verlag, New York-Berlin-Heidelberg, 2001.

[69] J.-P. Serre, 'Corps locaux', Publications de l'Institut de Mathématique de l'Université de Nancago, VIII Actualités Sci. Indust., No. 1296. Hermann, Paris (1962) 243 pp.

[70] C. L. Siegel, 'Zu zwei Bemerkungen Kummers', Nachr. Akad. Wiss. Göttingen, Math. Phys. Kl. II 1964 (1964), 51–62.

[71] C. Soulé, 'K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale', *Invent. Math.* 55 (1979), no. 3, 251–295.

[72] A. J. Van Der Poorten, H. J. J. te Riele and H. C. Williams, 'Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than 100000000000', *Math. Comp.* 70 (2001), no. 235, 1311–1328.

[73] A. J. Van Der Poorten, H. J. J. te Riele and H. C. Williams, 'Corrigenda and addition to : "Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than 100000000000"', *Math. Comp.* 70 (2001), no. 235, 1311–1328.

[74] L. C. Washington, 'Introduction to cyclotomic fields', 2nd ed., Graduate Texts in Mathematics 83. Springer-Verlag, New York, 1997.

[75] A. Wiles, 'The Iwasawa conjecture for totally real fields', *Ann. of Math.* (2) 131 (1990), no. 3, 493–540.

[76] A. Wiles, 'On class groups of imaginary quadratic fields', *J. Lond. Math. Soc.* (2) 92 (2015), no. 2, 411–426.