# Comptage asymptotique et algorithmique d'extensions cubiques relatives

Anna Morra

N° d'ordre : 3903

# THÈSE

**présentée à**

# L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par **Anna Morra**

POUR OBTENIR LE GRADE DE

## DOCTEUR

SPÉCIALITÉ : **Mathématiques Pures**

**********

## Comptage asymptotique et algorithmique d'extensions cubiques relatives

**********

Soutenue le 7 décembre 2009 à l'Institut de Mathématiques de Bordeaux

Après avis de :

| | | |
|---|---|---|
| J. CREMONA | Professeur, Warwick University, United Kingdom | **Rapporteur** |
| J. KLÜNERS | Professeur, Universität Paderborn, Germany | **Rapporteur** |

Devant la commission d'examen composée de :

| | | |
|---|---|---|
| K. BELABAS | Professeur, Université Bordeaux I | **Directeur** |
| H. COHEN | Professeur, Université Bordeaux I | |
| J. M. COUVEIGNES | Professeur, Université Toulouse 2 | |
| C. DELAUNAY | Maître de Conferences (HDR), Université Lyon 1 | |

**- 2009 -**

# Acknowledgements

This thesis was supported by the European Community under the Marie Curie Research Training Network GTEM (MRTN-CT-2006-035495). I would like in particular to thank all the scientists in charge of the project, who did a lot of work to make this network active, to organise meetings and workshops and, last but not least, to solve administrative problems : B. De Smit, M. Matignon, T. Crespo, G. Frey, H. Matzat, E. Bayer, J. Denef, P. Dèbes, J. Cremona, L. Schneps, R. Schoof and M. Jarden.

This grant allowed me to meet a lot of nice people, in particular, I would like to greet all the GTEM ESR's.

I would like to thank my thesis referees: John Cremona and Jürgen Klüners, who did a great work and moreover, they respected administrative deadlines.

I am grateful to the jury external members, wo accepted to come at my defense, also if we prevented them quite late : J. M. Couveignes and C. Delaunay.

Moreover, I would like to thank Warwick University staff and students who have been very nice during my stay there (hugs to Maite and Carlos).

I would also like to thank my italian professor, A. Languasco, who encouraged me to come to France.

**********

Je remercie mon directeur de thèse, Karim Belabas, pour m'avoir proposé ce sujet de thèse et m'avoir suivie pendant ces trois années, en me permettant de soutenir dans les délais souhaités.

Je remercie Henri Cohen, qui est depuis plusieurs années une de mes références principales, et qui est une personne de laquelle on peut toujours apprendre quelque chose.

Je remercie aussi tout le personnel administratif de l'Université Bordeaux 1, en particulier Annie Polzin, Karine Lecuona et Catherine Vrit qui ont souvent résolu mes problèmes. Un merci très sincère aux ingénieurs de calcul pour tous les batch que j'ai fait planter en trois ans, voire plus...

Je remercie le CELAR de Rennes où j'ai pu faire deux stages, et en particulier David Lubicz et Reynald Lercier.

Merci enfin à tous les collègues doctorants et ancien doctorants : Pascal (qui me supporte pendant mes permanences au bureau), Fabien, Florent, François, Joyce, Alice, et tous les autres.

Un merci spécial aux doctorants italiens qui on fait un séjour à Bordeaux et qui ont adouci ma peine d'être loin de mon Pays: un abbraccio a Marco I., Marco S., Chiara, Federico e Luca.

**********

Un saluto a tutti i miei amici italiani, che vedo troppo poco spesso, ma a cui voglio bene : Lucky, Elena, Vale, Elisa C., Elisa R., Francesca, Marco M. (con cui avevo fatto una scommessa qualche anno fa...).

Infine, un abbraccio a tutta la mia famiglia e un grazie di tutto cuore ai miei genitori, che hanno creduto in me anche quando io stessa non ci credevo e mi hanno sostenuta nei momenti difficili.

*Et merci Alexandre, car sans toi rien ne serait pareil.*

# Contents

# Introduction

## Motivation

Soit $K$ un corps de nombres, $G$ un groupe de permutations transitif sur $n$ éléments. On définit $\mathcal{F}_{K,n}(G)$ l'ensemble des classes d'isomorphisme d'extensions $L/K$ de degré $n$ telles que la clôture galoisienne $N$ de $L/K$ ait groupe de Galois isomorphe à $G$.

Cette thèse étudie la fonction de comptage

$$N_{K,n}(G,X) = |\{L \in \mathcal{F}_{K,n}(G), \mathcal{N}\mathfrak{d}(L/K) \leq X\}|,$$

qui énumère les éléments de $\mathcal{F}_{K,n}(G)$, ordonnés par discriminant relatif. On va adopter deux points de vue différents, et, en quelque sorte, complémentaires.

### Asymptotique

D'un côté, on a le point de vue asymptotique, quand $X$ tend vers l'infini. Celui-ci est un thème classique, qui remonte à Gauss [35], qui compta les classes de formes quadratiques binaires avec discriminant borné. Un certain nombre de conjectures importantes ont été formulées récemment à propos de ce sujet, par Malle [43], Bhargava ([3, §6.2]) et Ellenberg et Venkatesh [30]. La conjecture de Malle est sans doute la plus célèbre. Elle affirme que

$$N_{K,n}(G,X) \sim c(G,K)X^{a(G)}(\log X)^{b(G,K)-1},$$

avec des constantes explicites, $a$ dépendant seulement de $G$ et $b$ et $c$ dépendant de $G$ et de $K$.

Cette conjecture a été prouvée pour les groupes abéliens [42, 55], et pour la plupart des extensions de degré $\leq 5$, au moins sur $\mathbb{Q}$. Un certain nombre de résultats fondamentaux a été obtenu, en particulier, par Cohn [21], Davenport-Heilbronn [26], Datskovsky-Wright [27], Cohen-Diaz y Diaz-Olivier [17, 18, 19], et Bhargava [5, 6, 7]. Pour un survol historique sur les développements de ce sujet jusqu'à 2005, on invite le lecteur à faire référence à [16] et [3].

En 2005, Klüners [40] donna un contre-exemple à la conjecture de Malle, qui se basait sur la présence de certaines racines de l'unité dans des extensions intermediaires. Türkelli [52] a proposé une modification à la conjecture de Malle, qui évite ce type de contre-exemples.

### Algorithmique

Notre deuxième point de vue dans le comptage d'extensions de corps de nombres est algorithmique. Dans ce cadre, on peut placer le travail de Belabas [1, 2]

ainsi que beaucoup d'autres (pour un survol, voir [44]). Dans cette perspective particulière, la théorie de la réduction et la géometrie des nombres, ainsi que les bijections explicites motivées par la classification des espaces préhomogènes, deviennent les acteurs principaux. Si les derniers sont des objets plutôt récents, la théorie de la réduction a une histoire assez longue, qui remonte au moins au travail de Gauss sur les formes quadratiques binaires et ternaires. Après lui, Bianchi [10], Julia [39] et d'autres, ont generalisé cette théorie à d'autres corps de nombres, en particulier ceux quadratiques imaginaires. Tout le 19ème siècle a été fasciné par la théorie des invariants, un chapitre conclu par la preuve de Hilbert que l'algèbre des invariants est de type fini [37]. Après cela, la théorie des invariants a été rendue de plus en plus abstraite, en utilisant les répresentations de groupes et la théorie des invariants géometriques de Mumford [46]. Mais la théorie des invariants classique trouva des nouvelles applications, et devint à nouveau très actuelle dans les travaux plus récents de Elstrodt, Grunewald et Mennicke [31, 32, 33] (dans leur travail sur l'espace hyperbolique 3-dimensionnel), Cremona et Stoll [23, 25] (qui étaient motivés par l'étude des courbes elliptiques et hyperelliptiques) et enfin dans le travail de Bhargava [5, 6, 7, 8, 9], qui généralise la loi de composition de Gauss et trouve des bijections très intéressantes, pour paramétriser les corps de nombres de degré $\leq 5$ et des parties de leur groupe de classes.

## Structure de la thèse

Cette thèse s'intéresse aux deux manières de compter les corps de nombres décrites ci-dessus.

Le premier chapitre est un travail joint avec Henri Cohen; on prouve une nouvelle formule asymptotique pour les extensions quadratiques avec une résolvante quadratique fixée (Theorem 1.6.2), en raffinant la Conjecture de Malle.

Le second chapitre décrit un nouveau algorithme, pour énumerer toutes les extensions cubiques d'un corps de nombres quadratique imaginaire de nombre de classes 1, avec discriminant relatif borné, en temps presque-linéaire.

L'appendix A esquisse la preuve de l'extension de la théorie de Davenport-Heilbronn, dûe à Taniguchi.

L'appendix B décrit l'algorithme classique pour énumerer les extensions cubiques d'un corps de nombres donné, en utilisant la théorie des corps de classes de rayon.

L'appendix C étudie les erreurs d'arrondis dans les calculs en précision flottante dans notre algorithme principal.

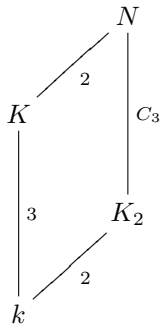
L'appendix D donne des polynômes explicites dont on a besoin pour vérifier rigoureusement les conditions de bords dans notre théorie de la réduction pour formes cubiques binaires sur des corps quadratiques imaginaires.

On va maintenant présenter en détail nos résultats principaux.

### Comptage d'extensions cubiques avec résolvante quadratique fixée

Soit $k$ un corps de nombres fixé. On considère une extension cubique $K/k$ et on appelle $N$ la clôture Galoisienne de $K/k$. Quand $K/k$ n'est pas cyclique on

a $\mathrm{Gal}(N/k) \simeq S_3$, et le corps de nombres $N$ contient une unique sous-extension quadratique $K_2/k$.




Quand $K/k$ est cyclique on a $N = K$ et $\mathrm{Gal}(N/k) \simeq C_3$. Ce cas a déjà été traité dans [18], mais on l'inclut ici pour des raisons d'exhaustivité, en posant $K_2 = k$; par abus de langage on appelle toujours $K_2$ une extension quadratique de $k$, même si $[K_2 : k] = 1$.

On fixe l'extension quadratique $K_2/k$, et on appelle $\mathcal{F}(K_2)$ l'ensemble des extensions cubiques $K/k$, modulo $k$-isomorphisme, telles que la sous-extension quadratique de la clôture Galoisienne de $K/k$ soit isomorphe à $K_2$.

On définit

$$N(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{d}(K/k)) \leq X\}| \ .$$

où $\mathfrak{d}(K/k)$ est le discriminant relatif de $K/k$ et $\mathcal{N}_{k/\mathbb{Q}}$ dénote la norme absolue. On invite le lecteur à remarquer que

$$N_{k,3}(S_3, X) = \sum_{K_2/k, K_2 \neq k} N(K_2/k, X), \quad \text{et} \quad N_{k,3}(C_3, X) = N(k/k, X),$$

donc on est en train d'étudier un raffinement de la conjecture de Malle. Notre théorème principal (Theorem 1.6.2) donne une formule asymptotique pour $N(K_2/k, X)$; on l'énonce ici seulement dans le cas $k = \mathbb{Q}$. Dans ce simple cas, on utilise la notation $N(K_2, X)$ à la place de $N(K_2/\mathbb{Q}, X)$.

**Théorème.** *Comme ci-dessus, soit $K_2 = \mathbb{Q}(\sqrt{D})$ une extension de $\mathbb{Q}$ avec $[K_2 : \mathbb{Q}] \leq 2$, on dénote par $K_2' = \mathbb{Q}(\sqrt{-3D})$ le corps miroir de $K_2$, et l'on pose $g(K_2') = 3$ si $K_2' = \mathbb{Q}(\sqrt{-3})$, et $g(K_2') = 1$ sinon. Alors:*

(1) *(Corps cubiques purs.) On a*

$$N(\mathbb{Q}(\sqrt{-3}), X) = C(\mathbb{Q}(\sqrt{-3}))Y(\log(Y) + D(\mathbb{Q}(\sqrt{-3})) - 1) + O(Y^{2/3+\varepsilon}),$$

*pour tout $\varepsilon > 0$, où $Y = \sqrt{X/\mathfrak{d}(K_2/k)}$*

$$C(\mathbb{Q}(\sqrt{-3})) = \frac{7}{30} \prod_p \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right)$$

$$D(\mathbb{Q}(\sqrt{-3})) = 2\gamma - \frac{16}{35}\log(3) + 6\sum_p \frac{\log(p)}{p^2 + p - 2} \ ,$$

*et $\gamma$ est la constante d'Euler.*

(2) *(Cas général.) Pour $D \neq -3$, on note $a_{K_2'}(p)$ le nombre d'idéaux premiers de degré 1 (non ramifiés) au dessus de $p$ dans $K_2'$. Alors*

$$N(\mathbb{Q}(\sqrt{D}), X) = C(\mathbb{Q}(\sqrt{D}))Y + O(Y^{2/3+\varepsilon}) ,$$

*où* $Y = \sqrt{X/\mathfrak{d}(K_2/k)}$

$$C(\mathbb{Q}(\sqrt{D})) = g(K_2')\frac{c_3(K_2')}{3^{3+r_2(K_2')}} \prod_{p\neq 3} \left(1 + \frac{a_{K_2'}(p)}{p}\right)\left(1 - \frac{1}{p}\right) ,$$

*et*

$$c_3(K_2') = \begin{cases} 11 & \text{si } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1^2 , \\ 15 & \text{si } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1 , \\ 21 & \text{si } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1\mathfrak{p}_2 . \end{cases}$$

On souligne le fait que la formule dans (2) a été donnée à cause de son élégance, mais elle *ne doit pas* être utilisée pour les calculs pratiques des constantes; pour cela se référer au Corollaire 1.8.6 ci-dessous.

## Un algorithme pour énumerer les extensions cubiques

Le second chapitre concerne le point de vue algorithmique. L'idée est de généraliser l'algorithme de Belabas énumérant les extensions cubiques de $\mathbb{Q}$, à d'autres corps de nombres. L'outil principal qui nous permet cette généralisation est le théorème de Taniguchi [50], qui étend les bijections de Davenport-Heilbronn.

Le théorème de Taniguchi énumère les $\mathcal{O}$-algèbres cubiques au dessus d'un anneau de Dedekind arbitraire $\mathcal{O}$, mais l'appliquer concrètement pour obtenir un algorithme m'a obligée à faire un certain nombre de restrictions.

En ce moment, l'algorithme presenté ici marche seulement sur les corps de nombres quadratiques imaginaires avec nombre de classes 1, c'est à dire $\mathbb{Q}(\sqrt{-D})$, avec $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

Une généralisation à d'autres corps de nombres quadratiques imaginaires est sans doute possible, mais nécessite un travail additionel sur les actions de certains groupes de matrices sur l'espace hyperbolique 3-dimensionnel, donc on le laissera comme un problème ouvert. Pour les corps de nombres avec un nombre infini d'unités, le problème semble même plus difficile.

Le résultat principal de ce chapitre est le suivant.

**Théorème.** *Soit $K$ un corps de nombres quadratique imaginaire avec nombre de classes 1. Il existe un algorithme qui énumère toutes les extensions de $K$ jusqu'à une borne $X$ sur la norme du discriminant relatif. Cet algorithme marche en temps $O_\varepsilon(X^{1+\varepsilon})$, pour tout $\varepsilon > 0$.*

Notre algorithme utilise la théorie de la réduction des formes hermitiennes binaires sur l'anneau des entiers $\mathcal{O}_K$ de $K$. Comme le nombre de corps de nombres calculés est $\gg_K X$, notre algorithme est essentiellement linéaire dans la taille de la sortie.

Il est intéressant de comparer cet algorithme avec le classique, qui utilise la théorie des corps de classes de rayon. Ce dernier marche sur un corps de

base quelconque $K$; une borne pour le discriminant relatif d'une extension cubique $L/K$ donne une borne pour le discriminant du sous-corps quadratique $K_2/K$ de sa clôture galoisienne $L_2/K$, mais aussi une borne sur le conducteur de l'extension cyclique cubique $L_2/K_2$. L'algorithme parcourt tous les corps possibles $K_2$, et les conducteurs $\mathfrak{f} \subset \mathcal{O}_{K_2}$ et étudie les sous-groupes d'indice 3 dans les corps de classes de rayon $\mathrm{Cl}_{\mathfrak{f}}(K_2)$.

On a étudié et implementé cet algorithme classique, qui requiert en particulier le calcul du corps de classes de rayon de tous les corps $K_2$; sans supposer GRH, cela requiert un temps $(\mathrm{disc}\, K_2)^{1/2}$ pour chaque corps, ce qui est de l'ordre de $X^{1/2}$; et il y a, malheuresement, $\gg_K X$ de tels corps $K_2$, ce qui donne un algorithme de complexité $\Omega(X^{3/2})$. On souligne le fait que notre algorithme est presque-linéaire *inconditionellement*: pour un corps de nombres quadratique imaginaire $K$ de nombre de classes 1 donné, on énumère les équations qui définissent toutes les extensions cubiques de $K$ de discriminant borné sans avoir besoin de calculer des invariants arithmétiques pour d'autres corps de nombres que $K$.

# Introduction

## Motivation

Let $K$ be a number field, $G$ a transitive permutation group on $n$ letters. We define $\mathcal{F}_{K,n}(G)$ as the set of isomorphism classes of extensions $L/K$ of degree $n$ such that the Galois closure $N$ of $L/K$ has Galois group isomorphic to $G$.

This thesis studies the counting function

$$N_{K,n}(G,X) = |\{L \in \mathcal{F}_{K,n}(G), \mathcal{N}\mathfrak{d}(L/K) \leq X\}|,$$

enumerating the elements of $\mathcal{F}_{K,n}(G)$, ordered by relative discriminant. We will use two different, and somehow complementary, points of view.

### Asymptotics

On one side, we have the asymptotic point of view, as $X$ tends to infinity.This is quite a classical theme dating back to Gauss [35], who counted classes of binary quadratic forms of bounded discriminant. A number of important conjectures have been formulated recently on this subject, by Malle [43], Bhargava (see [3, §6.2]) and Ellenberg and Venkatesh [30]. Malle's conjecture is perhaps the most famous. It says that

$$N_{K,n}(G,X) \sim c(G,K)X^{a(G)}(\log X)^{b(G,K)-1},$$

with explicit constants, $a$ depending only on $G$ and $b$ and $c$ depending on $G$ and $K$.

This conjecture have been proved for abelian groups [42, 55], and for most extensions of degree $\leq 5$, at least over $\mathbb{Q}$. A number of landmark results have been obtained in particular by Cohn [21], Davenport-Heilbronn [26], Datskovsky-Wright [27], Cohen-Diaz y Diaz-Olivier [17, 18, 19], and Bhargava [5, 6, 7]. For an historical survey on this topic developments until 2005, see [16] and [3].

In 2005, J. Klüners [40] gave a counterexample to Malle's conjecture, relying on the presence of appropriate roots of unity in intermediate extensions. Türkelli [52] proposed a modification to Malle's conjecture which avoids this kind of counterexamples.

### Algorithmics

Our second point of view in counting number field extensions is algorithmic. In this area we can place the work by Belabas [1, 2] and many others (for a survey, see [44]). In this particular perspective, reduction theory and geometry of

numbers, as well as explicit bijections motivated by the classification of prehomogeneous vector spaces, become the main actors. If the latter ones are rather recent objects, reduction theory has a quite long story, dating back at least to Gauss's work on binary and ternary quadratic forms. After him, Bianchi [10], Julia [39] and others generalized this theory to other number fields, in particular imaginary quadratic ones. The whole 19th century was fascinated by the theory of invariants, a chapter closed by Hilbert's proof of the finite generation of the algebra of invariants [37]. After that, invariant theory was more and more abstracted, using group representations and Mumford's geometric invariant theory [46]. But classical invariant theory found new applications, and it got again very actual in more recent works by Elstrodt, Grunewald and Mennicke [31, 32, 33] (on their work about the hyperbolic 3-space), Cremona and Stoll [23, 25] (who were motivated by the study of elliptic and hyperelliptic curves) and finally in the work of Bhargava [5, 6, 7, 8, 9], which generalizes Gauss's composition law and finds amazing bijections parametrizing number fields of degree $\leq 5$, and parts of their ideal class groups.

## Thesis' Structure

This thesis is about both "ways" of counting number fields.

The first chapter is joint work with Henri Cohen; it proves a new asymptotic formula for cubic extensions with given quadratic resolvent (Theorem 1.6.2), refining Malle's conjecture.

The second chapter describes a new (essentially) linear-time algorithm to list all the cubic extensions of an imaginary quadratic number fields of class number 1, given a bound on the relative discriminant.

Appendix A sketches the proof of Taniguchi's extension of the Davenport-Heilbronn theory.

Appendix B describes the classical class field theory algorithm to enumerate cubic extensions of a given number field.

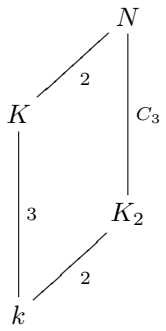
Appendix C studies the round-off errors in the floating point computations in our main algorithm.

Appendix D gives explicit polynomials needed to check rigorously the boundary conditions in our reduction theory for binary cubic forms over imaginary quadratic fields.

We now present in more detail our main results.

### Counting cubic extensions with given quadratic resolvent

Let us fix a number field $k$. We consider a cubic extension $K/k$ and we call $N$ the Galois closure of $K/k$. When $K/k$ is not cyclic we have $\mathrm{Gal}(N/k) \simeq S_3$, and the field $N$ contains a unique quadratic subextension $K_2/k$.




When $K/k$ is cyclic we have $N = K$ and $\mathrm{Gal}(N/k) \simeq C_3$. This case has already been treated in [18], but we include it for the sake of completeness by setting $K_2 = k$; by abuse of language we still call $K_2$ a quadratic extension of $k$, even though $[K_2 : k] = 1$.

We fix the quadratic extension $K_2/k$, and we call $\mathcal{F}(K_2)$ the set of cubic extensions $K/k$, up to $k$-isomorphism, such that the quadratic subextension of the Galois closure of $K/k$ is isomorphic to $K_2$.

We define

$$N(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{d}(K/k)) \leq X\}| \ .$$

where $\mathfrak{d}(K/k)$ is the relative discriminant ideal of $K/k$ and $\mathcal{N}_{k/\mathbb{Q}}$ denotes the absolute norm. Note that

$$N_{k,3}(S_3, X) = \sum_{K_2/k, K_2 \neq k} N(K_2/k, X), \quad \text{and} \quad N_{k,3}(C_3, X) = N(k/k, X),$$

so we are studying a refinement of Malle's conjecture. Our main theorem (Theorem 1.6.2) gives an asymptotic formula for $N(K_2/k, X)$; we state it here only for $k = \mathbb{Q}$. In this simple case, we will use the notation $N(K_2, X)$ instead of $N(K_2/\mathbb{Q}, X)$.

**Theorem.** *As above, let $K_2 = \mathbb{Q}(\sqrt{D})$ be an extension of $\mathbb{Q}$ with $[K_2 : \mathbb{Q}] \leq 2$, denote by $K_2' = \mathbb{Q}(\sqrt{-3D})$ the mirror field of $K_2$, and set $g(K_2') = 3$ if $K_2' = \mathbb{Q}(\sqrt{-3})$, and $g(K_2') = 1$ otherwise. Then:*

(1) *(Pure cubic fields.) We have*

$$N(\mathbb{Q}(\sqrt{-3}), X) = C(\mathbb{Q}(\sqrt{-3}))Y(\log(Y) + D(\mathbb{Q}(\sqrt{-3})) - 1) + O(Y^{2/3+\varepsilon}),$$

*for every $\varepsilon > 0$, where $Y = \sqrt{X/\mathfrak{d}(K_2/k)}$*

$$C(\mathbb{Q}(\sqrt{-3})) = \frac{7}{30} \prod_p \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right)$$

$$D(\mathbb{Q}(\sqrt{-3})) = 2\gamma - \frac{16}{35}\log(3) + 6\sum_p \frac{\log(p)}{p^2 + p - 2} \ ,$$

*and $\gamma$ is Euler's constant.*

(2) *(General case.) For $D \neq -3$, denote by $a_{K_2'}(p)$ the number of (unramified) degree 1 primes above $p$ in $K_2'$. Then*

$$N(\mathbb{Q}(\sqrt{D}), X) = C(\mathbb{Q}(\sqrt{D}))Y + O(Y^{2/3+\varepsilon}) ,$$

*where* $Y = \sqrt{X/\mathfrak{d}(K_2/k)}$

$$C(\mathbb{Q}(\sqrt{D})) = g(K_2')\frac{c_3(K_2')}{3^{3+r_2(K_2')}}\prod_{p\neq 3}\left(1+\frac{a_{K_2'}(p)}{p}\right)\left(1-\frac{1}{p}\right) ,$$

*and*

$$c_3(K_2') = \begin{cases} 11 & \text{if } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1^2 , \\ 15 & \text{if } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1 , \\ 21 & \text{if } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1\mathfrak{p}_2 . \end{cases}$$

Note that the formula in (2) is given because of its elegance, but it should *not* be used for practical computation of the constants; see Corollary 1.8.6 below.

## An algorithm for computing cubic extensions

The second chapter deals with the algorithmic point of view. The idea is to generalize Belabas's algorithm for listing cubic extensions of $\mathbb{Q}$ to other number fields. The main tool allowing us this generalization is Taniguchi's theorem [50], which generalizes Davenport-Heilbronn bijections.

Taniguchi's theorem enumerates cubic $\mathcal{O}$-algebras over an arbitrary Dedekind domain $\mathcal{O}$, but applying it concretely to obtain an algorithm obliged me to make a number of restrictions.

At this moment, the algorithm presented here works only over imaginary quadratic fields with class number 1, that is $\mathbb{Q}(\sqrt{-D})$, with $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

A generalization to other imaginary quadratic fields should be possible, but this needs some additional work on the actions of some groups of matrices on the hyperbolic 3-space, so we shall leave it as an open question. For number fields, with infinitely many units, the problem seems even more difficult.

Our main result in this chapter is the following.

**Theorem.** *Let $K$ be an imaginary quadratic number field with class number 1. There exists an algorithm which lists all cubic extensions of $K$ up to a bound $X$ on the norm of the relative discriminant ideal. This algorithm runs in time $O_\varepsilon(X^{1+\varepsilon})$, for all $\varepsilon > 0$.*

Our algorithm uses the reduction theory of binary Hermitian forms over the ring of integers $\mathcal{O}_K$ of $K$. Since the number of computed fields is $\gg_K X$, our algorithm is essentially linear in the output size.

It is interesting to compare this algorithm with the classical one, using class field theory. The latter works over an arbitrary base number field $K$; a bound for the relative discriminant of a cubic extension $L/K$ yields both a bound for the discriminant of the quadratic subfield $K_2/K$ of its Galois closure $L_2/K$, as well as on the conductor of the cyclic cubic extension $L_2/K_2$. The algorithm loops over all possible $K_2$, and conductors $\mathfrak{f} \subset \mathcal{O}_{K_2}$ and studies the index-3 subgroups in the ray class groups $\mathrm{Cl}_\mathfrak{f}(K_2)$.

We studied and implemented this classical algorithm, which requires in particular the computation of the class groups of all the fields $K_2$; without assuming the GRH, this already requires time $(\operatorname{disc} K_2)^{1/2}$ for a single field, which is of the order of $X^{1/2}$; and there are unfortunately $\gg_K X$ such fields $K_2$, yielding an $\Omega(X^{3/2})$ algorithm. We stress the fact that our algorithm is almost linear *unconditionally*: for a given imaginary quadratic number field $K$ of class number 1, we list defining equations for all cubic extensions of bounded discriminant of $K$ without needing to compute arithmetic invariants for number fields other than $K$.

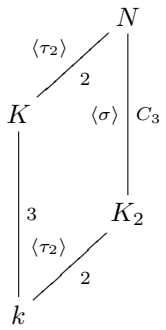
# Chapter 1

# Counting Cubic Extensions with given Quadratic Resolvent

This chapter is joint work with Henri Cohen [20].

## 1.1 Introduction

Let $k$ be a number field, fixed once and for all as our base field, let $K/k$ be a cubic extension of $k$, and let $N$ be a Galois closure of $K/k$. When $K/k$ is not cyclic we have $\mathrm{Gal}(N/k) \simeq S_3 \simeq D_3$, the dihedral group with 6 elements, and the field $N$ contains a unique quadratic subextension $K_2/k$, so the very simple field diagram is the following, denoting by $\tau_2$ the generator of $\mathrm{Gal}(K_2/k)$ and by $\sigma$ a generator of $\mathrm{Gal}(N/K_2)$:




The group relations are $\tau_2^2 = \sigma^3 = 1$ and $\tau_2\sigma\tau_2^{-1} = \sigma^{-1}$.

When $K/k$ is cyclic we have $N = K$ and $\mathrm{Gal}(N/k) \simeq C_3$. Although this case has already been treated in [18], since the methods are almost identical we include it in the present chapter by setting $K_2 = k$, which by abuse of language we will still call a quadratic extension of $k$, even though $[K_2 : k] = 1$.

We fix the quadratic extension $K_2/k$, and we call $\mathcal{F}(K_2)$ the set of cubic extensions $K/k$ (considered up to $k$-isomorphism) such that the quadratic

subextension of the Galois closure of $K/k$ is isomorphic to $K_2$. Our goal is to compute an asymptotic formula for

$$N(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{d}(K/k)) \le X\}| ,$$

where $\mathfrak{d}(K/k)$ is the relative ideal discriminant of $K/k$ and $\mathcal{N}$ denotes the absolute norm.

By a well-known theorem (see for example Theorem 9.2.6 of [12]), the conductor of the cyclic extension $N/K_2$ is of the form $\mathfrak{f}(N/K_2) = \mathfrak{f}(K/k)\mathbb{Z}_{K_2}$, where $\mathfrak{f}(K/k)$ is an ideal of the base field $k$ (when $K/k$ is noncyclic this is of course not a conductor in the usual sense). When $k = \mathbb{Q}$ we will write $f(K/\mathbb{Q})$ for the positive integer generating the ideal $\mathfrak{f}(K/\mathbb{Q})$ of $\mathbb{Z}$.

Since $\mathfrak{d}(K/k) = \mathfrak{d}(K_2/k)\mathfrak{f}(K/k)^2$, it is clear that

$$N(K_2/k, X) = M(K_2/k, (X/\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{d}(K_2/k)))^{1/2}) ,$$

where

$$\begin{aligned} M(K_2/k, X) &= |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{f}(K/k)) \le X\}| \\ &= |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{K_2/\mathbb{Q}}(\mathfrak{f}(N/K_2)) \le X^2\}| , \end{aligned}$$

so it is this quantity that we want to compute.

## 1.2 Galois Theory

**Definition 1.2.1.** *We denote by $\rho = \zeta_3$ a primitive cube root of unity and we set $L = K_2(\rho)$ and $k_z = k(\rho)$. We let $\tau$ be a generator of* $\mathrm{Gal}(L/K_2)$ *(so that $\tau = 1$ if $\rho \in K_2$), and we let $\tau_2$ be a generator of* $\mathrm{Gal}(K_2/k)$ *(so that $\tau_2 = 1$ if $K_2 = k$). We denote by $G = \mathrm{Gal}(L/k)$. Finally, as above we let $\sigma$ be one of the two generators of the cyclic group of order* 3 $\mathrm{Gal}(N/K_2) \simeq \mathrm{Gal}(N_z/L)$*, where $N_z = N(\rho)$.*

**Remarks**.

(1) By definition $K_2$ is the fixed field of $L$ by $\tau$, so that $\tau = 1$ if and only if $\tau(\rho) = \rho$. This is of course not true for $\tau_2$.

(2) We have the following relations:

$$\tau^2 = \tau_2^2 = 1 , \quad \tau\tau_2 = \tau_2\tau , \quad \tau\sigma = \sigma\tau .$$

It follows that when $\tau$ and $\tau_2$ are nontrivial we have $G \simeq V_4$, the Klein 4-group, and otherwise $G$ is either trivial or isomorphic to $C_2$.

We will need to distinguish five cases, according to the triviality or not of $\tau$ or $\tau_2$, and to their action on $\rho$. We will order them as follows, and this numbering will be kept throughout this chapter, so should be referred to.

(1) $\tau = \tau_2 = 1$: here $K/k$ is a cyclic cubic extension, in other words $K_2 = k$, $\mathrm{Gal}(N_z/k) \simeq C_3$, and $\rho \in k$.

(2) $\tau_2 = 1$ and $\tau(\rho) = \rho^{-1}$: here $K/k$ is a cyclic cubic extension, so that $K_2 = k$, $\mathrm{Gal}(N_z/k) \simeq C_6$, in other words $\tau\sigma = \sigma\tau$, and $\rho \notin k$ so $L = k(\rho)$.

(3) $\tau = 1$ and $\tau_2(\rho) = \rho$ but $\tau_2 \neq 1$: here $K/k$ is noncyclic, $\rho \in k$, and in particular $L = K_2$, and $\mathrm{Gal}(N_z/k) \simeq D_3$, in other words $\tau_2\sigma = \sigma^{-1}\tau_2$.

(4) $\tau = 1$ and $\tau_2(\rho) = \rho^{-1}$: here $L = K_2$, so that $\rho \in K_2$, but $\rho \notin k$, so $K_2 = k(\rho)$, and again $\mathrm{Gal}(N_z/k) \simeq D_3$, in other words $\tau_2\sigma = \sigma^{-1}\tau_2$.

(5) $\tau \neq 1$ and $\tau_2 \neq 1$: here $\rho \notin K_2$, so $\tau(\rho) = \rho^{-1}$ but $\tau_2(\rho) = \rho$, so that the fixed field of $L$ under $\tau_2$ is equal to $k_z = k(\rho)$, and $\mathrm{Gal}(N_z/k) \simeq D_3 \times C_2$, in other words $\tau\sigma = \sigma\tau$ and $\tau_2\sigma = \sigma^{-1}\tau_2$.

**Definition 1.2.2.** (1) *In cases (1) to (5) above, we set* $T = \emptyset$, $\{\tau + 1\}$, $\{\tau_2 + 1\}$, $\{\tau_2 - 1\}$, $\{\tau + 1, \tau_2 + 1\}$, *respectively, where* $T$ *is considered as a subset of the group ring* $\mathbb{Z}[\mathrm{Gal}(L/k)]$ *or of* $\mathbb{F}_3[\mathrm{Gal}(L/k)]$.

(2) *We define* $\iota(\tau \pm 1) = \tau \mp 1$ *and* $\iota(\tau_2 \pm 1) = \tau_2 \mp 1$.

(3) *For any group* $M$ *on which* $T$ *acts, we denote by* $M[T]$ *the subgroup of elements of* $M$ *annihilated by all the elements of* $T$.

We will need the following trivial lemma.

**Lemma 1.2.3.** *Let* $M$ *be an* $\mathbb{F}_3[G]$*-module. For any* $t \in T$ *we have* $M[t] = \iota(t)(M)$, *and conversely* $M[\iota(t)] = t(M)$.

*Proof.* It is clear that $t\iota(t) = \iota(t)t = 0$. Conversely, assume for instance that $x \in M[t]$, in other words that $t(x) = 1$. If $t = \tau + \varepsilon$ with $\varepsilon = \pm 1$ we thus have $\tau(x) = x^{-\varepsilon}$. But then since $\iota(t) = \tau - \varepsilon$, we have

$$\iota(t)(x^{\varepsilon}) = \tau(x^{\varepsilon})x^{-\varepsilon^2} = x^{-2\varepsilon^2} = x^{-2} = x \ ,$$

since $\varepsilon = \pm 1$ and since $x^3 = 1$, $M$ being an $\mathbb{F}_3$-vector space. Same for $\tau_2$. □

**Proposition 1.2.4.** (1) *There exists a bijection between on the one hand isomorphism classes of extensions* $K/k$ *having quadratic resolvent field isomorphic to* $K_2$, *and on the other hand classes of elements* $\overline{\alpha} \in (L^*/L^{*3})[T]$ *such that* $\overline{\alpha} \neq \overline{1}$ *modulo the equivalence relation identifying* $\overline{\alpha}$ *with its inverse.*

(2) *If* $\alpha \in L^*$ *is some representative of* $\overline{\alpha}$, *the extension* $K/k$ *corresponding to* $\alpha$ *is the fixed field under* $\mathrm{Gal}(L/k)$ *of the field* $N_z = L(\sqrt[3]{\alpha})$.

*Proof.* Since $\rho \in L$, by Kummer theory, cyclic cubic extensions $N_z$ of $L$ are of the form $N_z = L(\sqrt[3]{\alpha})$, where $\overline{\alpha} \neq \overline{1}$ is unique in $(L^*/L^{*3})$ modulo the equivalence relation identifying $\overline{\alpha}$ with its inverse. If $\theta^3 = \alpha$, then if necessary changing $\sigma$ into $\sigma^{-1}$ we may assume that $\sigma(\theta) = \rho\theta$. Consider first the relations involving $\tau$. Note that in all cases $\tau$ commutes with $\sigma$, and that it is nontrivial if and only if $\tau(\rho) = \rho^{-1}$ (cases (2) and (5)). Thus,

$$\sigma(\theta\tau(\theta)) = \rho\theta\tau(\sigma(\theta)) = \rho\theta\tau(\rho\theta) = \theta\tau(\theta) \ ,$$

so by Galois theory $\theta\tau(\theta) \in L$ (since it is trivially stable by $\tau$ it is in fact in $K_2$, but we do not need this), so $\alpha\tau(\alpha)$ is a cube, in other words $\alpha \in (L^*/L^{*3})[\tau+1]$.

Consider now the relations involving $\tau_2$. When it is nontrivial we have $\tau_2\sigma = \sigma^{-1}\tau_2$. Thus, if in addition $\tau_2(\rho) = \rho$ (cases (3) and (5)), a similar computation gives

$$\sigma(\theta\tau_2(\theta)) = \rho\theta\tau_2(\sigma^{-1}(\theta)) = \rho\theta\tau_2(\rho^{-1}\theta) = \theta\tau_2(\theta) \ ,$$

so $\alpha \in (L^*/L^{*3})[\tau_2 + 1]$. On the other hand, if $\tau_2(\rho) = \rho^{-1}$ (case (4)), we check in the same way that $\tau_2(\theta)/\theta$ is stable by $\sigma$ so here $\alpha \in (L^*/L^{*3})[\tau_2 - 1]$.

Conversely, assume that these conditions are satisfied. The group conditions on $\tau$ and $\tau_2$ are automatically satisfied, since they are so at the level of $G = \mathrm{Gal}(L/k)$ which is a trivial, $C_2$ or $V_4$ extension, and the group conditions on $\sigma$ are exactly those corresponding to the set $T$. It follows that $N_z/k$ is Galois with suitable Galois group. The uniqueness statement comes from the corresponding statement of Kummer theory, since $\alpha$ and $\alpha^{-1}$ give the same extension. □

Recall from [12] the following definition.

**Definition 1.2.5.** *We denote by $V_3(L)$ the group of* 3-virtual units *of $L$, in other words the group of $u \in L^*$ such that $u\mathbb{Z}_L = \mathfrak{q}^3$ for some ideal $\mathfrak{q}$ of $L$, or equivalently such that $3 \mid v_{\mathfrak{p}}(u)$ for any prime ideal $\mathfrak{p}$ of $L$. We define the* 3-Selmer group *$S_3(L)$ of $L$ by $S_3(L) = V_3(L)/L^{*3}$.*

Since we will only consider 3-virtual units and the 3-Selmer group, we will simply speak of virtual units and Selmer group. It is immediate that the Selmer group is finite: more precisely we have the following lemma.

**Lemma 1.2.6.** *We have a split exact sequence of $\mathbb{F}_3[G]$-modules*

$$1 \longrightarrow \frac{U(L)}{U^3(L)} \longrightarrow S_3(L) \longrightarrow Cl(L)[3] \longrightarrow 1 \ ,$$

*where the last nontrivial map sends $\overline{u}$ to the ideal class of $\mathfrak{q}$ such that $u\mathbb{Z}_L = \mathfrak{q}^3$.*

*Proof.* The exactness is immediate and left to the reader. Since it is also an exact sequence of $\mathbb{F}_3$-vector spaces and since $|G|$ divides 4 and is hence coprime to 3, it follows from a general theorem of commutative algebra that it is an exact sequence of $\mathbb{F}_3[G]$-modules. □

**Proposition 1.2.7.** (1) *There exists a bijection between isomorphism classes of cubic extensions $K/k$ with given quadratic resolvent field $K_2$ and equivalence classes of triples $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$ modulo the equivalence relation $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u}) \sim (\mathfrak{a}_1, \mathfrak{a}_0, 1/\overline{u})$, where $\mathfrak{a}_0$, $\mathfrak{a}_1$, and $\overline{u}$ are as follows:*

   *(a) The $\mathfrak{a}_i$ are coprime integral squarefree ideals of $L$ such that $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$ and $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$, where $I$ is the group of fractionals ideals of $L$.*

   *(b) $\overline{u} \in S_3(L)[T]$, and $\overline{u} \neq 1$ when $\mathfrak{a}_0 = \mathfrak{a}_1 = \mathbb{Z}_L$.*

(2) *If $(\mathfrak{a}_0, \mathfrak{a}_1)$ is a pair of ideals satisfying (a) there exist an ideal $\mathfrak{q}_0$ and an element $\alpha_0$ of $L$ such that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$ with $\alpha_0 \in (L^*/L^{*3})[T]$. The cubic extensions $K/k$ corresponding to such a pair $(\mathfrak{a}_0, \mathfrak{a}_1)$ are given as follows: for any $\overline{u} \in S_3(L)[T]$ the extension is the cubic subextension of $N_z = L(\sqrt[3]{\alpha_0 u})$ (for any lift $u$ of $\overline{u}$).*

*Proof.* Let $N_z = L(\sqrt[3]{\alpha})$ as above. We can write uniquely $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$ where the $\mathfrak{a}_i$ are coprime squarefree ideals of $L$. Since $\alpha \in (L^*/L^{*3})[T]$, we clearly have $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$. On the other hand the class of $\mathfrak{a}_0\mathfrak{a}_1^2$ is equal to that of $\mathfrak{q}^{-3}$ so $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$. Now let $\mathfrak{a}_0, \mathfrak{a}_1$ be given satisfying these properties. There exists an ideal $\mathfrak{q}$ (whose class is not necessary in the kernel of $T$) and an element $\alpha \in L$ such that $(\mathfrak{a}_0\mathfrak{a}_1^2)\mathfrak{q}^3 = \alpha\mathbb{Z}_L$. Applying any $t \in T$, we deduce from the assumption on $\mathfrak{a}_0\mathfrak{a}_1^2$ that $\mathfrak{q}_1^3 = t(\alpha)\mathbb{Z}_L$ for some ideal $\mathfrak{q}_1$, so that $t(\alpha)$ is a virtual unit, in other words that the class of $t(\alpha)$ is in $S_3(L)$. Since $t \circ \iota(t) = 0$, we have $t(\alpha) \in S_3(L)[\iota(t)]$, so by Lemma 1.2.3 we deduce that $t(\alpha) \in t(S_3(L))$, in other words that $t(\alpha) = \gamma^3 t(u)$, or equivalently $t(\alpha/u) = \gamma^3$, for some virtual unit $u$ and some element $\gamma$. Thus, if we set $\alpha_0 = \alpha/u$, we have $\alpha_0 \in (L^*/L^{*3})[t]$, and if $u\mathbb{Z}_L = \mathfrak{q}_2^3$ we have $\mathfrak{a}_0\mathfrak{a}_1^2(\mathfrak{q}/\mathfrak{q}_2)^3 = \alpha_0\mathbb{Z}_L$. We have thus shown that, given $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$, the condition that $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$ is necessary and sufficient for the existence of $\mathfrak{q}_0$ and $\alpha_0$ such that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$ with $\alpha_0 \in (L^*/L^{*3})[T]$.

The rest of the proof is immediate: if $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$ with $\alpha_0 \in (L^*/L^{*3})[T]$, then $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3 = \alpha\mathbb{Z}_L$ with the same property for $\alpha$ if and only if $\alpha/\alpha_0 = (\mathfrak{q}/\mathfrak{q}_0)^3 \in V_3(L)[T]$, so $\alpha = \alpha_0 u$ for some lift $u$ of $\overline{u} \in S_3(L)[T]$. Finally $\alpha$ and $\beta$ give equivalent extensions if and only if either $\beta = \alpha\gamma^3$, which does not change the $\mathfrak{a}_i$ and changes $u$ into $u\gamma^3$ so does not change $\overline{u}$, or if $\beta = \alpha^{-1}\gamma^3$. In this case

$$\beta\mathbb{Z}_L = \mathfrak{a}_0^{-1}\mathfrak{a}_1^{-2}\mathfrak{q}^{-3}\gamma^3 = \mathfrak{a}_1\mathfrak{a}_0^2(\gamma\mathfrak{a}_0^{-1}\mathfrak{a}_1^{-1}\mathfrak{q}^{-1})^3 \ ,$$

which interchanges $\mathfrak{a}_0$ and $\mathfrak{a}_1$, and since $\alpha$ is replaced by $\alpha^{-1}$, it changes $\overline{u}$ into $1/\overline{u}$, finishing the proof. Note that the only fixed point of this involution on triples is obtained for $\mathfrak{a}_0 = \mathfrak{a}_1$ and $\overline{u^2} = 1$, but since $\mathfrak{a}_0$ and $\mathfrak{a}_1$ are coprime this means that $\mathfrak{a}_0 = \mathfrak{a}_1 = \mathbb{Z}_L$, and $\overline{u} = \overline{u^3}/\overline{u^2} = 1$. □

**Lemma 1.2.8.** (1) *The condition $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$ is equivalent to $\mathfrak{a}_1 = \tau(\mathfrak{a}_0)$, $\mathfrak{a}_1 = \tau_2(\mathfrak{a}_0)$, $\mathfrak{a}_0 = \tau_2(\mathfrak{a}_0)$ and $\mathfrak{a}_1 = \tau_2(\mathfrak{a}_1)$, and $\mathfrak{a}_1 = \tau(\mathfrak{a}_0) = \tau_2(\mathfrak{a}_0)$ in cases (2), (3), (4), and (5), respectively.*

(2) *The ideal $\mathfrak{a}_0\mathfrak{a}_1$ of $L$ comes from an ideal $\mathfrak{a}_\alpha$ of $K_2$ (in other words $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$), and in cases (1), (2), and (3) it comes from an ideal of $k$, while in cases (4) and (5), $\mathfrak{a}_\alpha$ is an ideal of $K_2$ invariant by $\tau_2$.*

*Proof.* In case (4), we have $\tau_2(\mathfrak{a}_0)\tau_2(\mathfrak{a}_1)^2 = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$ for some ideal $\mathfrak{q}$. By uniqueness of the decomposition, it follows that $\mathfrak{a}_0$ and $\mathfrak{a}_1$ are stable by $\tau_2$ (and $\mathfrak{q} = \mathbb{Z}_L$), as claimed. In particular $\mathfrak{a}_0\mathfrak{a}_1$ is also stable by $\tau_2$, and by $\tau = 1$. In case (3), we have

$$\tau_2(\mathfrak{a}_0)\tau_2(\mathfrak{a}_1)^2 = \mathfrak{a}_0^{-1}\mathfrak{a}_1^{-2}\mathfrak{q}^3 = \mathfrak{a}_1\mathfrak{a}_0^2(\mathfrak{q}/\mathfrak{a}_0\mathfrak{a}_1)^3 \ ,$$

and again by uniqueness of this decomposition we deduce that $\mathfrak{a}_0$ and $\mathfrak{a}_1$ are exchanged by $\tau_2$, as claimed. In particular $\mathfrak{a}_0\mathfrak{a}_1$ (which is an ideal of $L = K_2$) is not only stable by $\tau_2$ but comes in fact from an ideal of $k$. The other cases follow similarly. □

Note that in case (4) where $L = K_2 = k(\rho)$, an ideal of $k$ is invariant by $\tau_2$, but conversely $\mathfrak{a}_0\mathfrak{a}_1$ is an ideal of $L$ invariant by $\tau_2$ if and only if it is equal to a product $\mathfrak{a}\mathfrak{r}$, where $\mathfrak{a}$ comes from an ideal of $k$, and $\mathfrak{r}$ is a product of distinct prime ideals $\mathfrak{p}$ of $L$ coprime to $\mathfrak{a}$ and above a ramified prime $p$ in $L/k$ (in particular above 3).

In case (5), which is the only case where $G = \mathrm{Gal}(L/k) \simeq V_4$, we define $K_2'$ to be the quadratic subextension of $L/k$ different from $K_2$ and $k_z$. For later use, we are interested in describing the prime ideals $p$ of $k$, $p\mathbb{Z}_{K_2} \mid \mathfrak{a}_\alpha$. For this, we set the following definition.

**Definition 1.2.9.** *We define $\mathcal{D}$ (resp., $\mathcal{D}_3$) to be the set of all prime ideals $p$ in $k$ with $p \nmid 3\mathbb{Z}_k$ (resp., with $p \mid 3\mathbb{Z}_k$), such that:*

- *no other conditions in cases (1) and (4);*
- *$p$ is split in $L/k$ in case (2) and (3);*
- *the ideals above $p$ are split in $L/K_2$ and $L/k_z$ in case (5).*

**Proposition 1.2.10.** (1) *Let $\mathfrak{p}$ be a prime ideal of $K_2$ dividing $\mathfrak{a}_\alpha$ and let $p$ be the prime ideal of $k$ below $\mathfrak{p}$. Then $p \in \mathcal{D}$ or $p \in \mathcal{D}_3$.*

(2) *In cases (2) and (3), set $K_2' = L$. Then in cases (2), (3), and (5) we have $p \in \mathcal{D}$ or $p \in \mathcal{D}_3$ if and only $p$ is split in $K_2'/k$.*

*Proof.* (1). Let us treat case (2). Let $\mathfrak{p}_z$ be an ideal of $L$ above $\mathfrak{p}$. Thus $\mathfrak{p}_z$ divides one of the $\mathfrak{a}_i$, so $\tau(\mathfrak{p}_z)$ divides $\tau(\mathfrak{a}_i) = \mathfrak{a}_j$ with $j \neq i$. Since the $\mathfrak{a}_i$ are coprime, we conclude that $\tau(\mathfrak{p}_z)$ is coprime to $\mathfrak{p}_z$, so $p$ is split. Cases (3) and (5) are proved in the same way.

(2). Since cases (2) and (3) repeat the definition, assume we are in case (5), let $\mathfrak{p}_z$ be an ideal of $L$ above $p$, let $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ be the ideals below $\mathfrak{p}_z$ in $k_z$, $K_2$, and $K_2'$ respectively, and denote as usual by $D()$ the decomposition groups. Now $\mathfrak{p}_z/\mathfrak{p}_2$ is split if and only if $D(\mathfrak{p}_z/\mathfrak{p}_2) = 1$, and since $D(\mathfrak{p}_z/\mathfrak{p}_2) = D(\mathfrak{p}_z/p) \cap \mathrm{Gal}(L/K_2)$, this is if and only if $\tau \notin D(\mathfrak{p}_z/p)$. Similarly, $\mathfrak{p}_z/\mathfrak{p}_1$ is split if and only if $\tau_2 \notin D(\mathfrak{p}_z/p)$. Since $\mathrm{Gal}(L/k) = \{1, \tau, \tau_2, \tau\tau_2\}$, it follows that the ideals above $p$ are split in $L/K_2$ and $L/k_z$ if and only if $D(\mathfrak{p}_z/p) \subset \{1, \tau\tau_2\}$. On the other hand, $p$ is split in $K_2'/k$ if and only if $D(\mathfrak{p}_3/p) = 1$, and since $D(\mathfrak{p}_3/p) \simeq D(\mathfrak{p}_z/p)/D(\mathfrak{p}_z/\mathfrak{p}_3)$, this is the case if and only if $D(\mathfrak{p}_z/p) = D(\mathfrak{p}_z/\mathfrak{p}_3)$, and again since $D(\mathfrak{p}_z/\mathfrak{p}_3) = D(\mathfrak{p}_z/p) \cap \mathrm{Gal}(L/K_2')$, if and only if $D(\mathfrak{p}_z/p) \subset \mathrm{Gal}(L/K_2') = \{1, \tau\tau_2\}$, proving the result. □

## 1.3 Conductors

The discriminant (equivalently, the conductor) of a cyclic Kummer extension is given by an important theorem of Hecke (see [12], Section 10.2.9). We will mainly need it in the cubic case, but we also need it in the quadratic case, where it takes an especially nice form:

**Theorem 1.3.1.** *Let $k$ be a number field, let $K_2 = k(\sqrt{D})$ be a quadratic extension with $D \in k^* \setminus k^{*2}$, and write uniquely $D\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$, where $\mathfrak{a}$ is an integral squarefree ideal. Then*

$$\mathfrak{d}(K_2/k) = \mathfrak{f}(K_2/k) = 4\mathfrak{a}/\mathfrak{c}^2 ,$$

*where $\mathfrak{c}$ is the largest ideal (for divisibility) dividing $2\mathbb{Z}_k$ and coprime to $\mathfrak{a}$ such that the congruence $x^2/D \equiv 1 \pmod{{}^*\mathfrak{c}^2}$ has a solution.*

**Corollary 1.3.2.** *Let $K$ be a number field such that $\rho \notin k$, where $\rho = \zeta_3$ is a primitive cube root of unity, and set $K_z = K(\rho)$. Then*

$$\mathfrak{d}(K_z/K) = \prod_{\substack{\mathfrak{p}|3\mathbb{Z}_K \\ e(\mathfrak{p}/3)\ odd}} \mathfrak{p}\ .$$

*In particular, the ramified primes in $K_z/K$ are those above 3 such that $e(\mathfrak{p}/3)$ is odd.*

*Proof.* We have $K_z = K(\sqrt{-3})$, so we use the theorem with $D = -3$. We have $D\mathbb{Z}_K = 3\mathbb{Z}_K = \mathfrak{a}\mathfrak{q}^2$ with

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p}|3\mathbb{Z}_K \\ e(\mathfrak{p}/3)\ \text{odd}}} \mathfrak{p}\ .$$

On the other hand $\mathfrak{a}$ is coprime to 2 and the congruence $x^2 \equiv -3 \pmod 4$ has the solution $x = 1$, so $\mathfrak{c} = 2\mathbb{Z}_K$ and the corollary follows. □

If $\mathfrak{p}$ is a prime ideal of $K_2$, we will denote by $\mathfrak{p}_z$ any prime ideal of $L$ above $\mathfrak{p}$. By the above corollary, we have $e(\mathfrak{p}_z/\mathfrak{p}) = 2$ if and only if $L \neq K_2$ and $e(\mathfrak{p}/3)$ is odd, otherwise $e(\mathfrak{p}_z/\mathfrak{p}) = 1$.

In the case of cyclic cubic extensions, the result is more complicated, especially when $L \neq K_2$. We first need some definitions.

**Definition 1.3.3.** *Let $p$ be a prime ideal of $k$, $\mathfrak{p}$ a prime ideal of $K_2$ above $p$, $\mathfrak{p}_z$ a prime ideal of $L$ above $\mathfrak{p}$. To simplify notation:*

- *We set $p^{1/2} = \mathfrak{p}$ if $p$ is ramified in $K_2/k$ (i.e., $p\mathbb{Z}_{K_2} = \mathfrak{p}^2$), and similarly $\mathfrak{p}^{1/2} = \mathfrak{p}_z$ if $\mathfrak{p}$ is ramified in $L/K_2$ (i.e., $\mathfrak{p}\mathbb{Z}_L = \mathfrak{p}_z^2$).*
- *We set $r = r(\mathfrak{p}/p) = 1/e(\mathfrak{p}/p)$*
- *We say that $p \subset k$ divides some ideal $\mathfrak{b}$ of $K_2$ (resp., of $L$) when $(p\mathbb{Z}_{K_2})^r$ (resp., $(p\mathbb{Z}_L)^{1/e(\mathfrak{p}_z/p)}$) does.*

Note that $e(\mathfrak{p}_z/p) \leq 2$ (indeed, if for instance $e(\mathfrak{p}/p) = 2$ then $e(\mathfrak{p}/3)$ is even so $\mathfrak{p}_z/\mathfrak{p}$ is unramified by Corollary 1.3.2), so we will never need to define "$p^{1/4}$".

**Definition 1.3.4.** *Let $\overline{\alpha} \in (L^*/L^{*3})[T]$ as above, let $p$ be an ideal of $k$ above 3, let $\mathfrak{p}$ be an ideal of $K_2$ above $p$, let $\mathfrak{p}_z$ be an ideal of $L$ above $\mathfrak{p}$, and denote by $C_n$ the congruence $x^3/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}_z^n}$ in $L$. If this congruence is soluble for $n = 3e(\mathfrak{p}_z/3)/2$ we set $A_\alpha(p) = 3e(\mathfrak{p}_z/3)/2 + 1$. Otherwise, if $n < 3e(\mathfrak{p}_z/3)/2$ is the largest exponent for which it has a solution, we set $A_\alpha(p) = n$. In both cases we set*

$$a_\alpha(p) = \frac{A_\alpha(p) - 1}{e(\mathfrak{p}_z/p)}\ .$$

It is clear that $A_\alpha(p)$ and $a_\alpha(p)$ do not depend on the ideal $\mathfrak{p}_z$ above $p$, whence the notation.

In addition, we have the following properties:

**Proposition 1.3.5.** (1) *We have* $3 \nmid A_\alpha(p)$*, and in addition when* $e(\mathfrak{p}_z/\mathfrak{p}) = 2$ *and* $A_\alpha(p) < 3e(\mathfrak{p}_z/3)/2 + 1$ *we also have* $2 \nmid A_\alpha(p)$*.*

(2) *We have* $0 \le a_\alpha(p) < 3e(p/3)/2 - 1/e(\mathfrak{p}/p)$ *and* $a_\alpha(p)e(\mathfrak{p}/p) \in \mathbb{Z}$*, or* $a_\alpha(p) = 3e(p/3)/2$*, which happens if and only if* $A_\alpha(p) = 3e(\mathfrak{p}_z/3)/2 + 1$*, in which case it is only a half integer when* $e(\mathfrak{p}_z/\mathfrak{p}) = 2$*.*

(3) *We have* $a_\alpha(p) \not\equiv -e(\mathfrak{p}_z/p) \pmod 3$*.*

**Theorem 1.3.6.** *Let* $N$ *correspond to* $\alpha$ *as above, write uniquely* $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$ *with* $\mathfrak{a}_0$ *and* $\mathfrak{a}_1$ *integral coprime squarefree ideals, and let* $\mathfrak{a}_\alpha$ *be the ideal of* $K_2$ *such that* $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$ *(see Lemma 1.2.8). Then*

$$\mathfrak{f}(N/K_2) = \frac{3\mathfrak{a}_\alpha \prod_{p|3\mathbb{Z}_k} (p\mathbb{Z}_{K_2})^{e(p/3)/2} \prod_{\substack{p|3\mathbb{Z}_k \\ e(\mathfrak{p}/3)\ odd}} (p\mathbb{Z}_{K_2})^{1/2}}{\prod_{\substack{p|3\mathbb{Z}_k \\ p\nmid\mathfrak{a}_\alpha}} (p\mathbb{Z}_{K_2})^{\lceil a_\alpha(p)e(\mathfrak{p}/p)\rceil/e(\mathfrak{p}/p)}} .$$

All these results come from similar results in [18] where we have just replaced $a_\alpha(\mathfrak{p})$ by $a_\alpha(p) = a_\alpha(\mathfrak{p})/e(\mathfrak{p}/p)$.

Note that $\lceil ae(\mathfrak{p}/p)\rceil/e(\mathfrak{p}/p)$ is equal to $a$ when $e(\mathfrak{p}/p) = 2$ (recall that in that case $a$ can be a half integer) and equal to $\lceil a\rceil$ otherwise (in particular when $e(\mathfrak{p}_z/\mathfrak{p}) = 2$).

**Definition 1.3.7.** *Let* $p$ *be an ideal of* $k$*, let* $\mathfrak{p}$ *be an ideal of* $K_2$ *above* $p$*, and let* $\mathfrak{p}_z$ *be an ideal of* $L$ *above* $\mathfrak{p}$*. Let* $a$ *be such that* $0 \le a < 3e(p/3)/2 - 1/e(\mathfrak{p}/p)$ *and* $ae(\mathfrak{p}/p) \in \mathbb{Z}$*, or* $a = 3e(p/3)/2$*. For* $\varepsilon = 0$ *or* $1$ *we define* $h(\varepsilon, a, p)$ *as follows:*

(1) *when* $a = 3e(p/3)/2$ *we set* $h(0, a, p) = 0$*;*

(2) *when* $a < 3e(p/3)/2$ *we set*

$$h(0, a, p) = \begin{cases} 1 & \text{if } e(\mathfrak{p}_z/p) = 1, \\ 1/2 & \text{if } e(\mathfrak{p}/p) = 2 \text{ (hence } e(\mathfrak{p}_z/\mathfrak{p}) = 1), \\ 0 & \text{if } e(\mathfrak{p}_z/\mathfrak{p}) = 2 \text{ (hence } e(\mathfrak{p}/p) = 1); \end{cases}$$

(3) *we set* $h(1, a, p) = 2/e(\mathfrak{p}_z/p)$*.*

**Lemma 1.3.8.** *Let* $b = a + h(\varepsilon, a, p)$*.*

(1) *Assume that* $b \le 3e(p/3)/2$*. Then* $h(\varepsilon, b, p) = h(\varepsilon, a, p)$*, so that* $a = b - h(\varepsilon, b, p)$*.*

(2) *We have* $b = 0$ *if and only if* $a = 0$*,* $\varepsilon = 0$*, and* $e(\mathfrak{p}_z/\mathfrak{p}) = 2$*. In particular, if* $e(\mathfrak{p}_z/\mathfrak{p}) = 1$ *we have* $b > 0$*.*

*Proof.* (1). If $h(\varepsilon, a, p) = 0$ we have $b = a$, and $h(1, a, p)$ only depends on the value of $e(\mathfrak{p}_z/p)$ (and the fact that $a \le 3e(p/3)/2$), so the result is trivial in both cases. We may therefore assume that $\varepsilon = 0$ and that $h(0, a, p) > 0$, so that $a < 3e(p/3)/2$ and $e(\mathfrak{p}_z/p) = 1$ or $e(\mathfrak{p}/p) = 2$, hence by definition $h(0, a, p) = 1/e(\mathfrak{p}/p)$. Since by assumption $a < 3e(p/3)/2 - 1/e(\mathfrak{p}/p)$ it follows that $b < 3e(p/3)/2$, so $h(\varepsilon, b, p) = h(\varepsilon, a, p)$ as claimed.

(2). Evidently $b = 0$ if and only if $a = 0$ and $h(\varepsilon, a, p) = 0$, hence $h(\varepsilon, 0, p) = 0$. Since $0 < 3e(p/3)/2$, by definition this is the case if and only if $\varepsilon = 0$ and $e(\mathfrak{p}_z/\mathfrak{p}) = 2$. □

**Lemma 1.3.9.** *Let $p$ be a prime ideal of $k$ and denote by $D_k$ the congruence $x^3/\alpha \equiv 1 \pmod{{}^*p^k}$ in $L$. If $a$ is as in the above definition, then $a_\alpha(p) = a$ if and only if $D_k$ is soluble for $k = a + h(0,a,p)$ and not soluble for $k = a + h(1,a,p)$, where this last condition is ignored if $a + h(1,a,p) > 3e(p/3)/2$.*

*Proof.* Since $\alpha \in (L^*/L^{*3})[T]$ it is clear that the solubility of the congruence $C_k$ for $\mathfrak{p}_z^k$ is equivalent to that for $\tau(\mathfrak{p}_z)^k$ or $\tau_2(\mathfrak{p}_z)^k$ in all cases. Thus the solubility of $D_k$ is equivalent to that of $C_k$ when $e(\mathfrak{p}_z/p) = 1$, and to that of $C_{2k}$ when $e(\mathfrak{p}_z/p) = 2$.

Assume first that $a = a_\alpha(p) = 3e(p/3)/2$. By definition, this is equivalent to the solubility of the congruence $C_k$ for $k = 3e(\mathfrak{p}_z/3)/2 = 3e(p/3)e(\mathfrak{p}_z/p)/2$, hence to that of $D_{3e(p/3)/2} = D_a$ whether $e(\mathfrak{p}_z/p) = 1$ or 2, proving the result since $h(0,a,p) = 0$ in this case.

Assume now that $a < 3e(p/3)/2$ and that $e(\mathfrak{p}_z/p) = 1$, so the solubility of $D_k$ is equivalent to that of $C_k$. In this case $A_\alpha(p) = a_\alpha(p) + 1$, so $a_\alpha(\mathfrak{p}) = a$ is equivalent to the solubility of $D_{a+1}$ and the nonsolubility of $D_{a+2}$, proving the result since $h(0,a,p) = 1$ and $h(1,a,p) = 2$.

Assume that $a < 3e(p/3)/2$ and that $e(\mathfrak{p}_z/\mathfrak{p}) = 2$. The congruence $D_k$ is now the same as the congruence $C_{2k}$. By Proposition 1.3.5 we have $A_\alpha(\mathfrak{p}_z) = 2a_\alpha(p) + 1 < 3e(\mathfrak{p}_z/3)/2$, with $a_\alpha(p) \in \mathbb{Z}$, which means that the maximal $m$ for which $C_m$ is soluble is *odd*. Thus $a_\alpha(\mathfrak{p}) = a$ means that $C_{2a+1}$ is soluble and $C_{2a+2}$ is not, so equivalently that $D_a = C_{2a}$ is soluble and $D_{a+1} = C_{2a+2}$ is not, so $h(0,a,p) = 0$ and $h(1,a,p) = 1$.

Finally assume that $a < 3e(p/3)/2$ and that $e(\mathfrak{p}/p) = 2$. The congruence $D_k$ is equivalent to the congruence $C_{2k}$. Since $a_\alpha(p)$ can be a half integer, the choice $h(0,a,p) = 1/2$ and $h(1,a,p) = 1$ that we have made finishes the proof. □

**Remark**. We have used in an essential way the fact that $A_\alpha(p)$ is odd when $e(\mathfrak{p}_z/\mathfrak{p}) = 2$ and $A_\alpha(p) \le 3e(\mathfrak{p}_z/3)/2$. Note that this result is rather subtle, and follows from the study of higher ramification groups. On the other hand, it is not necessary to use the fact that $3 \nmid A_\alpha(p)$, contrary to what was done in [18]. The resulting formulas, which are of course equivalent, are simpler.

## 1.4 The Dirichlet Series

Recall that $\mathfrak{f}(N/K_2) = \mathfrak{f}(K/k)\mathbb{Z}_{K_2}$ for some ideal $\mathfrak{f}(K/k)$ of $k$, and that this result also comes from the computation of higher ramification groups. In particular, $\mathcal{N}_{K_2/\mathbb{Q}}(\mathfrak{f}(N/K_2)) = \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{f}(K/k))^{[K_2:k]}$. To avoid having both the norm from $K_2/\mathbb{Q}$ and from $k/\mathbb{Q}$, and to emphasize the fact that we are mainly interested in the latter, we set explicitly the following definition:

**Definition 1.4.1.** *If $\mathfrak{a}$ is an ideal of $k$, we set $\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{a})$, while if $\mathfrak{a}$ is an ideal of $K_2$, we set*

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{K_2/\mathbb{Q}}(\mathfrak{a})^{1/[K_2:k]} .$$

This practical abuse of notation cannot create any problems since if $\mathfrak{a}$ is an ideal of $k$ we have $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{a}\mathbb{Z}_{K_2})$. For instance, since $\mathfrak{f}(N/K_2) = \mathfrak{f}(K/k)\mathbb{Z}_{K_2}$, we have $\mathcal{N}(\mathfrak{f}(K/k)) = \mathcal{N}(\mathfrak{f}(N/K_2))$. We emphasize that unless explicitly written otherwise, from now on we will only use the above notation.

**Definition 1.4.2.** *The fundamental Dirichlet series is defined by*

$$\Phi(s) = \frac{1}{2} + \sum_{K \in \mathcal{F}(K_2)} \frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s} ,$$

*where $\mathcal{N}$ is as in the preceding definition.*

By the fundamental bijection (Proposition 1.2.7), we have

$$\Phi(s) = \frac{1}{2} \sum_{(\mathfrak{a}_0,\mathfrak{a}_1) \in J} \sum_{\overline{u} \in S_3(L)[T]} \frac{1}{\mathcal{N}(\mathfrak{f}(N/K_2))^s} ,$$

where $J$ is the set of pairs $(\mathfrak{a}_0, \mathfrak{a}_1)$ of coprime integral squarefree ideals of $L$ such that $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$ and $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$, and where $\mathfrak{f}(N/K_2)$ is the conductor of the extension $N/K_2$ corresponding to the triple $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$.

Indeed, the addition of $1/2$ in the definition of $\Phi$ corresponds to the excluded triple $(\mathbb{Z}_L, \mathbb{Z}_L, \overline{1})$, and the factor $1/2$ in the above formula corresponds to the equivalence relation between triples.

Thus, replacing $\mathfrak{f}(N/K_2)$ by the formula given by Theorem 1.3.6 we obtain

$$\Phi(s) = \frac{1}{2 \cdot 3^{(3/2)[k:\mathbb{Q}]s} \prod_{\substack{\mathfrak{p} \mid 3\mathbb{Z}_k, \\ e(\mathfrak{p}/3) \text{ odd}}} \mathcal{N}(p)^{s/2}} \sum_{(\mathfrak{a}_0,\mathfrak{a}_1) \in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s}, \quad \text{where}$$

$$S_{\alpha_0}(s) = \sum_{\overline{u} \in S_3(L)[T]} \prod_{\substack{\mathfrak{p} \mid 3\mathbb{Z}_k \\ \mathfrak{p} \nmid \mathfrak{a}_\alpha}} \mathcal{N}(p)^{\lceil a_{\alpha_0 u}(p) e(\mathfrak{p}/p) \rceil s / e(\mathfrak{p}/p)} ,$$

and where $\alpha_0$ is any element of $L$ such that there exists an ideal $\mathfrak{q}_0$ such that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$ and $\alpha_0 \in (L^*/L^{*3})[T]$. Note that it is possible to require this additional property thanks to Proposition 1.2.7.

**Definition 1.4.3.** *For $\alpha_0 \in L^*$ and $\mathfrak{b}$ an ideal of $L$ we introduce the function*

$$f_{\alpha_0}(\mathfrak{b}) = \left| \{ \overline{u} \in S_3(L)[T],\ x^3/(\alpha_0 u) \equiv 1 \pmod{^*\mathfrak{b}} \quad \textit{soluble in } L \} \right| ,$$

*with the convention that $f_{\alpha_0}(\mathfrak{b}) = 0$ if $\mathfrak{b} \nmid 3\sqrt{-3}$.*

Let $p_i$ for $1 \le i \le g$ be the prime ideals of $k$ above 3 and not dividing $\mathfrak{a}_\alpha$ (in the sense of Definition 1.3.3), set $e_i = e(p_i/3)$, and for each $i$ let $a_i$ be such that $0 \le a_i < 3e_i/2 - 1/e(\mathfrak{p}_i/p_i)$ with $a_i e(\mathfrak{p}_i/p_i) \in \mathbb{Z}$ (where as usual $\mathfrak{p}_i$ is an ideal of $K_2$ above $p_i$), or $a_i = 3e_i/2$. Note that since $p_i$ is above 3 we have $e_i = e(p_i/3) \ge 1$.

Thanks to Lemma 1.3.9, an easy inclusion-exclusion argument shows that

$$\sum_{\substack{\overline{u} \in S_3(L)[T] \\ \forall i,\ a_{\alpha_0 u}(\mathfrak{p}_i) = a_i}} 1 = \sum_{(\varepsilon_1,\dots,\varepsilon_g) \in \{0,1\}^g} (-1)^{\sum_i \varepsilon_i} f_{\alpha_0} \left( \prod_{1 \le i \le g} (p_i \mathbb{Z}_{K_2})^{b_i} \right) ,$$

where $b_i = a_i + h(\varepsilon_i, a_i, p_i)$, and since we have set $f_{\alpha_0}(\mathfrak{b}) = 0$ when $\mathfrak{b} \nmid 3\sqrt{-3}\mathbb{Z}_L$, we may assume that $0 \le b_i \le 3e_i/2$. Note also that $e(\mathfrak{p}_i/p_i)b_i \in \mathbb{Z} \cup \{3e(\mathfrak{p}_i/3)/2\}$.

From Lemma 1.3.8 it follows that if we let $B$ be the set of $g$-uples $(b_1,\dots,b_g)$ such that $0 \le b_i \le 3e_i/2$, $b_i e(\mathfrak{p}_i/p_i) \in \mathbb{Z} \cup \{3e(\mathfrak{p}_i/3)/2\}$, then we have

$$S_{\alpha_0}(s) = \sum_{\substack{(b_1,\dots,b_g)\in B\\(\varepsilon_1,\dots,\varepsilon_g)\in\{0,1\}^g}} \prod_{1\le i\le g} \mathcal{N}(p_i)^{\lceil (b_i - h(\varepsilon_i,b_i,e_i))e(\mathfrak{p}_i/p_i)\rceil s/e(\mathfrak{p}_i/p_i)} (-1)^{\sum_i \varepsilon_i} f_{\alpha_0}\left(\prod_i (p_i\mathbb{Z}_{K_2})^{b_i}\right) .$$

**Lemma 1.4.4.** *We have*

$$S_{\alpha_0}(s) = \sum_{(b_1,\dots,b_g)\in B} f_{\alpha_0}\left(\prod_{1\le i\le g}(p_i\mathbb{Z}_{K_2})^{b_i}\right) \prod_{1\le i\le g}\left(\mathcal{N}(p_i)^{\lceil b_i e(\mathfrak{p}_i/p_i)\rceil s/e(\mathfrak{p}_i/p_i)} Q((p_i\mathbb{Z}_{K_2})^{b_i}, s)\right),$$

*where $Q((p\mathbb{Z}_{K_2})^b, s)$ is defined as follows. Set $e = e(p/3)$, $\mathfrak{p}$ an ideal of $K_2$ above $p$ and $\mathfrak{p}_z$ an ideal of $L$ above $\mathfrak{p}$, and define $s' = s/e(\mathfrak{p}/p)$. Then:*

- *if $e(\mathfrak{p}_z/\mathfrak{p}) = 1$, (hence $e(\mathfrak{p}/3)$ is even) we have*

$$Q((p\mathbb{Z}_{K_2})^b, s) = \begin{cases} 0 & \text{if } b = 0\ , \\ 1/\mathcal{N}(p)^{s'} & \text{if } b = 1/e(\mathfrak{p}/p)\ , \\ 1/\mathcal{N}(p)^{s'} - 1/\mathcal{N}(p)^{2s'} & \text{if } 2/e(\mathfrak{p}/p) \le b \le 3e/2 - 1/e(\mathfrak{p}/p)\ , \\ 1 - 1/\mathcal{N}(p)^{2s'} & \text{if } b = 3e/2\ . \end{cases}$$

- *if $e(\mathfrak{p}_z/\mathfrak{p}) = 2$ (hence $e(\mathfrak{p}/p) = 1$) we have*

$$Q((p\mathbb{Z}_{K_2})^b, s) = \begin{cases} 1 & \text{if } b = 0\ , \\ 1 - 1/\mathcal{N}(p)^{s'} & \text{if } 1 \le b \le 3e/2 - 3/2\ , \\ -1/\mathcal{N}(p)^{s'} & \text{if } b = 3e/2 - 1/2\ , \\ 1 & \text{if } b = 3e/2\ . \end{cases}$$

*Proof.* Since the indices are independent, it is enough to prove the formulas for $g = 1$. In this case we have

$$\begin{aligned} S_{\alpha_0}(s) = &\sum_{\substack{0\le a<3e/2-1/e(\mathfrak{p}/p) \text{ or } a=3e/2\\ ae(\mathfrak{p}/p)\in\mathbb{Z}\cup\{3e(\mathfrak{p}/3)/2\}}} \mathcal{N}(p)^{\lceil ae(\mathfrak{p}/p)\rceil s/e(\mathfrak{p}/p)} f_{\alpha_0}\left((p\mathbb{Z}_{K_2})^{(a+h(0,a,e))}\right) \\ &- \sum_{\substack{0\le a<3e/2-1/e(\mathfrak{p}/p) \text{ or } a=3e/2\\ ae(\mathfrak{p}/p)\in\mathbb{Z}\cup\{3e(\mathfrak{p}/3)/2\}}} \mathcal{N}(p)^{\lceil ae(\mathfrak{p}/p)\rceil s/e(\mathfrak{p}/p)} f_{\alpha_0}\left((p\mathbb{Z}_{K_2})^{(a+h(1,a,e))}\right). \end{aligned}$$

Thus,

$$\begin{aligned} S_{\alpha_0}(s) = &\sum_{\substack{0\le a<3e/2-1/e(\mathfrak{p}/p)\\ ae(\mathfrak{p}/p)\in\mathbb{Z}}} \mathcal{N}(p)^{as} f_{\alpha_0}\left((p\mathbb{Z}_{K_2})^{(a+h(0,a,e))}\right) \\ &\qquad + \mathcal{N}(p)^{\lceil 3e/2\rceil s} f_{\alpha_0}\left((p\mathbb{Z}_{K_2})^{3e/2}\right) \\ &- \sum_{\substack{0\le a<3e/2-1/e(\mathfrak{p}/p)\\ ae(\mathfrak{p}/p)\in\mathbb{Z}}} \mathcal{N}(p)^{as} f_{\alpha_0}\left((p\mathbb{Z}_{K_2})^{(a+h(1,a,e))}\right) , \end{aligned}$$

so by an easy change of variables

$$S_{\alpha_0}(s) = \sum_{\substack{h_0 \le b < 3e/2 - 1/e(\mathfrak{p}/p) + h_0 \\ be(\mathfrak{p}/p) \in \mathbb{Z}}} \mathcal{N}(p)^{(b-h_0)s} f_{\alpha_0}\left((p\mathbb{Z}_{K_2})^b\right) + \mathcal{N}(p)^{\lceil 3e/2 \rceil s} f_{\alpha_0}\left((p\mathbb{Z}_{K_2})^{3e/2}\right)$$

$$- \sum_{\substack{h_1 \le b < 3e/2 - 1/e(\mathfrak{p}/p) + h_1 \\ be(\mathfrak{p}/p) \in \mathbb{Z}}} \mathcal{N}(p)^{(b-h_1)s} f_{\alpha_0}\left((p\mathbb{Z}_{K_2})^b\right),$$

where $h_0 = 1, 1/2, 0$ if $e(\mathfrak{p}_z/p) = 1$, $e(\mathfrak{p}/p) = 2$, $e(\mathfrak{p}_z/\mathfrak{p}) = 2$, respectively, and $h_1 = 2/e(\mathfrak{p}_z/p)$.

Looking at the coefficients of $f_{\alpha_0}((p\mathbb{Z}_{K_2})^b)\,\mathcal{N}(p)^{\lceil be(\mathfrak{p}/p)\rceil s/e(\mathfrak{p}/p)}$ gives the formulas for $Q((p\mathbb{Z}_{K_2})^b, s)$. □

**Definition 1.4.5.** (1) *We let $\mathcal{B}$ be the set of formal products of the form $\prod_{p_i|3\mathbb{Z}_k}(p_i\mathbb{Z}_{K_2})^{b_i}$, where the $b_i$ are such that $0 \le b_i \le 3e(p_i/3)/2$ and $e(\mathfrak{p}_i/p_i)b_i \in \mathbb{Z} \cup \{3e(\mathfrak{p}_i/3)/2\}$.*

*This is the same as taking*

$$\prod_{\substack{\mathfrak{p}_i|3\mathbb{Z}_{K_2} \\ p_i \text{ inert in } K_2/k}} \mathfrak{p}_i^{b_i} \prod_{\substack{\mathfrak{p}_i|3\mathbb{Z}_{K_2} \\ p_i \text{ split in } K_2/k}} (\mathfrak{p}_i\tau_2(\mathfrak{p}_i))^{b_i} \prod_{\substack{\mathfrak{p}_i|3\mathbb{Z}_{K_2} \\ p_i \text{ ramified in } K_2/k}} \mathfrak{p}_i^{2b_i},$$

*in other words, the product of prime ideals $\mathfrak{p}$ of $K_2$ above 3 with exponents $b'$ such that $0 \le b' \le 3e(\mathfrak{p}/3)/2$, $b' \in \mathbb{Z} \cup \{3e(\mathfrak{p}/3)/2\}$, and which are stable by $\tau_2$.*

(2) *We will consider any $\mathfrak{b} \in \mathcal{B}$ as an ideal of $K_2$ where, by abuse of language, we accept to have half powers of prime ideals of $K_2$ and we will set $\mathfrak{b}_z = \mathfrak{b}\mathbb{Z}_L$.*

(3) *If $\mathfrak{b} = \prod_{\mathfrak{p}_i|3\mathbb{Z}_{K_2}} \mathfrak{p}_i^{b_i{}'} \in \mathcal{B}$, $b_i{}' = e(\mathfrak{p}_i/p_i)b_i$, we set*

$$\lceil \mathcal{N} \rceil(\mathfrak{b}) = \prod_{\mathfrak{p}_i|\mathfrak{b}} \mathcal{N}(\mathfrak{p}_i)^{\lceil b_i{}' \rceil}.$$

We would now like to set

$$\mathfrak{b} = \prod_{1 \le i \le g} (p_i\mathbb{Z}_{K_2})^{b_i} \in \mathcal{B}$$

and rewrite the formulas as functions of $\mathfrak{b}$ instead of the $b_i$, but in doing so we would lose the informations about the set of the $p_i$ (in particular we lose the information about the $p_i$ for which $b_i = 0$).

Thus, we let $E = \{p_1, \dots, p_g\} \subset \{p \mid 3\mathbb{Z}_k\}$ to be the set of (distinct) prime ideals of $k$ above 3 not dividing $\mathfrak{a}_\alpha$, so that

$$\mathfrak{a}_\alpha = \prod_{\substack{p_i|3\mathbb{Z}_k \\ p_i \notin E}} (p_i\mathbb{Z}_{K_2})^{r_i},$$

where as usual $r_i = 1/(e(\mathfrak{p}_i/p_i))$. We obtain

$$\sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{E\subset\{p|3\mathbb{Z}_k\}} \sum_{\substack{(\mathfrak{a}_0,\mathfrak{a}_1)\in J\\ \{p|3\mathbb{Z}_k,p\nmid\mathfrak{a}_\alpha\}=E}} \frac{1}{\mathcal{N}(\mathfrak{a}_\alpha)^s} \sum_{(\mathfrak{b}_1,\dots,\mathfrak{b}_g)\in B} f_{\alpha_0}\left(\prod_{1\le i\le g} (p_i\mathbb{Z}_{K_2})^{b_i}\right)\cdot$$
$$\cdot \prod_{p_i\in E} (Q((p_i\mathbb{Z}_{K_2})^{b_i},s)\,\mathcal{N}(p_i^{\lceil b_i e(\mathfrak{p}_i/p_i)\rceil s/e(\mathfrak{p}_i/p_i)}))\ ,$$

so that

$$\sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{E\subset\{p|3\mathbb{Z}_k\}} \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ p|\mathfrak{b}\Rightarrow p\in E}} \lceil\mathcal{N}\rceil\mathfrak{b}^s \prod_{p_i\in E} Q((p_i\mathbb{Z}_{K_2})^{b_i},s) \sum_{\substack{(\mathfrak{a}_0,\mathfrak{a}_1)\in J\\ \{p|3\mathbb{Z}_k,p\nmid\mathfrak{a}_\alpha\}=E}} \frac{f_{\alpha_0}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ .$$

It is easy to see that when $b_i = 0$ we get

$$Q(p^{b_i},s) = \begin{cases} 1 & \text{if } e(\mathfrak{p}/3) \text{ is odd}\\ 0 & \text{if } e(\mathfrak{p}/3) \text{ is even,}\end{cases}$$

so when $e(\mathfrak{p}_i/3)$ is odd we can omit the corresponding $p_i$ in the product, and when $e(\mathfrak{p}_i/3)$ is even we get a zero term.

Thus we can write

$$\sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{E\subset\{p|3\mathbb{Z}_k\}} \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ p|\mathfrak{b}\Rightarrow p\in E\\ p\in E \text{ and } e(\mathfrak{p}/3) \text{ even}\Rightarrow p|\mathfrak{b}}} \lceil\mathcal{N}\rceil\mathfrak{b}^s \prod_{p|\mathfrak{b}} Q((p\mathbb{Z}_{K_2})^{v_p(\mathfrak{b})},s)\cdot$$
$$\cdot \sum_{\substack{(\mathfrak{a}_0,\mathfrak{a}_1)\in J\\ \{p|3\mathbb{Z}_k,p\nmid\mathfrak{a}_\alpha\}=E}} \frac{f_{\alpha_0}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}$$
$$= \sum_{\mathfrak{b}\in\mathcal{B}} \lceil\mathcal{N}\rceil(\mathfrak{b})^s P_{\mathfrak{b}}(s) \sum_{\substack{E\subset\{p|3\mathbb{Z}_k\}\\ p|\mathfrak{b}\Rightarrow p\in E\\ p\nmid\mathfrak{b} \text{ and } e(\mathfrak{p}/3) \text{ even}\Rightarrow p\notin E}} \sum_{\substack{(\mathfrak{a}_0,\mathfrak{a}_1)\in J\\ \{p|3\mathbb{Z}_k,p\nmid\mathfrak{a}_\alpha\}=E}} \frac{f_{\alpha_0}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ ,$$

where $P_{\mathfrak{b}}(s) = \prod_{p|\mathfrak{b}} Q((p\mathbb{Z}_{K_2})^{v_p(\mathfrak{b})},s)$, so that

$$\sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{\mathfrak{b}\in\mathcal{B}} \lceil\mathcal{N}\rceil(\mathfrak{b})^s P_{\mathfrak{b}}(s) \sum_{\substack{(\mathfrak{a}_0,\mathfrak{a}_1)\in J\\ (\mathfrak{a}_\alpha,\mathfrak{b})=1\\ \mathfrak{p}\nmid\mathfrak{b} \text{ and } e(\mathfrak{p}/3) \text{ even}\Rightarrow\mathfrak{p}|\mathfrak{a}_\alpha}} \frac{f_{\alpha_0}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ .$$

Now we have the following lemma.

**Lemma 1.4.6.** *With the present notation, we have*

$$(\mathfrak{a}_\alpha, 3\mathbb{Z}_{K_2}) = \prod_{\substack{\mathfrak{p}|3\mathbb{Z}_{K_2},\ \mathfrak{p}\nmid\mathfrak{b}\\ e(\mathfrak{p}/3)\ even}} \mathfrak{p}\ .$$

*Proof.* Both sides being squarefree ideals of $K_2$ dividing $3\mathbb{Z}_{K_2}$, we must show that each prime ideal above 3 dividing one side divides the other. In one direction this is clear: if $\mathfrak{p} \nmid \mathfrak{b}$ and $e(\mathfrak{p}/3)$ is even then $\mathfrak{p} \mid \mathfrak{a}_\alpha$. Conversely, let $\mathfrak{p} \mid \mathfrak{a}_\alpha$ above 3. Since $(\mathfrak{a}_\alpha, \mathfrak{b}) = 1$ we already know that $\mathfrak{p} \nmid \mathfrak{b}$. In cases (1), (3), and (4) we have $\rho \in K_2$ so $e(\mathfrak{p}/3) = v_\mathfrak{p}(3) = 2v_\mathfrak{p}(1-\rho)$ is even. In cases (2) and (5), if $e(\mathfrak{p}/3)$ was odd, then by Corollary 1.3.2, $\mathfrak{p}$ would be ramified in $L/K_2$, and in particular would not be split, so that $\mathfrak{p} \notin \mathcal{D}_3$, contradicting Proposition 1.2.10, and proving the lemma. □

Thus, we set the following definition:

**Definition 1.4.7.** (1) *For $\mathfrak{b}$ as above we define*

$$\mathfrak{r}^e(\mathfrak{b}) = \prod_{\substack{\mathfrak{p} \mid 3\mathbb{Z}_{K_2},\ \mathfrak{p} \nmid \mathfrak{b} \\ e(\mathfrak{p}/3)\ even}} \mathfrak{p}\ .$$

(2) *We set $\mathfrak{d}_3 = \prod_{p \in \mathcal{D}_3} p$.*

The above lemma states that $(\mathfrak{a}_\alpha, 3\mathbb{Z}_{K_2}) = \mathfrak{r}^e(\mathfrak{b})$, and it is clear that if this is the case then $\mathfrak{a}_\alpha$ is coprime to $\mathfrak{b}$ and that $\mathfrak{p} \nmid \mathfrak{b}$, $e(\mathfrak{p}/3)$ even implies that $\mathfrak{p} \mid \mathfrak{a}_\alpha$. Furthermore, again by Proposition 1.2.10 since $\mathfrak{p} \mid (\mathfrak{a}_\alpha, 3\mathbb{Z}_{K_2})$ implies that $p \in \mathcal{D}_3$, we must have $\mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_3$. Note that by contraposition, this is clearly equivalent to $\mathfrak{d}_3' \mid \mathfrak{b}$, where $\mathfrak{d}_3' = \prod_{\substack{p \mid 3\mathbb{Z}_k,\ p \notin \mathcal{D}_3 \\ e(\mathfrak{p}/3)\ \text{even}}} \mathfrak{p}$.

Thus we obtain

$$\sum_{(\mathfrak{a}_0, \mathfrak{a}_1) \in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{\substack{\mathfrak{b} \in \mathcal{B} \\ \mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_3}} \lceil \mathcal{N} \rceil(\mathfrak{b})^s P_\mathfrak{b}(s) \sum_{\substack{(\mathfrak{a}_0, \mathfrak{a}_1) \in J \\ (\mathfrak{a}_\alpha, 3\mathbb{Z}_{K_2}) = \mathfrak{r}^e(\mathfrak{b})}} \frac{f_{\alpha_0}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}.$$

## 1.5 Computation of $f_{\alpha_0}(\mathfrak{b})$

Recall that $\mathfrak{b}_z \mid 3\sqrt{-3}$ and that the $\mathfrak{a}_i$ are coprime squarefree ideals such that $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$ and $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$. We have also set $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$ with $\alpha_0 \in (L^*/L^{*3})[T]$. Changing $\mathfrak{q}_0$ and $\alpha_0$ if necessary, we may assume that $\alpha_0$ is coprime to $\mathfrak{b}_z$, although this is not essential for the proof. Finally, recall that

$$f_{\alpha_0}(\mathfrak{b}) = \left|\{\overline{u} \in S_3(L)[T],\ x^3 \equiv \alpha_0 u \pmod{{}^*\mathfrak{b}_z} \quad \text{soluble in } L\}\right|,$$

where we have replaced the congruence $x^3/(\alpha_0 u) \equiv 1 \pmod{{}^*\mathfrak{b}_z}$ by the above since we assume $\alpha_0$ coprime to $\mathfrak{b}_z$.

Finally, recall that for each $\mathfrak{b} \in \mathcal{B}$ we have $\mathfrak{b} = \tau_2(\mathfrak{b})$.

To compute $f_{\alpha_0}(\mathfrak{b})$, we will proceed by a series of lemmas.

**Definition 1.5.1.** *Set*

$$S_\mathfrak{b}(L)[T] = \{\overline{u} \in S_3(L)[T],\ x^3 \equiv u \pmod{{}^*\mathfrak{b}_z}\ \textit{soluble}\}\ ,$$

*where $u$ is any lift of $\overline{u}$ coprime to $\mathfrak{b}_z$, and the congruence is in $L$.*

**Lemma 1.5.2.** *If $f_{\alpha_0}(\mathfrak{b}) \neq 0$ then $f_{\alpha_0}(\mathfrak{b}) = |S_{\mathfrak{b}}(L)[T]|$.*

*Proof.* Indeed, assume that $x_0^3 \equiv \alpha_0 u_0 \pmod{{}^*\mathfrak{b}_z}$ for some $u_0 \in S_3(L)[T]$. The congruence $x^3 \equiv \alpha_0 u \pmod{{}^*\mathfrak{b}_z}$ is thus equivalent to $(x/x_0)^3 \equiv (u/u_0) \pmod{{}^*\mathfrak{b}_z}$, in other words to $u/u_0 \in S_{\mathfrak{b}}(L)[T]$, so the set of possible $\overline{u}$ is equal to $\overline{u_0}S_{\mathfrak{b}}(L)[T]$, whose cardinality is $|S_{\mathfrak{b}}(L)[T]|$. □

**Lemma 1.5.3.** *Let $\mathfrak{a}_0, \mathfrak{a}_1$ as in condition (1) of Proposition 1.2.7. Then $f_{\alpha_0}(\mathfrak{b}) \neq 0$ if and only if $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl_{\mathfrak{b}}(L)^3$.*

*Proof.* The condition $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl_{\mathfrak{b}}(L)^3$ is equivalent to the existence of $\mathfrak{q}_1$ and $\beta_1 \equiv 1 \pmod{{}^*\mathfrak{b}_z}$ such that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_1^3 = \beta_1\mathbb{Z}_L$. Assume first that $u$ exists, so that $x_0^3 = \alpha_0 u\beta$ for some $\beta \equiv 1 \pmod{{}^*\mathfrak{b}_z}$ and $u\mathbb{Z}_L = \mathfrak{q}^3$. It follows that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3\mathfrak{q}^3 = \alpha_0 u\mathbb{Z}_L = (x_0^3/\beta)\mathbb{Z}_L$, so we can take $\mathfrak{q}_1 = \mathfrak{q}_0\mathfrak{q}/x_0$ and $\beta_1 = 1/\beta \equiv 1 \pmod{{}^*\mathfrak{b}_z}$. Conversely, assume that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_1^3 = \beta_1\mathbb{Z}_L$ with $\beta_1 \equiv 1 \pmod{{}^*\mathfrak{b}_z}$. Since $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$, we have $t(\beta_2) = \gamma^3$ for some $\gamma \in L^*$. It follows that $\alpha_0\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \beta_1(\mathfrak{q}_0/\mathfrak{q}_1)^3$. Thus, $u = \alpha_0/\beta_2$ is a virtual unit, and $u^t$ is a cube of $L$ since this is true for $\alpha_0$ and for $\beta_1$. Thus $\overline{u} \in S_3(L)[T]$ and $1^3 \equiv \beta_1 \equiv \alpha_0/u \pmod{{}^*\mathfrak{b}_z}$, so $f_{\alpha_0}(\mathfrak{b}) \neq 0$, proving the lemma. □

Remark that when we suppose $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl_{\mathfrak{b}}(L)^3$ we have automatically $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$, so we just need to suppose $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$.

**Lemma 1.5.4.** *Set $Z_{\mathfrak{b}} = (\mathbb{Z}_L/\mathfrak{b}_z)^*$. Then*

$$|S_{\mathfrak{b}}(L)[T]| = \frac{|(U(L)/U(L)^3)[T]||(Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]|}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|} .$$

*In particular*

$$|S_3(L)[T]| = |(U(L)/U(L)^3)[T]||(Cl(L)/Cl(L)^3)[T]| .$$

*Proof.* Since this is now standard (see [12] and [18]) we only sketch the proof. From Lemma 1.2.6 we have the exact sequence of $\mathbb{F}_3[T]$-modules

$$1 \longrightarrow \frac{U(L)}{U(L)^3} \longrightarrow S_3(L) \longrightarrow Cl(L)[3] \longrightarrow 1 ,$$

Taking the kernel by $T$ thus keeps exactness, so we deduce that

$$|S_3(L)[T]| = |(U(L)/U(L)^3)[T]||(Cl(L)[3])[T]| .$$

Since $T$ has order dividing 4, it is coprime to 3, so it is well-known that the finite $\mathbb{F}_3[T]$ modules $Cl(L)[3]$ and $Cl(L)/Cl(L)^3$ are isomorphic, so in particular $(Cl(L)[3])[T] \simeq (Cl(L)/Cl(L)^3)[T]$, proving the second formula of the lemma. For the first, we have the exact sequence of $\mathbb{F}_3[T]$-modules

$$1 \longrightarrow S_{\mathfrak{b}}(L) \longrightarrow S_3(L) \longrightarrow \frac{Z_{\mathfrak{b}}}{Z_{\mathfrak{b}}^3} \longrightarrow \frac{Cl_{\mathfrak{b}}(L)}{Cl_{\mathfrak{b}}(L)^3} \longrightarrow \frac{Cl(L)}{Cl(L)^3} \longrightarrow 1 ,$$

from which it follows that

$$|S_{\mathfrak{b}}(L)[T]| = \frac{|S_3(L)[T]||(Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]|}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]||(Cl(L)/Cl(L)^3)[T]|} ,$$

giving the desired formula after replacing $|S_3(L)[T]|$ by what we have computed above. □

The quantity $|(Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]|$ will in fact disappear in subsequent computations, and in any case cannot be computed more explicitly.
The quantity $|(U(L)/U(L)^3)[T]|$ is given by the following lemma.

**Lemma 1.5.5.** *For any number field $K$, denote by $\mathrm{rk}_3(K)$ the 3-rank of the group of units of $K$, in other words $\mathrm{rk}_3(K) = \dim_{\mathbb{F}_3}(U(K)/U(K)^3)$, so that $|U(K)/U(K)^3| = 3^{\mathrm{rk}_3(K)}$.*

(1) *With evident notation we have*

$$\mathrm{rk}_3(K) = \begin{cases} r_1(K) + r_2(K) - 1 & \text{if } \rho \notin K, \\ r_1(K) + r_2(K) & \text{if } \rho \in K. \end{cases}$$

(2) *We have $|(U(L)/U(L)^3)[T]| = 3^{r(U)}$, where*

$$r(U) = \begin{cases} \mathrm{rk}_3(k) & \text{in cases (1) and (4),} \\ \mathrm{rk}_3(L) - \mathrm{rk}_3(k) & \text{in cases (2) and (3),} \\ \mathrm{rk}_3(L) + \mathrm{rk}_3(k) - \mathrm{rk}_3(K_2) - \mathrm{rk}_3(k_z) & \text{in case (5).} \end{cases}$$

*Proof.* (1) is clear from Dirichlet's theorem, so let us prove (2). Case (1) is trivial, and it is immediate to see that in case (4) we have $(U(L)/U(L)^3)[T] = U(k)/U(k)^3$. For cases (2) and (3), we have the exact sequence

$$1 \longrightarrow \frac{U(k)}{U(k)^3} \longrightarrow \frac{U(K_2)}{U(K_2)^3} \longrightarrow \frac{U(K_2)}{U(K_2)^3}[\tau_2 + 1] \longrightarrow 1 \ ,$$

where the rightmost nontrivial map is induced by $u \mapsto \tau_2(u)/u$, as well as the exact sequence

$$1 \longrightarrow \frac{U(K_2)}{U(K_2)^3} \longrightarrow \frac{U(L)}{U(L)^3} \longrightarrow \frac{U(L)}{U(L)^3}[\tau + 1] \longrightarrow 1 \ ,$$

which enables us to conclude. Finally, for case (5) we have

$$1 \longrightarrow \frac{U(K_2)}{U(K_2)^3}[\tau_2 + 1] \longrightarrow \frac{U(L)}{U(L)^3}[\tau_2 + 1] \longrightarrow \frac{U(L)}{U(L)^3}[\tau + 1, \tau_2 + 1] \longrightarrow 1 \ ,$$

and

$$1 \longrightarrow \frac{U(k_z)}{U(k_z)^3} \longrightarrow \frac{U(L)}{U(L)^3} \longrightarrow \frac{U(L)}{U(L)^3}[\tau_2 + 1] \longrightarrow 1$$

so we can conclude. □

The last quantity that we need to compute is $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|$.

**Lemma 1.5.6.** *Assume that $\mathfrak{b}$ is an ideal of $\mathcal{B}$, stable by $\tau_2$ and such that $\mathfrak{b}_z \mid 3\sqrt{-3}$, and define*

$$\mathfrak{c}_z = \prod_{\substack{\mathfrak{p}_z \subset L \\ \mathfrak{p}_z \mid \mathfrak{b}_z}} \mathfrak{p}_z^{\lceil v_{\mathfrak{p}_z}(\mathfrak{b}_z)/3 \rceil} \ .$$

*Then*

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]| = \left| \frac{\mathfrak{c}_z}{\mathfrak{b}_z}[T] \right| \ .$$

*Proof.* This has also been proved in a slightly different context in [18], but again for completeness we sketch the proof. We first claim that we have the exact sequence

$$1 \longrightarrow \frac{1+\mathfrak{c}_z}{1+\mathfrak{b}_z} \longrightarrow Z_{\mathfrak{b}} \longrightarrow Z_{\mathfrak{b}}^3 \longrightarrow 1\ ,$$

where the map to $Z_{\mathfrak{b}}^3$ is of course cubing. Indeed, first note that if $x \in \mathfrak{c}_z$ then $(1+x)^3 = 1+3x+3x^2+x^3 \equiv 1 \pmod{\mathfrak{b}_z}$ since $x^3 \in \mathfrak{b}_z$ by definition of $\mathfrak{c}_z$, and

$$v_{\mathfrak{p}_z}(3x) \geq e(\mathfrak{p}_z/3) + v_{\mathfrak{p}_z}(\mathfrak{b}_z)/3 \geq v_{\mathfrak{p}_z}(\mathfrak{b}_z)$$

since $\mathfrak{b}_z \mid 3\sqrt{-3}$, so that $(1+\mathfrak{c}_z)/(1+\mathfrak{b}_z)$ is in the kernel of the cubing map. Conversely, assume that $x^3 \equiv 1 \pmod{\mathfrak{b}_z}$, so that $\prod_{0\leq j\leq 2}(x-\rho^j) \in \mathfrak{b}_z$. Thus for any prime $\mathfrak{p}_z \mid \mathfrak{b}_z$ we must have $v_{\mathfrak{p}_z}(x-\rho^j) \geq v_{\mathfrak{p}_z}(\mathfrak{b}_z)/3$ for at least one $j$, so that for that $j$ we have $v_{\mathfrak{p}_z}(x-\rho^j) \geq v_{\mathfrak{p}_z}(\mathfrak{c}_z)$. Since $v_{\mathfrak{p}_z}(\mathfrak{c}_z) \leq e(\mathfrak{p}_z/3)/2 = v_{\mathfrak{p}_z}(1-\rho)$, it follows that for all $j$ we will have $v_{\mathfrak{p}_z}(x-\rho^j) \geq v_{\mathfrak{p}_z}(\mathfrak{c}_z)$, and in particular $x \equiv 1 \pmod{\mathfrak{c}_z}$.

Thus the $\mathbb{F}_3[T]$-modules $(1+\mathfrak{c}_z)/(1+\mathfrak{b}_z)$ and $Z_{\mathfrak{b}}[3]$ are isomorphic, and since 2 and 3 are coprime once again the latter is $\mathbb{F}_3[T]$-isomorphic to $Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3$, so in particular $(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T] \simeq ((1+\mathfrak{c}_z)/(1+\mathfrak{b}_z))[T]$. The use of the Artin–Hasse logarithm and exponential maps (here simply $x-x^2/2$ and $x+x^2/2$) shows that $(1+\mathfrak{c}_z)/(1+\mathfrak{b}_z)$ is isomorphic to the additive group $\mathfrak{c}_z/\mathfrak{b}_z$, so we conclude $\square$

**Lemma 1.5.7.**

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]| = \begin{cases} |\mathfrak{c}_z/\mathfrak{b}_z| & \text{in case (1)} \\ \dfrac{|\mathfrak{c}_z/\mathfrak{b}_z|}{|(\mathfrak{c}_z\cap k)/(\mathfrak{b}_z\cap k)|} & \text{in cases (2) and (3)} \\ |(\mathfrak{c}_z\cap k)/(\mathfrak{b}_z\cap k)| & \text{in case (4)} \\ \dfrac{|\mathfrak{c}_z/\mathfrak{b}_z||(\mathfrak{c}_z\cap k)/(\mathfrak{b}_z\cap k)|}{|(\mathfrak{c}_z\cap K_2)/(\mathfrak{b}_z\cap K_2)||(\mathfrak{b}_z\cap k_z)/(\mathfrak{c}_z\cap k_z)|} & \text{in case (5).} \end{cases}$$

*Proof.* Note that

$$\left|\frac{\mathfrak{c}_z}{\mathfrak{b}_z}[\tau'-1]\right| = \left|\frac{\mathfrak{c}_z\cap L^{\tau'}}{\mathfrak{b}_z\cap L^{\tau'}}\right|\ ,$$

where $\tau' \in \{\tau, \tau_2\}$ and $L^{\tau'}$ is the subextension of $L$ stable by $\tau'$.

Moreover, we have the exact sequence

$$1 \longrightarrow \frac{\mathfrak{c}_z}{\mathfrak{b}_z}[\tau'-1] \longrightarrow \frac{\mathfrak{c}_z}{\mathfrak{b}_z} \longrightarrow \frac{\mathfrak{c}_z}{\mathfrak{b}_z}[\tau'+1] \longrightarrow 1,$$

so we can conclude. $\square$

**Lemma 1.5.8.** *In case (5) we have*

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]| = \prod_{\substack{p\subset k\\ p\mid\mathfrak{b}}} \mathcal{N}(p)^{(2b/3+x(b,p))}\ ,$$

*where* $x(b,p) = r_3(2b)/3$ *if* $e(\mathfrak{p}_z/p) = 1$, $x(b,p) = {r_3}'(b)/3$ *if* $e(\mathfrak{p}_z/\mathfrak{p}) = 2$ *and* $b < 3e(p/3)/2$, $x(b,p) = -1/(3r_3(2b))$ *if* $e(\mathfrak{p}/p) = 2$ *and* $2b \not\equiv 0 \pmod 3$, *and* $r_3(b)$ *is the class modulo* 3 *of* $b$ *in* $\{0,1,2\}$ *and* ${r_3}'(b)$ *is the class of* $b$ *modulo* 3 *in* $\{-1,0,1\}$.

*Proof.* By multiplicativity it is enough to prove the formulas for a prime $p$ of $k$ dividing $\mathfrak{b}$.

- If $e(\mathfrak{p}_z/p) = 1$ then there is no ramification in $L/k$, so $\mathfrak{b}_z = \prod_{\mathfrak{p}_z|\mathfrak{b}} \mathfrak{p}_z^b$, $\mathfrak{c}_z = \prod_{\mathfrak{p}_z|\mathfrak{b}} \mathfrak{p}_z^{\lceil b/3 \rceil}$, and similarly $\mathfrak{b}_z \cap K_2 = \prod_{\mathfrak{p}|\mathfrak{b}} \mathfrak{p}^b$, $\mathfrak{c}_z \cap K_2 = \prod_{\mathfrak{p}|\mathfrak{b}} \mathfrak{p}^{\lceil b/3 \rceil}$ $\mathfrak{b}_z \cap k = \prod_{p|\mathfrak{b}} p^b$, $\mathfrak{c}_z \cap k = \prod_{p|\mathfrak{b}} p^{\lceil b/3 \rceil}$ $\mathfrak{b}_z \cap k_z = \prod_{\mathfrak{p}'|\mathfrak{b}, \mathfrak{p}' \subset k_z} \mathfrak{p}'^b$, $\mathfrak{c}_z \cap k_z = \prod_{\mathfrak{p}'|\mathfrak{b}} \mathfrak{p}'^{\lceil b/3 \rceil}$.

  Moreover $\mathcal{N}_{L/\mathbb{Q}}(p\mathbb{Z}_L) = \mathcal{N}(p)^4$ and $\mathcal{N}_{K_2/\mathbb{Q}}(p\mathbb{Z}_{K_2}) = \mathcal{N}_{k_z/\mathbb{Q}}(p\mathbb{Z}_{k_z}) = \mathcal{N}(p)^2$.

  So we get

$$|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| = \mathcal{N}(p)^{b - \lceil b/3 \rceil} = \mathcal{N}(p)^{(2b/3 + r_3(2b)/3)}.$$

- If $e(\mathfrak{p}_z/\mathfrak{p}) = 2$ then $p$ is ramified in $L/K_2$, $e(p/3)$ is odd and so $p$ is also ramified in $k_z/k$.

  We have $\mathfrak{b}_z \cap K_2 = \prod_{\mathfrak{p}|\mathfrak{b}} \mathfrak{p}^{\lceil b \rceil}$, $\mathfrak{c}_z \cap K_2 = \prod_{\mathfrak{p}|\mathfrak{b}} \mathfrak{p}^{\lceil \lceil 2b/3 \rceil /2 \rceil}$; $\mathfrak{b}_z \cap k = \prod_{p|\mathfrak{b}} p^{\lceil b \rceil}$, $\mathfrak{c}_z \cap k = \prod_{p|\mathfrak{b}} p^{\lceil \lceil 2b/3 \rceil /2 \rceil}$ and $\mathfrak{b}_z \cap k_z = \prod_{\mathfrak{p}'|\mathfrak{b}} \mathfrak{p}'^{2b}$, $\mathfrak{c}_z \cap k_z = \prod_{\mathfrak{p}'|\mathfrak{b}} \mathfrak{p}'^{\lceil 2b/3 \rceil}$.

  Now, $\mathcal{N}_{L/\mathbb{Q}}((p\mathbb{Z}_L)^{1/2}) = \mathcal{N}_{K_2/\mathbb{Q}}(p\mathbb{Z}_{K_2}) = \mathcal{N}(p)^2$ and $\mathcal{N}_{k_z/\mathbb{Q}}((p\mathbb{Z}_{k_z})^{1/2}) = \mathcal{N}(p)$.

  So we obtain

$$|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| \quad = \quad \mathcal{N}(p)^{2b - \lceil 2b/3 \rceil - \lceil b \rceil + \lceil \lceil 2b/3 \rceil /2 \rceil} = \mathcal{N}(p)^{\lfloor b \rfloor - \lfloor \lceil 2b/3 \rceil /2 \rfloor}.$$

  In particular, when $b = 3e(p/3)/2$ we obtain

$$|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| = \mathcal{N}(p)^{e(p/3)},$$

  and if $b < 3e(p/3)/2$, then $b \in \mathbb{Z}$ and we obtain

$$|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| = \mathcal{N}(p)^{b - \lfloor \lceil 2b/3 \rceil /2 \rfloor} = \mathcal{N}(p)^{2b/3 + {r_3}'(b)/3}.$$

- When $e(\mathfrak{p}/p) = 2$ then $p$ is ramified in $K_2/k$ and it can be ramified or not in $k_z/k$ depending on $e(\mathfrak{p}/3)$ parity.

  We have $\mathfrak{b}_z \cap K_2 = \prod_{\mathfrak{p}|\mathfrak{b}} \mathfrak{p}^{2b}$, $\mathfrak{c}_z \cap K_2 = \prod_{\mathfrak{p}|\mathfrak{b}} \mathfrak{p}^{\lceil 2b/3 \rceil}$, $\mathfrak{b}_z \cap k = \prod_{p|\mathfrak{b}} p^{\lceil b \rceil}$, $\mathfrak{c}_z \cap k = \prod_{p|\mathfrak{b}} p^{\lceil \lceil 2b/3 \rceil /2 \rceil}$ and $\mathfrak{b}_z \cap k_z = \prod_{\mathfrak{p}'|\mathfrak{b}} \mathfrak{p}'^{2b}$, $\mathfrak{c}_z \cap k_z = \prod_{\mathfrak{p}'|\mathfrak{b}} \mathfrak{p}'^{\lceil 2b/3 \rceil}$ if $e(p/3)$ is odd, otherwise we get $b_z \cap k_z = \prod_{\mathfrak{p}'|\mathfrak{b}} \mathfrak{p}'^{\lceil b \rceil}$ and $\mathfrak{c}_z \cap k_z = \prod_{\mathfrak{p}'|\mathfrak{b}} \mathfrak{p}'^{\lceil \lceil 2b/3 \rceil /2 \rceil}$.

  So we have $\mathcal{N}_{L/\mathbb{Q}}((p\mathbb{Z}_L)^{1/2}) = \mathcal{N}(p)^2$, $\mathcal{N}_{K_2/\mathbb{Q}}((p\mathbb{Z}_{K_2})^{1/2}) = \mathcal{N}(p)$ and $\mathcal{N}_{k_z/\mathbb{Q}}(p\mathbb{Z}_{k_z}^{1/2}) = \mathcal{N}(p)$ if $e(p/3)$ is odd, otherwise $\mathcal{N}_{k_z/\mathbb{Q}}(p\mathbb{Z}_{k_z}) = \mathcal{N}(p)^2$.

  So if $e(p/3)$ is odd we obtain

$$|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| = \mathcal{N}(p)^{\lceil b \rceil - \lceil \lceil 2b/3 \rceil /2 \rceil}$$

  and if $e(p/3)$ is even we have

$$|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| = \mathcal{N}(p)^{\lfloor b \rfloor - \lfloor \lceil 2b/3 \rceil /2 \rfloor}$$

which leads to the formulas, after some calculations. □

This finishes the computation of $f_{\alpha_0}(\mathfrak{b})$.

## 1.6 Final Form of the Dirichlet Series

We can now put together all the work that we have done. Recall that we have computed $|U(L)/U(L)^3[T]|$ in Lemma 1.5.5 and $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|$ in Lemmas 1.5.7 and 1.5.8. Moreover, $\mathcal{B}$ and $\lceil\mathcal{N}\rceil$ are defined in Definition 1.4.5 and $P_{\mathfrak{b}}(s) = \prod_{p|\mathfrak{b}} Q((p\mathbb{Z}_{K_2})^{v_p(\mathfrak{b})}, s)$, where $Q(p^b, s)$ is defined in Lemma 1.4.4. Finally, recall that we have

$$\Phi(s) = \frac{1}{2} + \sum_{K\in\mathcal{F}(K_2)} \frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s} \cdot$$

**Theorem 1.6.1.** *Set $\mathfrak{d}_3 = \prod_{p\in\mathcal{D}_3} p$, and for any ideal $\mathfrak{b}$, set for simplicity $G_{\mathfrak{b}} = (Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]$. We have*

$$\Phi(s) = \frac{|(U(L)/U(L)^3)[T]|}{2\cdot 3^{(3/2)[k:\mathbb{Q}]s}\prod_{\substack{p|3\mathbb{Z}_k,\\ e(\mathfrak{p}/3)\ odd}} \mathcal{N}(p)^{s/2}} \cdot$$
$$\cdot \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ \mathfrak{r}^e(\mathfrak{b})|\mathfrak{d}_3}} \left(\frac{\lceil\mathcal{N}\rceil(\mathfrak{b})}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))}\right)^s \frac{P_{\mathfrak{b}}(s)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|} \sum_{\chi\in\widehat{G_{\mathfrak{b}}}} F(\mathfrak{b},\chi,s)\ ,$$

*where*

$$F(\mathfrak{b},\chi,s) = \prod_{\substack{p|\mathfrak{r}^e(\mathfrak{b})\\ p\in\mathcal{D}_3'(\chi)}} 2 \prod_{\substack{p|\mathfrak{r}^e(\mathfrak{b})\\ p\in\mathcal{D}_3\setminus\mathcal{D}_3'(\chi)}} (-1) \prod_{p\in\mathcal{D}'(\chi)} \left(1+\frac{2}{\mathcal{N}(p)^s}\right) \prod_{p\in\mathcal{D}\setminus\mathcal{D}'(\chi)} \left(1-\frac{1}{\mathcal{N}(p)^s}\right)\ ,$$

*where in cases (1) and (4), $\mathcal{D}'(\chi)$ (respectively $\mathcal{D}_3'(\chi)$) is the set of $p\in\mathcal{D}$ (respectively $p\in\mathcal{D}_3$) such that $\chi(p\mathbb{Z}_L) = 1$, while in the other cases it is the set of $p\in\mathcal{D}$ (respectively $p\in\mathcal{D}_3$) such that $\chi(\mathfrak{p}_z) = \chi(\tau'(\mathfrak{p}_z))$ if $p\mathbb{Z}_L = \mathfrak{p}_z\tau'(\mathfrak{p}_z)$, $\tau'\in\{\tau,\tau_2\}$ or $\chi(\mathfrak{p}_z\tau\tau_2(\mathfrak{p}_z)) = \chi(\tau(\mathfrak{p}_z)\tau_2(\mathfrak{p}_z))$ if $p\mathbb{Z}_L = \mathfrak{p}_z\tau(\mathfrak{p}_z)\tau_2(\mathfrak{p}_z)\tau\tau_2(\mathfrak{p}_z)$.*

*Proof.* We have shown above that

$$\Phi(s) = \frac{1}{2\cdot 3^{(3/2)[k:\mathbb{Q}]s}\prod_{\substack{p|3\mathbb{Z}_k,\\ e(\mathfrak{p}/3)\ \mathrm{odd}}} \mathcal{N}(p)^{s/2}} \sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ ,$$

where $J$ is a suitable set of pairs of ideals $(\mathfrak{a}_0,\mathfrak{a}_1)$, and we have computed that

$$\sum_{(\mathfrak{a}_0,\mathfrak{a}_1)\in J} \frac{S_{\alpha_0}(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ \mathfrak{r}^e(\mathfrak{b})|\mathfrak{d}_3}} \lceil\mathcal{N}\rceil(\mathfrak{b})^s P_{\mathfrak{b}}(s) \sum_{\substack{(\mathfrak{a}_0,\mathfrak{a}_1)\in J\\ (\mathfrak{a}_\alpha,3\mathbb{Z}_{K_2})=\mathfrak{r}^e(\mathfrak{b})}} \frac{f_{\alpha_0}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}.$$

where $P_{\mathfrak{b}}(s)$ is given by Lemma 1.4.4. In the preceeding section we have seen that $f_{\alpha_0}(\mathfrak{b}) \neq 0$ if and only if $\mathfrak{a}_0\mathfrak{a}_1^2 \in Cl_{\mathfrak{b}}(L)^3$ (so we only need to assume condition (1) of Lemma 1.2.8), and in that case that

$$f_{\alpha_0}(\mathfrak{b}) = \frac{|(U(L)/U(L)^3)[T]||(Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]|}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|}.$$

Set $G_{\mathfrak{b}} = (Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]$. Let $\mathfrak{a}_0$ and $\mathfrak{a}_1$ be as in condition (a) of Proposition 1.2.7. We have $\mathfrak{a}_0\mathfrak{a}_1^2 \in Cl_{\mathfrak{b}}(L)^3$ if and only if $\chi(\mathfrak{a}_0\mathfrak{a}_1^2) = 1$ for all characters

$\chi \in \widehat{G_{\mathfrak{b}}}$. The number of such characters being equal to $|G_{\mathfrak{b}}|$, by orthogonality of characters we have

$$\Phi(s) = \frac{|(U(L)/U(L)^3)[T]|}{2 \cdot 3^{(3/2)[k:\mathbb{Q}]s} \prod_{\substack{p|3\mathbb{Z}_k, \\ e(\mathfrak{p}/3) \text{ odd}}} \mathcal{N}(p)^{s/2}} \cdot$$
$$\cdot \sum_{\substack{\mathfrak{b} \in \mathcal{B} \\ \mathfrak{r}^e(\mathfrak{b})|\mathfrak{d}_3}} \frac{[\mathcal{N}](\mathfrak{b})^s P_{\mathfrak{b}}(s)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|} \sum_{\chi \in \widehat{G_{\mathfrak{b}}}} H(\mathfrak{b}, \chi, s) \ ,$$

with

$$H(\mathfrak{b}, \chi, s) = \sum_{\substack{(\mathfrak{a}_0, \mathfrak{a}_1) \in J' \\ (\mathfrak{a}_\alpha, 3\mathbb{Z}_{K_2}) = \mathfrak{r}^e(\mathfrak{b})}} \frac{\chi(\mathfrak{a}_0 \mathfrak{a}_1^2)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} \ ,$$

where $J'$ is the set of pairs of coprime squarefree ideals of $L$, satisfying the condition (1) of Lemma 1.2.8, with no class group condition.

Thus

$$H(\mathfrak{b}, \chi, s) = \frac{\chi(\mathfrak{r}^e(\mathfrak{b}))}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s} \sum_{\substack{(\mathfrak{a}, 3\mathbb{Z}_L) = 1 \\ \mathfrak{a} \text{ squarefree} \\ \tau(\mathfrak{a}) = \tau_2(\mathfrak{a}) = \mathfrak{a}}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} \sum_{\mathfrak{a}_1 | \mathfrak{a}\mathfrak{r}^e(\mathfrak{b}), \ \mathfrak{a}_1 \in J''} \chi(\mathfrak{a}_1) \ ,$$

where $J''$ is the set of squarefree ideals $\mathfrak{a}_1$ such that $\mathfrak{a}_1$ is stable by $\tau_2$ in case (4), $\mathfrak{a}_1 \tau'(\mathfrak{a}_1) = \mathfrak{a}\mathfrak{r}^e(\mathfrak{b})$ for each nontrivial $\tau' \in \{\tau, \tau_2\}$ in the other cases.

Let us define $G(\chi, p)$ by:

$$G(\chi, p) = \begin{cases} 1 + \chi(p\mathbb{Z}_L) & \text{in cases (1) and (4), and otherwise :} \\ \chi(\mathfrak{p}_z) + \chi(\tau'(\mathfrak{p}_z)) & \text{when } p\mathbb{Z}_L = \mathfrak{p}_z \tau'(\mathfrak{p}_z) \\ \chi(\mathfrak{p}_z \tau\tau_2(\mathfrak{p}_z)) + \chi(\tau(\mathfrak{p}_z)\tau_2(\mathfrak{p}_z)) & \text{when } p\mathbb{Z}_L = \mathfrak{p}_z \tau(\mathfrak{p}_z)\tau_2(\mathfrak{p}_z)\tau\tau_2(\mathfrak{p}_z). \end{cases}$$

Since $\mathfrak{a}$ is coprime to 3, by multiplicativity we have $H(\mathfrak{b}, \chi, s) = S_1 S_2$ with

$$S_1 = \frac{\chi(\mathfrak{r}^e(\mathfrak{b}))}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s} \prod_{p | \mathfrak{r}^e(\mathfrak{b})} G(\chi, p) \quad \text{and}$$
$$S_2 = \sum_{\substack{(\mathfrak{a}, 3\mathbb{Z}_L) = 1 \\ \mathfrak{a} \text{ squarefree} \\ \tau(\mathfrak{a}) = \tau_2(\mathfrak{a}) = \mathfrak{a}}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} \prod_{p | \mathfrak{a}} G(\chi, p) = \prod_{p \in \mathcal{D}} \left(1 + \frac{\chi(p\mathbb{Z}_L) G(\chi, p)}{\mathcal{N}(p)^s}\right) \ ,$$

where $\mathcal{D}$ is given by Definition 1.2.9.

Now, $\chi$ takes only values 1, $\rho$, and $\rho^2$, so looking at the possible values for $G(\chi, p)$, in cases (1) and (4) we have just to distinguish wheter $\chi(p\mathbb{Z}_L) = 1$ or not, while in the other cases we need to take also into account the values of $\chi(\mathfrak{p}_z)$, $\chi(\tau'(\mathfrak{p}_z))$ or $\chi(\mathfrak{p}_z \tau\tau_2(\mathfrak{p}_z))$, $\chi(\tau(\mathfrak{p}_z)\tau_2(\mathfrak{p}_z))$, so we obtain

$$S_1 = \frac{1}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s} \prod_{\substack{p | \mathfrak{r}^e(\mathfrak{b}) \\ p \in \mathcal{D}_3'(\chi)}} 2 \prod_{\substack{p | \mathfrak{r}^e(\mathfrak{b}) \\ p \in \mathcal{D}_3 \setminus \mathcal{D}_3'(\chi)}} (-1) \ ,$$
$$S_2 = \prod_{p \in \mathcal{D}'(\chi)} \left(1 + \frac{2}{\mathcal{N}(p)^s}\right) \prod_{p \in \mathcal{D} \setminus \mathcal{D}'(\chi)} \left(1 - \frac{1}{\mathcal{N}(p)^s}\right) \ .$$

□

From the previous theorem we obtain :

**Theorem 1.6.2.** *In cases (2) and (3), set $K_2' = L$, and in all cases denote by $\mathfrak{d}(K_2'/k)$ the relative discriminant of $K_2'/k$. Let us define*

$$c_1 = \frac{|(U(L)/U(L)^3)[T]|}{2 \cdot 3^{(3/2)[k:\mathbb{Q}]} \prod_{\substack{p|3\mathbb{Z}_k \\ e(\mathfrak{p}/3)\ odd}} \mathcal{N}(p)^{1/2}} ,$$

$$c_2 = \sum_{\substack{\mathfrak{b}\in\mathcal{B} \\ \mathfrak{r}^e(\mathfrak{b})|\mathfrak{d}_3}} \frac{\lceil\mathcal{N}\rceil(\mathfrak{b})}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))} \frac{P_{\mathfrak{b}}(1)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|} 2^{\omega(\mathfrak{r}^e(\mathfrak{b}))} ,$$

$$c_3 = \prod_{p\subset k} \left(1 - \frac{3}{\mathcal{N}(p)^2} + \frac{2}{\mathcal{N}(p)^3}\right) \prod_{p|3\mathbb{Z}_k} \left(1 + \frac{2}{\mathcal{N}(p)}\right)^{-1} ,$$

$$c_4 = \frac{1}{\zeta_k(2)} \prod_{p\in\mathcal{D}} \left(1 - \frac{2}{\mathcal{N}(p)(\mathcal{N}(p)+1)}\right) \prod_{p|\mathfrak{d}(K_2'/k)} \left(1 - \frac{1}{\mathcal{N}(p)+1}\right) ,$$

*where $\omega(\mathfrak{r}^e(\mathfrak{b})) = \sum_{p|\mathfrak{r}^e(\mathfrak{b})} 1$.*

- *In cases (1) and (4), around $s = 1$ we have*

$$\Phi(s) = \frac{C(K_2/k)}{(s-1)^2} + \frac{C(K_2/k)D(K_2/k)}{s-1} + O(1) ,$$

*with constants*

$$C(K_2/k) = c_1c_2c_3(\mathrm{Res}_{s=1}\,\zeta_k(s))^2 \quad \textit{and}$$

$$D(K_2/k) = 2\gamma_k + \lim_{s\to1} \frac{G'(s)}{G(s)} \quad \textit{where}$$

$$G(s) = \frac{\Phi(s)}{\zeta_k(s)^2} \quad \textit{and} \quad \gamma_k = \lim_{s\to1} \left(\frac{\zeta_k(s)}{\mathrm{Res}_{s=1}\,\zeta_k(s)} - \frac{1}{s-1}\right) ,$$

*and where $\lim_{s\to1} G'(s)/G(s)$ can easily be computed more explicitly if desired.*

*In addition, using the notation given at the beginning of this chapter, as $X \to \infty$, for all $\varepsilon > 0$ we have*

$$M(K_2/k, X) = C(K_2/k)X(\log(X) + D(K_2/k) - 1) + O(X^{\alpha+\varepsilon}), \ . \quad (1.1)$$

*for some $\alpha < 1$ (see Section 1.7).*

- *In cases (2), (3), and (5) we have*

$$\Phi(s) = \frac{C(K_2/k)}{(s-1)} + O(1),$$

*with*

$$C(K_2/k) = c_1c_2c_4(\mathrm{Res}_{s=1}\,\zeta_{K_2'}(s)) ,$$

*and for all $\varepsilon > 0$ we have*

$$M(K_2/k, X) = C(K_2/k)X + O(X^{\alpha+\varepsilon}), \quad (1.2)$$

*for some $\alpha < 1$ (see Section 1.7).*

*Proof.* It is easy to see that when $\chi$ is not the trivial character, the functions $F(\mathfrak{b},\chi,s)$ are holomorphic for $\mathrm{Re}(s) > 1/2$, so do not occur in the polar part at $s = 1$. On the other hand, since $\mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_3$, for $\chi = 1$ we have $F(\mathfrak{b},1,s) = 2^{\omega(\mathfrak{r}^e(\mathfrak{b}))}P(s)$, where $P(s) = \prod_{p\in\mathcal{D}}\left(1+\frac{2}{\mathcal{N}(p)^s}\right)$, so in cases (1) and (4) we get

$$P(s) = \frac{\zeta_k(s)^2\prod_{p\subset k}\left(1-\frac{3}{\mathcal{N}(p)^{2s}}+\frac{2}{\mathcal{N}(p)^{3s}}\right)}{\prod_{p\mid 3\mathbb{Z}_k}\left(1+\frac{2}{\mathcal{N}(p)^s}\right)},$$

so we obtain $C(K_2/k) = c_1c_2c_3(\mathrm{Res}_{s=1}\,\zeta_k(s))^2$. Now to compute $D(K_2/k)$ we remark that

$$D(K_2/k) = \lim_{s\to 1}\left(\frac{\Phi'(s)}{\Phi(s)}+\frac{2}{s-1}\right),$$

and that

$$\frac{2}{s-1} = -\frac{2\zeta_k'(s)}{\zeta_k(s)} + 2\gamma_k + O((s-1)),$$

where $R = \mathrm{Res}_{s=1}\,\zeta_k(s)$, so

$$D(K_2/k) = \lim_{s\to 1}\left(\frac{\Phi'(s)}{\Phi(s)} - \frac{2\zeta_k'(s)}{\zeta_k(s)} + 2\gamma_k\right).$$

Now we remark that

$$\frac{\Phi'(s)}{\Phi(s)} - \frac{2\zeta_k'(s)}{\zeta_k(s)} = \frac{G'(s)}{G(s)},$$

where $G(s) = \dfrac{F(s)}{\zeta_k(s)^2}$, so we obtain

$$D(K_2/k) = \lim_{s\to 1}\frac{G'(s)}{G(s)} + 2\gamma_k\ .$$

In cases (2), (3) and (5) we obtain with evident notation

$$P(s) = \frac{\zeta_{K_2'}(s)\prod_{\left(\frac{K_2'/k}{p}\right)=1}\left(1-\frac{3}{\mathcal{N}(p)^{2s}}+\frac{2}{\mathcal{N}(p)^{3s}}\right)}{\prod_{\left(\frac{K_2'/k}{p}\right)=0}(1-1/\mathcal{N}(p)^s)^{-1}\prod_{\left(\frac{K_2'/k}{p}\right)=-1}(1-1/\mathcal{N}(p)^{2s})^{-1}}$$

so the formula for the polar part of $\Phi(s)$ follows after an immediate computation, with $c_4$ given by

$$c_4 = \prod_{\left(\frac{K_2'/k}{p}\right)=1}\left(1-\frac{3}{\mathcal{N}(p)^2}+\frac{2}{\mathcal{N}(p)^3}\right) \prod_{\left(\frac{K_2'/k}{p}\right)=0}\left(1-\frac{1}{\mathcal{N}(p)}\right)\prod_{\left(\frac{K_2'/k}{p}\right)=-1}\left(1-\frac{1}{\mathcal{N}(p)^2}\right).$$

Indeed, note that since in cases (2) and (3) we have set $K_2' = L$, by Proposition 1.2.10 the condition $p\in\mathcal{D}$ is equivalent to $\left(\frac{K_2'/k}{p}\right) = 1$.

Now we have evidently $1/\zeta_k(2) = P_{-1}P_0P_1$ with

$$P_\varepsilon = \prod_{\left(\frac{K_2'/k}{p}\right)=\varepsilon} \left(1 - \frac{1}{\mathcal{N}(p)^2}\right),$$

so replacing $P_{-1}$ by $(\zeta_k(2)P_0P_1)^{-1}$ in the formula for $c_4$ gives the formula of the corollary.

Finally, since our Dirichlet series have nonnegative and polynomially bounded coefficients, the asymptotic results follow from a general (and in this case easy) Tauberian theorem. For the error term $O(X^\alpha)$ with an explicit $\alpha < 1$, we refer to the following section. □

**Remark**. The asymptotic (1.1) for $k = \mathbb{Q}$ (corresponding to cyclic cubic fields) is due to Cohn [21], and over a general number field to Cohen, Diaz y Diaz and Olivier [18]. The equation (1.2) over $\mathbb{Q}$ is certainly also in the literature (at least its main term), but over a general number field it seems to be new.

## 1.7 Error term of the asymptotic formula

The aim of this section is to compute the error term in the asymptotic formulas (1.1) and (1.2).

First of all, we need some properties of the Dirichlet series $\Phi(s)$.

**Lemma 1.7.1.** *For the Dirichlet series $\Phi(s) = \sum_{n=1}^\infty a_n n^{-s}$ we have $|a_n| \ll n^\varepsilon$, for every $\varepsilon > 0$.*

*Proof.* This can be proved just referring to [27, Lemma 6.1], who prove the bound for the number of cubic extensions with fixed norm of the discriminant.

We give a direct proof for the convenience of the reader.

The only part we need to bound is $F(\mathfrak{b}, \chi, s)$ and in particular we need to bound the Dirichlet coefficients $b_n$ of

$$\sum_{n=1}^\infty b_n n^{-s} := \prod_{p\in\mathcal{D}'(\chi)} \left(1 + \frac{2}{\mathcal{N}(p)^s}\right) \prod_{p\in\mathcal{D}\setminus\mathcal{D}'(\chi)} \left(1 - \frac{1}{\mathcal{N}(p)^s}\right), \quad \mathrm{Re}(s) > 1.$$

but for every $n$ we just need to count the number of distinct primes ($\in \mathbb{Z}$) dividing $n$ (that is $\omega(n)$) and for each one of those we will have at most $[k:\mathbb{Q}]$ prime ideals of $k$ above it, so we obtain

$$|b_n| \ll 2^{\omega(n)[k:\mathbb{Q}]}$$

and since $\omega(n) \le (1 + o(1))\frac{\log n}{\log\log n}$ (for $n \to \infty$) ([51, §5.3]) we obtain

$$|b_n| \ll n^\varepsilon, \quad \forall \varepsilon > 0,$$

but $|a_n|/|b_n|$ is bounded, and we conclude that $|a_n| \ll n^\varepsilon$, for all $\varepsilon > 0$. □

So $\Phi(s)$ is absolutely convergent for $\mathrm{Re}(s) > 1$.

Let us define $S(x) = \sum_{n\le x} a_n$ and $S^*(x) = \sum_{n<x} a_n + \frac{1}{2}a_x$, where $a_x$ is defined to be 0 if $x \in \mathbb{R} \setminus \mathbb{N}$ ($x \ge 0$).

Our aim is to compute $S(x)$, for this we will need some complex analysis results.

Let us fix $\delta > 0$, set $\kappa = 1 + \delta$, $\kappa_0 = 1/2 + \delta$. By Perron formula [51, §2.1, Théorème 1], we have

$$S^*(x) = \frac{1}{2\pi i} \int_{\kappa - i\infty}^{\kappa + i\infty} \Phi(s) x^s s^{-1} ds, \quad (x > 0)$$

and the effective formula [51, §2.1, Théorème 2]

$$S(x) = \frac{1}{2\pi i} \int_{\kappa - iT}^{\kappa + iT} \Phi(s) x^s s^{-1} ds + O\left( x^\kappa \sum_{n=1}^{\infty} \frac{|a_n|}{n^\kappa (1 + T|\log(x/n)|)} \right), \quad T \geq 1.$$

Let $\Gamma$ be the border of the rectangle of vertices $\kappa_0 - iT$, $\kappa_0 + iT$, $\kappa + iT$, $\kappa - iT$.

$$S(x) = \frac{1}{2\pi i} \left( \int_\Gamma \Phi(s) x^s s^{-1} ds - B(T) - B(-T) - C \right) + O(A),$$

where

$$A = x^\kappa \sum_{n=1}^{\infty} \frac{|a_n|}{n^\kappa (1 + T|\log(x/n)|)}$$

$$B(t) = \int_{\kappa_0 + it}^{\kappa + it} \Phi(s) x^s s^{-1} ds$$

$$C = \int_{\kappa_0 - iT}^{\kappa_0 + iT} \Phi(s) x^s s^{-1} ds.$$

We have

$$\frac{1}{2\pi i} \int_\Gamma \Phi(s) x^s s^{-1} ds = \mathrm{Res}_{s=1} \left( \frac{\Phi(s) x^s}{s} \right).$$

So we obtain

$$S(x) = Res_{s=1} \left( \frac{\Phi(s) x^s}{s} \right) + E,$$

where the error term $E$ is given by

$$E = E(\delta, T) = -\frac{1}{2\pi i}(B(T) + B(-T) + C) + O(A).$$

To bound this error term we will need to bound $\Phi(s)$ polynomially in $\mathrm{Im}(s)$ in the strip $\frac{1}{2} \leq \mathrm{Re}(s) \leq 1$. We will be content with the simplest such bound, namely the convexity bound (Phragmén-Lindelöf's principle), but it is possible to improve it for certain classes of base fields $k$.

By [38, (5.20)], we have

$$\frac{s-1}{s+1} \zeta_k(s) \ll \mathfrak{q}(\zeta_k, s)^{(1-\sigma)/2 + \varepsilon}, \quad \text{for all } \varepsilon > 0, \tag{1.3}$$

where in our case the analytic conductor $\mathfrak{q}(\zeta_k, s)$ is less than $|d_k|\,(|t|+4)^{[k:\mathbb{Q}]}$ [38, §5.10, p. 125]. The implied constant only depends on the field degree and $\varepsilon$.

In particular for $|t| \geq 1$ we have

$$\zeta_k(s) \ll |t|^{\mu_k(\sigma) + \varepsilon}, \quad s = \sigma + it, \tag{1.4}$$

for some $\mu_k(\sigma)$. We can for instance use $\mu_k(\sigma) = (1 - \sigma)[k : \mathbb{Q}]/2$, and the implied constant now depends on the field discriminant and $\varepsilon$ : the dependence on the degree is no longer needed by Odlyzko's bound : $[k : \mathbb{Q}] = O(\log |d_k|)$.

**Lemma 1.7.2.** *For all $s = \sigma + it$, $\frac{1}{2} + \delta \leq \sigma \leq 1 + \delta$, $|t| \geq 1$, we have*

$$|\Phi(s)| \ll |t|^{\mu(\sigma)+\varepsilon}, \quad \text{for all } \varepsilon > 0,$$

*where $\mu(\sigma) = 0$ for $\sigma > 1$ and $\mu(\sigma)$ is convex and decreasing in the strip $0 < \sigma < 1$. A possible choice for $\mu$ is $\mu(\sigma) = 2\mu_k(\sigma)$.*

*Proof.* We only need to bound $|F(\mathfrak{b}, \chi, s)|$. When $\chi$ is non trivial, $F(\mathfrak{b}, \chi, s)$ is holomorphic for $\mathrm{Re}(s) > \frac{1}{2}$, so we just need to deal with the case $\chi = \chi_0$ the trivial character. In this case we obtain $F(\mathfrak{b}, 1, s) = 2^{\omega(\mathfrak{r}^e(\mathfrak{b}))}P(s)$, where $P(s) = \prod_{p \in \mathcal{D}} \left(1 + \frac{2}{\mathcal{N}(p)^s}\right)$ so in cases (1) and (4) we get

$$P(s) = \frac{\zeta_k(s)^2 \prod_{p \subset k} \left(1 - \frac{3}{\mathcal{N}(p)^{2s}} + \frac{2}{\mathcal{N}(p)^{3s}}\right)}{\prod_{p | 3\mathbb{Z}_k} \left(1 + \frac{2}{\mathcal{N}(p)^s}\right)},$$

while in cases (2), (3) and (5) we obtain with evident notation

$$P(s) = \frac{\zeta_{K_2'}(s) \prod_{\left(\frac{K_2'/k}{p}\right)=1} \left(1 - \frac{3}{\mathcal{N}(p)^{2s}} + \frac{2}{\mathcal{N}(p)^{3s}}\right)}{\prod_{\left(\frac{K_2'/k}{p}\right)=0} \left(1 - 1/\mathcal{N}(p)^s\right)^{-1} \prod_{\left(\frac{K_2'/k}{p}\right)=-1} \left(1 - 1/\mathcal{N}(p)^{2s}\right)^{-1}}.$$

The products in the formula are holomorphic for $\mathrm{Re}(s) > 1/2$, and we can extend $\zeta_{K_2'}$ to a meromorphic function in this vertical strip so that

$$|F(\mathfrak{b}, 1, s)| \ll |\zeta_{K_2'}(s)| \ll |\zeta_k^2(s)|$$

and we conclude by (1.4). □

Our goal is the following proposition :

**Proposition 1.7.3.** *The error term $E$ satisfies*

$$|E| \ll_{\varepsilon, d_k} x^{\alpha+\varepsilon}, \quad \text{for all } \varepsilon > 0,$$

*where $\mu$ is as in Lemma 1.7.2 and*

$$\alpha = 1 - \frac{1}{2\left(1 + \mu\left(\frac{1}{2}\right)\right)}.$$

*The implied constant only depends on $\varepsilon$ and the field discriminant.*

In order to prove this proposition, we need to bound $|A|$, $|B(\pm T)|$ and $|C|$. We may assume $x \geq 1$.

**Lemma 1.7.4.** *We have*

$$|A| \ll_\delta \frac{x^\kappa}{T} + \frac{x}{T} \log T.$$

*Proof.* Let us write $A = A_1 + A_2$, where $A_2$ is the contribution of the $n$ in the interval $[\frac{1}{2}x, 2x]$, and $A_1$ is the contribution of all the other $n$.

For $n$ not in the interval $[\frac{1}{2}x, 2x]$ we have $|\log(x/n)| > \log 2$, hence

$$|A_1| \leq \frac{x^\kappa}{T} \log 2 \sum_{n=1}^{\infty} \frac{|a_n|}{n^\kappa},$$

but now the sum is exactly $\Phi(\kappa)$ (remember that the $a_n \geq 0$), which is convergent for $\kappa > 1$, so $|A_1| \ll_\delta \frac{x^\kappa}{T}$.

It remains to deal with the $n$ in the interval $[\frac{1}{2}x, 2x]$.

Let us suppose for simplicity that $x$ is an integer, and let us write $n = x + h$, where $|h| < x$.

We have that $|\log(x/n)| = |\log(1 + \frac{h}{x})| \gg \frac{|h|}{x}$, since $\frac{|h|}{x} < 1$.

$$A_2 = \sum_{x/2 \leq n \leq 2x} \frac{x^\kappa}{n^\kappa} \frac{|a_n|}{1 + T|\log(x/n)|} \ll_\varepsilon (2x)^\varepsilon \sum_{-x/2 \leq h \leq x} \frac{1}{1 + T|h|/x},$$

where we use $\frac{x}{n} = O(1)$ and $|a_n| = O_\varepsilon(n^\varepsilon)$. Finally

$$\begin{aligned} \sum_{-x/2 < h \leq x} \frac{1}{1 + T|h|/x} \leq 2 \sum_{0 \leq h \leq x} \frac{1}{1 + Th/x} &\ll 1 + \sum_{1 \leq h \leq x/T} 1 + \sum_{x/T < h \leq x} \frac{x}{Th} \\ &\ll 1 + \frac{x}{T} + x\frac{\log T}{T}. \end{aligned}$$

So $|A_2| \ll \frac{x}{T} \log T$, and we conclude. □

**Lemma 1.7.5.** *For all $|T| \geq 1$, we have*

$$|B(\pm T)| \ll_{\varepsilon, d_k} \left(\frac{x}{T^{\mu(0)}}\right)^\kappa T^{(\mu(0)-1)+\varepsilon},$$

*where the implied constant only depends on $\varepsilon$ and the field discriminant.*

*Proof.* We have

$$B(t) = \int_{\kappa_0}^{\kappa} x^{\sigma+it} \frac{\Phi(\sigma + it)}{\sigma + it} d\sigma,$$

hence

$$|B(t)| \ll_{\varepsilon, d_k} \int_{\kappa_0}^{\kappa} x^\sigma |t|^{\mu(\sigma)+\varepsilon} \frac{d\sigma}{|t|}, \quad \text{for } |t| \geq 1.$$

By convexity $\mu(\sigma) \leq \mu(0) - \sigma\mu(0)$. So

$$|B(t)| \ll_{\varepsilon, d_k} |t|^{(\mu(0)-1)+\varepsilon} \int_{\kappa_0}^{\kappa} \left(\frac{x}{|t|^{\mu(0)}}\right)^\sigma d\sigma \leq |t|^{(\mu(0)-1)+\varepsilon} |\kappa - \kappa_0| \left(\frac{x}{|t|^{\mu(0)}}\right)^\kappa.$$

Since $|\kappa - \kappa_0| = 1/2$, the result follows. □

**Lemma 1.7.6.** *We have*

$$|C| \ll_{\varepsilon, d_k} x^{\kappa_0} T^{\mu(\kappa_0)+\varepsilon}.$$

*Proof.* Now let us estimate

$$C = \int_{-T}^{T} x^{\kappa_0+it}\Phi(\kappa_0+it)(\kappa_0+it)^{-1} i\, dt.$$

Hence

$$|C| \ll_{\varepsilon,d_k} \int_0^1 x^{\kappa_0} \left|\Phi(\kappa_0+it)\right| \frac{dt}{\kappa_0} + \int_1^T x^{\kappa_0}|t|^{\mu(\kappa_0)+\varepsilon}\frac{dt}{|t|}.$$

Using (1.3) and $\kappa_0 > 1/2$ we obtain

$$\int_0^1 \left|\Phi(\kappa_0+it)\right| \frac{dt}{\kappa_0} \ll_{d_k} 1.$$

Finally

$$C \ll_{\varepsilon,d_k} x^{\kappa_0} T^{\mu(\kappa_0)+\varepsilon} \int_1^T \frac{dt}{t} \ll_{\varepsilon,d_k} x^{\kappa_0} T^{\mu(\kappa_0)+2\varepsilon},$$

for all $\varepsilon > 0$. □

**Proof of the Proposition 1.7.3**. Thanks to the previous lemmas, we conclude that the error term

$$E = -\frac{1}{2\pi i}(B(T) + B(-T) + C) + O(A)$$

satisfies

$$|E| \ll_{\delta,\varepsilon,d_k} \left(\frac{x^\kappa}{T} + \frac{x}{T}\log T\right) + \left(\frac{x}{T^{\mu(0)}}\right)^\kappa T^{(\mu(0)-1)+\varepsilon} + x^{\kappa_0}T^{\mu(\kappa_0)+\varepsilon}.$$

Below, we will choose $T = x^\tau$ for some $\tau > 0$. Since $\kappa > 1$ we can then simplify

$$|E| \ll_{\delta,\varepsilon,d_k} \frac{x^\kappa}{T} + x^{\kappa_0}T^{\mu(\kappa_0)+\varepsilon}.$$

The best error term is obtained when we choose

$$T = x^{\frac{\kappa-\kappa_0}{1+\mu(\kappa_0)}} :$$

recalling that $\kappa - \kappa_0 = 1/2$, we then obtain

$$|E| \ll_{\delta,\varepsilon,d_k} x^{\alpha+\varepsilon},$$

where

$$\alpha = \kappa - \frac{1}{2\left(1+\mu\left(\kappa_0\right)\right)}\ . \tag{1.5}$$

Since $\mu$ is decreasing, we have $\mu(\kappa_0) \le \mu(1/2)$, hence

$$\alpha \le \kappa - \frac{1}{2\left(1+\mu(1/2)\right)}. \tag{1.6}$$

We then let $\delta = \varepsilon$ and the result follows. □

In particular when $k = \mathbb{Q}$ we can take $\mu(1/2) = 1/2$, and we obtain an error term $|E| \ll_\varepsilon x^{2/3+\varepsilon}$.

**Remark**. For $k = \mathbb{Q}$ we used the convexity bound

$$\zeta(s) \ll_\varepsilon t^{(1-\sigma)/2+\varepsilon}.$$

Using subconvexity bounds, for instance $\zeta(1/2+it) \ll_\varepsilon t^{1/6+\varepsilon}$ ([38, page 101]), we would get better error terms.

Over an arbitrary number field $k$ the convexity bound gives $\mu_k(1/2) = d/4$, where $d = [k:\mathbb{Q}]$, so the error term in Proposition

gets bigger, but we still get a power saving in the error term, since we obtain $O(X^{1-\beta})$, for some $\beta > 0$.

**Corollary 1.7.7** (of Proposition 1.7.3)**.**

(1) *Unconditionally, the error term is*

$$E \ll_{\varepsilon,d_k} x^{1-1/(2+[k:\mathbb{Q}])+\varepsilon}, \quad \textit{for all } \varepsilon > 0.$$

(2) *Under Lindelöf Hypothesis, the error term is*

$$E \ll_\varepsilon x^{1/2+\varepsilon}, \quad \textit{for all } \varepsilon > 0.$$

*Proof.* The first point follows from Proposition 1.7.3, (1.4) with $\mu_k(1/2) = [k:\mathbb{Q}]/4$, and $\mu(1/2) = 2\mu_k(1/2)$. Under Lindelöf Hypothesis, we have $\mu(\sigma) = 0$ for every $\sigma > 1/2$. □

In particular, Corollary 1.7.7 holds under the GRH [38, Corollary 5.20]. We sum up the work of this section in a slightly more general proposition.

**Proposition 1.7.8.** *Let $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ be a Dirichlet series which is absolutely convergent for $\mathrm{Re}(s) > 1$, which can be extended meromorphically to $\mathrm{Re}(s) > 1/2$ with a pole of order $k \geq 1$ at $s = 1$ and no other pole in the strip $\frac{1}{2} < \mathrm{Re}(s) < 1$. In addition, assume the following:*

(1) *The coefficients $a_n$ are nonnegative, and for all $\varepsilon > 0$ we have*

$$a_n \ll_\varepsilon n^\varepsilon .$$

(2) *$F(s)$ is a function of finite order in the vertical strip $\frac{1}{2} < \sigma \leq 1$ : we have*

$$|F(\sigma+it)| \ll_\varepsilon |t|^{\mu(\sigma)+\varepsilon}, \quad \textit{when } |t| \geq 1, \textit{ for all } \varepsilon > 0,$$

*where $\mu(1) = 0$, and $\mu(\sigma)$ is convex and decreasing in the strip.*

(3) *The integral*

$$\int_0^1 |F(\sigma+it)|\, dt$$

*is bounded independently of $\frac{1}{2} < \sigma < \frac{1}{2} + \delta$, for some $\delta > 0$.*

*Then for all $\varepsilon > 0$, we have*

$$\sum_{n \leq x} a_n = \mathrm{Res}_{s=1}\left(F(s)\frac{x^s}{s}\right) + O(x^{\alpha+\varepsilon}) ,$$

*where*

$$\alpha = 1 - \frac{1}{2\,(1+\mu(1/2))}. \tag{1.7}$$

*Proof.* Straightforward from the previous section. □

## 1.8 Special Cases: $k = \mathbb{Q}$, Cases (2), (4), and (5)

The computations that we have done are not very difficult, and extremely similar to those of [18], but still they are quite complex, and it is very easy to make mistakes. In addition, there are many different cases. It is thus essential to compute some special cases for each. We begin by the simplest for $k = \mathbb{Q}$, and since $\rho \notin k$ only cases (2), (4), and (5) occur.

### 1.8.1 Case (2): Cyclic Cubic Extensions

This case is classical (see [21]), but we treat it nonetheless. Here $K_2 = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-3})$. By Lemma 1.5.5 we have $|(U(L)/U(L)^3)[T]| = 3$, $[K_2 : \mathbb{Q}] = 1$, and if $\mathfrak{p}_3 = \sqrt{-3}\mathbb{Z}_L$ is the unique ideal above 3, the possible ideals $\mathfrak{b}_z$ are $\mathfrak{p}_3^j$ for $j = 0$, 2, and 3, with corresponding ideals $\mathfrak{c}_z$ equal to $\mathbb{Z}_L$, $\mathfrak{p}_3$, and $\mathfrak{p}_3$. Thus, $|\mathfrak{c}_z/\mathfrak{b}_z| = 1$, 3, 9, and $|(\mathfrak{c}_z \cap \mathbb{Q})/(\mathfrak{b}_z \cap \mathbb{Q})| = 1$, 1, 3, so by Lemma 1.5.7 we have $|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| = 1$, 3, 3. Since $e(3/3) = 1$, $\mathfrak{r}^e(\mathfrak{b})$ is always trivial, and we have respectively $\lceil \mathcal{N} \rceil(\mathfrak{b})^s = 1$, $3^s$, $3^{2s}$, and $P_\mathfrak{b}(s) = 1$, $-1/3^s$, 1. By Definition 1.2.9 we have $\mathcal{D}_3 = \emptyset$, and $\mathcal{D}$ is the set of primes $p \equiv 1 \pmod 3$. Finally, an easy computation shows that $G_\mathfrak{b}$ is trivial for all $\mathfrak{b}$, so the sum over $\chi$ of the functions $F(\mathfrak{b}, \chi, s)$ is always equal to $F(s) = \prod_{p \equiv 1 \pmod 3}(1 + 2/p^s)$. We deduce that, with evident notation

$$\Phi(s) = \frac{3/2}{3^{2s}} \frac{(1, 3^s, 3^{2s})(1, -1/3^s, 1)}{(1, 3, 3)} F(s) = \frac{1}{2}(1 + 2/3^{2s})F(s) \; .$$

We have thus proved the following:

**Proposition 1.8.1.** *We have*

$$\sum_{K/\mathbb{Q} \; cyclic \; cubic} \frac{1}{f(K/\mathbb{Q})^s} = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{2s}}\right) \prod_{p \equiv 1 \pmod 3} \left(1 + \frac{2}{p^s}\right) \; .$$

**Corollary 1.8.2.** *If, as above, $M(\mathbb{Q}/\mathbb{Q}, X)$ denotes the number of cyclic cubic fields $K$ up to isomorphism with $f(K/\mathbb{Q}) \le X$, for all $\varepsilon > 0$ we have*

$$\begin{aligned} M(\mathbb{Q}/\mathbb{Q}, X) &= C(\mathbb{Q}/\mathbb{Q})X + O(X^{2/3+\varepsilon}) \quad \textit{with} \\ C(\mathbb{Q}/\mathbb{Q}) &= \frac{11\sqrt{3}}{36\pi} \prod_{p \equiv 1 \pmod 3} \left(1 - \frac{2}{p(p+1)}\right) \\ &= 0.15852825839614206028350782035 75\ldots \end{aligned}$$

### 1.8.2 Case (4): Pure Cubic Fields

In case (4), we have $K_2 = \mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$, so that $L = K_2$, and $K/\mathbb{Q}$ is a pure cubic field, in other words $K = \mathbb{Q}(\sqrt[3]{m})$.

By Lemma 1.5.5 we have $|(U(L)/U(L)^3)[T]| = 1$, $[K_2 : \mathbb{Q}] = 2$, and since $\mathfrak{p}_3 = \sqrt{-3}\mathbb{Z}_L$ is the only ideal above 3, the possible ideals $\mathfrak{b} = \mathfrak{b}_z$ are $\mathfrak{b} = \mathfrak{p}_3^j$ for $0 \le j \le 3$ (this time including $j = 1$), all of course stable by $\tau_2$, with corresponding ideals $\mathfrak{c} = \mathfrak{c}_z$ equal to $\mathbb{Z}_L$, $\mathfrak{p}_3$, $\mathfrak{p}_3$, and $\mathfrak{p}_3$. Thus by Lemma 1.5.7 we have $|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| = (\mathfrak{c}_z \cap \mathbb{Q})/(\mathfrak{b}_z \cap \mathbb{Q})| = 1$, 1, 1, 3. By Definition 1.2.9 we have $\mathcal{D}_3 = \{3\}$ and $\mathcal{D}$ is the set of all primes $p \ne 3$, so that $\mathfrak{d}_3 = 3\mathbb{Z}$. We

have respectively $\lceil\mathcal{N}\rceil(\mathfrak{b})^s = 1$, $3^{s/2}$, $3^s$, $3^{3s/2}$, $\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s = 3^{s/2}$, 1, 1, 1, and the condition $\mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_3$ is always satisfied. Since $e(\mathfrak{p}/3) = 2$, we have $P_{\mathfrak{b}}(s) = 1$, $1/3^{s/2}$, $1/3^{s/2} - 1/3^s$, $1 - 1/3^s$. If $\chi = \chi_0$ is the trivial character, we thus have $F(\mathfrak{p}_3^j, \chi_0, s) = F(s) = \prod_{p\neq 3}(1 + 2/p^s)$ for $j \geq 1$, while $F(\mathbb{Z}_{K_2}, \chi_0, s) = 2F(s)$. Thus, with the same evident notation as the one used above, the contribution of the trivial characters is equal to

$$\begin{aligned}\Phi_0(s) &= \frac{1/2}{3^{3s/2}} \frac{(1/3^{s/2}, 3^{s/2}, 3^s, 3^{3s/2})(2, 1/3^{s/2}, 1/3^{s/2} - 1/3^s, 1 - 1/3^s)}{(1,1,1,3)} F(s) \\ &= \frac{1}{6}\left(1 + \frac{2}{3^s} + \frac{6}{3^{2s}}\right) \prod_{p\neq 3}\left(1 + \frac{2}{p^s}\right) .\end{aligned}$$

An easy computation shows that the group $G_{\mathfrak{b}}$ is trivial for $\mathfrak{b} = \mathfrak{p}_3^j$ with $0 \leq j \leq 2$, but has order 3 for $\mathfrak{b} = \mathfrak{p}_3^3$. Thus, we must simply add the contribution of the two conjugate nontrivial characters of order 3 of $G_{\mathfrak{p}_3^3}$. By definition, if $\chi$ is one of these characters we have

$$F(\mathfrak{p}_3^3, \chi, s) = \prod_{\chi(p)=1}(1 + 2/p^s) \prod_{\chi(p)\neq 1}(1 - 1/p^s) .$$

The condition $\chi(p) = 1$ is easily seen to be equivalent to $p \equiv \pm 1 \pmod 9$, so we obtain the following proposition:

**Proposition 1.8.3.** *We have*

$$\begin{aligned}\sum_{K/\mathbb{Q}\ pure\ cubic} \frac{1}{f(K/\mathbb{Q})^s} = -\frac{1}{2} + \frac{1}{6}\left(1 + \frac{2}{3^s} + \frac{6}{3^{2s}}\right) \prod_{p\neq 3}\left(1 + \frac{2}{p^s}\right) \\ + \frac{1}{3} \prod_{p\equiv\pm 1 \pmod 9}\left(1 + \frac{2}{p^s}\right) \prod_{p\not\equiv\pm 1 \pmod 9}\left(1 - \frac{1}{p^s}\right) ,\end{aligned}$$

*where $p \not\equiv \pm 1 \pmod 9$ includes $p = 3$.*

**Corollary 1.8.4.** *If, as above, $M(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}, X)$ denotes the number of pure cubic fields $K$ up to isomorphism with $f(K/\mathbb{Q}) \leq X$, for all $\varepsilon > 0$ we have*

$$M(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}, X) = C(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})X(\log(X) + D(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) - 1) + O(X^{2/3+\varepsilon}) ,$$

*where*

$$\begin{aligned}C(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) &= \frac{7}{30}\prod_p\left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right) \\ &= 0.06690773330137837129184163298429563750134 4\ldots \\ D(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) &= 2\gamma - \frac{16}{35}\log(3) + 6\sum_p \frac{\log(p)}{p^2 + p - 2} \\ &= 3.45022279783059196279071191967111041826885\ldots ,\end{aligned}$$

*where $\gamma$ is Euler's constant and the sum is over all primes including $p = 3$.*

To check the validity of these constants, we note that for instance for $X = 10^{16}$ we have

$$M(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}, X) = 26289108423790515\ , \quad \text{while}$$
$$C(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})X(\log(X) + D(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) - 1) = 26289108423786084\ldots$$

As already mentioned, the error is of the order of $O(X^{1/4})$ (in this precise case $0.4431X^{1/4}$), much smaller than $O(X^{2/3+\varepsilon})$ proved above.

### 1.8.3 Case (5): $K_2 = \mathbb{Q}(\sqrt{D})$ with $D \neq -3$

In case (5), we have $K_2 = \mathbb{Q}(\sqrt{D})$ with $D \neq -3$, so $L = \mathbb{Q}(\sqrt{D}, \sqrt{-3})$. Recall from the introduction that we denote by $\mathcal{F}(K_2)$ the set of cubic extensions $K/\mathbb{Q}$ up to isomorphism such that the quadratic subextension of the Galois closure of $K/\mathbb{Q}$ is isomorphic to $K_2$. The goal of this subsection is the proof of the following result.

**Proposition 1.8.5.** *Let $D$ be a fundamental discriminant with $D \neq -3$, let $K_2 = \mathbb{Q}(\sqrt{D})$, and let $r_2(D) = 1$ for $D < 0$ and $r_2(D) = 0$ for $D > 0$. There exists a function $\phi_D(s)$ holomorphic for $\mathrm{Re}(s) > 1/2$ such that*

$$\sum_{K \in \mathcal{F}(K_2)} \frac{1}{f(K/\mathbb{Q})^s} = \phi_D(s) + \frac{3^{r_2(D)}}{6} L_3(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1 + \frac{2}{p^s}\right)\ ,$$

*where*

$$L_3(s) = \begin{cases} 1 + 2/3^{2s} & \text{if } 3 \nmid D, \\ 1 + 2/3^s & \text{if } D \equiv 3 \pmod 9, \\ 1 + 2/3^s + 6/3^{2s} & \text{if } D \equiv 6 \pmod 9. \end{cases}$$

*Proof.* If we denote by $\phi_D(s)$ the contribution of the nontrivial characters in Theorem 1.6.1 it is clear that $\phi_D(s)$ is a holomorphic function for $\mathrm{Re}(s) > 1/2$, so it is sufficient to consider the contribution of the trivial characters. We consider the three cases separately.

(1). Assume first that $3 \nmid D$.
By Lemma 1.5.5 we have $|(U(L)/U(L)^3)[T]| = 3^{r_2(D)}$ where $r_2(D) = 1$ if $D < 0$ and $r_2(D) = 0$ if $D > 0$, we have $[K_2 : \mathbb{Q}] = 2$, and since 3 is unramified in $K_2/\mathbb{Q}$ the possible ideals $\mathfrak{b}_z$ are $\mathfrak{b}_z = \mathfrak{p}_3^j$ for $j = 0$, 2, or 3, where as usual $\mathfrak{p}_3 = \sqrt{-3}\mathbb{Z}_L$, which is not necessarily a prime ideal since 3 may split in $K_2/\mathbb{Q}$, with corresponding ideals $\mathfrak{c}_z = \mathbb{Z}_L$, $\mathfrak{p}_3$, $\mathfrak{p}_3$. Thus by Lemma 1.5.7 we have with our usual notation

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]| = \frac{(1, 3^2, 3^4)(1, 1, 3)}{(1, 1, 3^2)(1, 3, 3^2)}\ ,$$

so $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]| = 1$, 3, 3. We have $\lceil \mathcal{N} \rceil(\mathfrak{b})^s = 1$, $3^s$, $3^{2s}$, and $P_{\mathfrak{b}}(s) = 1$, $-1/3^s$, 1. By Definition 1.2.9 we have $\mathcal{D}_3 = \emptyset$ and $\mathcal{D}$ is the set of all primes $p$ such that $\left(\frac{-3D}{p}\right) = 1$. Thus $\mathfrak{r}^e(\mathfrak{b})$ is always trivial and in particular the condition $\mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_3$ is always satisfied. If $\chi = \chi_0$ is the trivial character, we thus have

$F(\mathfrak{p}_3^j,\chi_0,s)=F(s)=\prod_{(-3D/p)=1}(1+2/p^s)$. It follows that the contribution of the trivial characters is equal to

$$\begin{aligned}\Phi_0(s)&=\frac{3^{r_2(D)}/2}{3^{2s}}\frac{(1,3^s,3^{2s})(1,-1/3^s,1)}{(1,3,3)}F(s)\\&=\frac{3^{r_2(D)}}{6}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{-3D}{p}\right)=1}\left(1+\frac{2}{p^s}\right)\ ,\end{aligned}$$

proving the formula in the case $3\nmid D$.

(2). Assume now that $D\equiv 3 \pmod 9$.
Once again by Lemma 1.5.5 we have $|(U(L)/U(L)^3)[T]|=3^{r_2(D)}$. On the other hand, 3 is ramified in $K_2/\mathbb{Q}$, so denote by $\mathfrak{p}_3$ the prime ideal of $K_2$ above 3 (so that $\mathfrak{p}_3\mathbb{Z}_L=\sqrt{-3}\mathbb{Z}_L$). The possible ideals $\mathfrak{b}$ are $\mathfrak{b}=\mathfrak{p}_3^j$ with $0\le j\le 3$ (including $j=1$), with corresponding ideals $\mathfrak{c}=\mathbb{Z}_{K_2}$, $\mathfrak{p}_3$, $\mathfrak{p}_3$, $\mathfrak{p}_3$. Thus by Lemma 1.5.7 we have with our usual notation

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|=\frac{(1,1,3^2,3^4)(1,1,1,3)}{(1,1,3,3^2)(1,1,3,3^2)}\ ,$$

so $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|=1,1,1,3$. We have $\lceil\mathcal{N}\rceil(\mathfrak{b})^s=1,3^{s/2},3^s,3^{3s/2}$, and $P_{\mathfrak{b}}(s)=1$, $1/3^{s/2}$, $1/3^{s/2}-1/3^s$, $1-1/3^s$. By Definition 1.2.9, since 3 is inert in $K_2'=\mathbb{Q}(\sqrt{-D/3})$ (because $-D/3\equiv 2 \pmod 3$), we have $\mathcal{D}_3=\emptyset$ (so that $\mathfrak{d}_3=\mathbb{Z}_{K_2}$), and $\mathcal{D}$ is the set of all primes $p$ such that $\left(\frac{-3D}{p}\right)=1$. We have $\mathfrak{r}^e(\mathfrak{b})=\mathfrak{p}_3,\mathbb{Z}_{K_2},\mathbb{Z}_{K_2},\mathbb{Z}_{K_2}$ respectively, so the condition $\mathfrak{r}^e(\mathfrak{b})\mid\mathfrak{d}_3$ implies that $\mathfrak{b}=\mathbb{Z}_{K_2}$ must be excluded from the sum. Since $F(\mathfrak{p}_3^j,\chi_0,s)=F(s)=\prod_{(-3D/p)=1}(1+2/p^s)$, it follows that the contribution of the trivial characters is equal to

$$\begin{aligned}\Phi_0(s)&=\frac{3^{r_2(D)}/2}{3^{3s/2}}\frac{(1,3^{s/2},3^s,3^{3s/2})(0,1/3^{s/2},1/3^{s/2}-1/3^s,1-1/3^s)}{(1,1,1,3)}F(s)\\&=\frac{3^{r_2(D)}}{6}\left(1+\frac{2}{3^s}\right)\prod_{\left(\frac{-3D}{p}\right)=1}\left(1+\frac{2}{p^s}\right)\ ,\end{aligned}$$

proving the formula of the proposition in the case $D\equiv 3 \pmod 9$.

(3). Assume finally that $D\equiv 6 \pmod 9$ with $D\neq -3$.
This case is very similar to the preceding one. The initial computations are the same, but now 3 is split in $K_2'$, so $\mathcal{D}_3=\{3\}$, hence $\mathfrak{d}_3=3\mathbb{Z}_k$. We have the same values of $\mathfrak{b}$ and $\mathfrak{r}^e(\mathfrak{b})$, but since $\mathfrak{d}_3=3\mathbb{Z}_k$ the condition $\mathfrak{r}^e(\mathfrak{b})\mid\mathfrak{d}_3$ is always satisfied, even for $\mathfrak{b}=\mathbb{Z}_{K_2}$. Thus for $1\le j\le 3$ we have as above $F(\mathfrak{p}_3^j,\chi_0,s)=F(s)=\prod_{(-3D/p)=1}(1+2/p^s)$, while for $j=0$ we have $F(\mathbb{Z}_{K_2},\chi_0,s)=2F(s)$. It follows that the contribution of the trivial characters is equal to

$$\begin{aligned}\Phi_0(s)&=\frac{3^{r_2(D)}/2}{3^{3s/2}}\frac{(1/3^{s/2},3^{s/2},3^s,3^{3s/2})(2,1/3^{s/2},1/3^{s/2}-1/3^s,1-1/3^s)}{(1,1,1,3)}F(s)\\&=\frac{3^{r_2(D)}}{6}\left(1+\frac{2}{3^s}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{-3D}{p}\right)=1}\left(1+\frac{2}{p^s}\right)\ ,\end{aligned}$$

giving the third formula of the proposition. □

**Corollary 1.8.6.** *Set $D' = -3D$ if $3 \nmid D$ and $D' = -D/3$ if $3 \mid D$, and denote as usual by $\chi_{D'}$ the character $\left(\frac{D'}{\cdot}\right)$. Then if $D \neq -3$ is a fundamental discriminant, for all $\varepsilon > 0$ we have*

$$M(\mathbb{Q}(\sqrt{D})/\mathbb{Q}, X) = C(\mathbb{Q}(\sqrt{D})/\mathbb{Q})X + O(X^{2/3+\varepsilon}) \quad \textit{with}$$
$$C(\mathbb{Q}(\sqrt{D})/\mathbb{Q}) = \frac{3^{r_2(D)}\ell_3 L(\chi_{D'}, 1)}{\pi^2} \prod_{p \mid D'} \left(1 - \frac{1}{p+1}\right) \prod_{\left(\frac{D'}{p}\right)=1} \left(1 - \frac{2}{p(p+1)}\right) ,$$

*where*

$$\ell_3 = \begin{cases} 11/9 & \text{if } 3 \nmid D, \\ 5/3 & \text{if } D \equiv 3 \pmod 9, \\ 7/5 & \text{if } D \equiv 6 \pmod 9. \end{cases}$$

Note that $L(\chi_{D'}, 1)$ is given by Dirichlet's class number formula, in other words with standard notation, $L(\chi_{D'}, 1) = 2\pi h(D')/(w(D')\sqrt{|D'|})$ if $D' < 0$ and $L(\chi_{D'}, 1) = 2h(D')R(D')/\sqrt{D'}$ if $D' > 0$.

The formula in the above Corollary allows to compute the constant $C$ using the the folklore method explained in detail in [15, §10.3.6].

### 1.8.4 Comparison with the Results of [14]

The results of this paper are the cubic analogue of the corresponding results for quartic extensions studied in [14]. It is interesting to note that the final formula (essentially Corollary 1.8.6 above) is extremely similar to that obtained in [14].

**Proposition 1.8.7.** *Keep the notation of Corollary 1.8.6, and denote by $a_{D'}(p)$ the number of copies of $\mathbb{Q}_p$ occurring in $K_2' \otimes \mathbb{Q}_p$ ($a_{D'}(p) = 0$ or $2$ according to whether the number of prime ideals $\mathfrak{p}_i$ above $p$ in $K_2'$ equals $1$ or $2$). For $D \neq -3$ we have*

$$M(\mathbb{Q}(\sqrt{D})/\mathbb{Q}, X) = C(\mathbb{Q}(\sqrt{D})/\mathbb{Q})X + O(X^{2/3+\varepsilon}) \quad \textit{with}$$
$$C(\mathbb{Q}(\sqrt{D})/\mathbb{Q}) = \frac{c_3(D')}{3^{3+r_2(D')}} \prod_{p \neq 3} \left(1 + \frac{a_{D'}(p)}{p}\right)\left(1 - \frac{1}{p}\right) ,$$

*where*

$$c_3(D') = \begin{cases} 11 & \text{if } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1^2 , \\ 15 & \text{if } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1 , \\ 21 & \text{if } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1\mathfrak{p}_2 . \end{cases}$$

*Proof.* By Proposition 1.8.5 we can write

$$\Phi_D(s) = \phi_D(s) + \frac{3^{r_2(D)}}{6} L_3(s) \prod_{p \neq 3} \left(1 + \frac{a_{D'}(p)}{p^s}\right) ,$$

so that

$$\frac{\Phi_D(s)}{(1 - 1/3^s)\zeta(s)} = \psi_D(s) + \frac{3^{r_2(D)}}{6} L_3(s) \prod_{p \neq 3} \left(1 + \frac{a_{D'}(p)}{p^s}\right)\left(1 - \frac{1}{p^s}\right) ,$$

where $\psi_D(s) = \phi_D(s)/((1-1/3^s)\zeta(s))$. When $s$ tends to 1, $\psi_D(s)$ tends to 0, the left-hand side tends to a limit, and it is easy to see that the right-hand side tends to a semi-convergent Euler product. Thus, if we set $P(D') = \prod_{p\neq 3}((1+a_{D'}(p)/p)(1-1/p))$, we have

$$C(\mathbb{Q}(\sqrt{D}/\mathbb{Q})) = \mathrm{Res}_{s=1}\,\Phi_D(s) = \frac{1}{3^{2-r_2(D)}}L_3(1)P(D') = \frac{c_3(D')}{3^{3+r_2(D')}}P(D')\ ,$$

where $c_3(D')$ is given in the proposition, since the different cases for $L_3(1)$ correspond to the different splittings of 3 in $K_2'/\mathbb{Q}$. □

For comparison, we recall the results of [14]. We let $k$ be a cubic number field, and set $g(k) = 3$ if $k$ is cyclic, $g(k) = 1$ otherwise. We let $\mathcal{F}(k)$ be the set of isomorphism classes of quartic number fields $K$ whose cubic resolvent is isomorphic to $k$. If $K \in \mathcal{F}(k)$ then its discriminant $d(K)$ is of the form $d(K) = d(k)f^2$ for some integer $f$, which by abuse of language we call the conductor of $K$ and denote by $f(K/\mathbb{Q})$. As in our case, we let

$$M(k/\mathbb{Q}, X) = |\{K \in \mathcal{F}(k),\ f(K/\mathbb{Q}) \leq X\}|\ .$$

The main result of [14] is then as follows:

**Theorem 1.8.8.** *Denote by $a_k(p)$ the number of copies of $\mathbb{Q}_p$ in $k\otimes\mathbb{Q}_p$ ($a_k(p) = 0$, 1 or 3 according to whether the number of prime ideals $\mathfrak{p}_i$ above $p$ in $k$ equals 1, 2 or 3). We have*

$$M(k/\mathbb{Q}, X) = C(k/\mathbb{Q})X + O(X^{1/2+\varepsilon}) \quad \textit{with}$$
$$C(k/\mathbb{Q}) = \frac{1}{g(k)}\frac{c_2(k)}{2^{4+r_2(k)}}\prod_{p\neq 2}\left(1+\frac{a_k(p)}{p}\right)\left(1-\frac{1}{p}\right)\ ,$$

*where*

$$c_2(k) = \begin{cases} 11 & \text{if } 2\mathbb{Z}_k = \mathfrak{p}_1 \\ 14 & \text{if } 2\mathbb{Z}_k = \mathfrak{p}_1^3 \\ 15 & \text{if } 2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2 \\ 16 & \text{if } 2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2 \text{ and } v_2(d(k)) = 3 \\ 18 & \text{if } 2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2 \text{ and } v_2(d(k)) = 2 \\ 23 & \text{if } 2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \end{cases}$$

The similarities are striking.

### 1.8.5 An Exact Result when $D < 0$ and $3 \nmid h(D)$

It is interesting to note that when $D < 0$ and $3 \nmid h(D)$, one can prove that nontrivial characters do not occur in the above formulas, so that $\phi_D(s) = 0$, thus giving exact formulas for the Dirichlet series. This is based on the following proposition.

**Proposition 1.8.9.** *Assume that $K_2 = \mathbb{Q}(\sqrt{D})$ with $D < 0$, $D \neq -3$, and $3 \nmid h(D) = |Cl(K_2)|$. Then for any ideal $\mathfrak{b} \in \mathcal{B}$ occurring in the sum of Theorem 1.6.1, the group $G_{\mathfrak{b}} = (Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]$ is trivial.*

*Proof.* An important theorem of Scholz ([47]) says that if $D<0$ is a negative fundamental discriminant different from $-3$ we have

$$0 \le \mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{D}))) - \mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{-3D}))) \le 1$$

and that $\mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{D}))) = \mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{-3D})))$ if and only if $\varepsilon$ is not 3-primary, in other words if and only if $\varepsilon$ is not a cube modulo $3\sqrt{-3}\mathbb{Z}_L$, where $L=\mathbb{Q}(\sqrt{D},\sqrt{-3})$, and where $\varepsilon$ is a fundamental unit of $\mathbb{Q}(\sqrt{-3D})$. Since in our case we assume that $\mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{D}))) = 0$, it follows that we also have $\mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{-3D}))) = 0$ and that $\varepsilon$ is not a cube modulo $3\sqrt{-3}\mathbb{Z}_L$.

We now consider the exact sequence of $\mathbb{F}_3[T]$-modules already used above in the computation of $f_{\alpha_0}(\mathfrak{b})$:

$$1 \longrightarrow S_{\mathfrak{b}}(L)[T] \longrightarrow S_3(L)[T] \longrightarrow \frac{Z_{\mathfrak{b}}}{Z_{\mathfrak{b}}^3}[T] \longrightarrow \frac{Cl_{\mathfrak{b}}(L)}{Cl_{\mathfrak{b}}(L)^3}[T] \longrightarrow \frac{Cl(L)}{Cl(L)^3}[T] \longrightarrow 1\ .$$

By Hasse's formula giving the class number of biquadratic number fields ([36]), we have $|Cl(L)| = 2^{-j}|Cl(K_2)||Cl(K_2')|$ with $j=0$ or 1, so in particular by Scholz's theorem we deduce that $3 \nmid |Cl(L)|$. We thus have the exact sequence

$$1 \longrightarrow S_{\mathfrak{b}}(L)[T] \longrightarrow S_3(L)[T] \longrightarrow \frac{Z_{\mathfrak{b}}}{Z_{\mathfrak{b}}^3}[T] \longrightarrow G_{\mathfrak{b}} \longrightarrow 1\ .$$

In addition, also since $3 \nmid |Cl(L)|$, $S_3(L)$ is an $\mathbb{F}_3$-vector space of dimension $r_1(L)+r_2(L)=2$, generated by the classes modulo cubes of $\rho$ and a fundamental unit $\varepsilon$ of $K_2'=\mathbb{Q}(\sqrt{-3D})$. The action of $\tau$ and $\tau_2$ is given by $\tau(\rho)=\rho^{-1}$, $\tau_2(\rho)=\rho$, $\tau(\varepsilon)=\pm\varepsilon^{-1}$, $\tau_2(\varepsilon)=\pm\varepsilon^{-1}$ (where $\pm=\mathcal{N}_{K_2'/\mathbb{Q}}(\varepsilon)$), and modulo cubes the $\pm$ signs disappear. Since $T=\{\tau+1,\tau_2+1\}$, it follows that $S_3(L)[T]$ is a 1-dimensional $\mathbb{F}_3$-vector space generated by the class of $\varepsilon$.

Since $G_{\mathfrak{b}}$ maps surjectively onto $G_{\mathfrak{b}'}$ for $\mathfrak{b}' \mid \mathfrak{b}$, it is sufficient to consider $\mathfrak{b}=3\sqrt{-3}$. In that case, we have seen that $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|=3$ in all cases, and since we have just shown that $|S_3(L)[T]|=3$, by the above exact sequence it follows that $G_{\mathfrak{b}}$ is trivial if and only if $S_{\mathfrak{b}}(L)[T]$ is trivial, hence by definition if and only if $\varepsilon$ is not congruent to a cube modulo $\mathfrak{b}_z=3\sqrt{-3}\mathbb{Z}_L$, which is exactly the second statement of Scholz's theorem, proving the proposition. □

**Remark.** The same proof shows the following result for $D>0$: if $D>0$ and $3 \nmid h(D')$, where as usual $D'=-3D$ if $3 \nmid D$ and $D'=-D/3$ if $3 \mid D$, then $G_{\mathfrak{b}}$ is canonically isomorphic to $(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]$, hence has order 1 unless $\mathfrak{b}=3\sqrt{-3}$ or $3 \nmid D$ and $\mathfrak{b}=3\mathbb{Z}_L$, in which case it has order 3.

**Corollary 1.8.10.** *Under the same assumptions, we have*

$$\sum_{K\in\mathcal{F}(K_2)} \frac{1}{f(K/\mathbb{Q})^s} = -\frac{1}{2} + \frac{1}{2}L_3(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1+\frac{2}{p^s}\right)\ ,$$

*where*

$$L_3(s) = \begin{cases} 1+2/3^{2s} & \text{if } 3 \nmid D, \\ 1+2/3^s & \text{if } D \equiv 3 \pmod 9, \\ 1+2/3^s+6/3^{2s} & \text{if } D \equiv 6 \pmod 9. \end{cases}$$

*Proof.* Clear from the proposition. □

**Examples.**

$$\sum_{K\in\mathcal{F}(\mathbb{Q}(\sqrt{-1}))}\frac{1}{f(K/\mathbb{Q})^s}=-\frac{1}{2}+\frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{12}{p}\right)=1}\left(1+\frac{2}{p^s}\right),$$

$$\sum_{K\in\mathcal{F}(\mathbb{Q}(\sqrt{-2}))}\frac{1}{f(K/\mathbb{Q})^s}=-\frac{1}{2}+\frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{24}{p}\right)=1}\left(1+\frac{2}{p^s}\right),$$

$$\sum_{K\in\mathcal{F}(\mathbb{Q}(\sqrt{-6}))}\frac{1}{f(K/\mathbb{Q})^s}=-\frac{1}{2}+\frac{1}{2}\left(1+\frac{2}{3^{s}}\right)\prod_{\left(\frac{8}{p}\right)=1}\left(1+\frac{2}{p^s}\right),$$

$$\sum_{K\in\mathcal{F}(\mathbb{Q}(\sqrt{-21}))}\frac{1}{f(K/\mathbb{Q})^s}=-\frac{1}{2}+\frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{\substack{\left(\frac{28}{p}\right)=1\\ p\neq 3}}\left(1+\frac{2}{p^s}\right).$$

## 1.9 Special Cases: $k$ Imaginary Quadratic

### 1.9.1 Case (1): $k=\mathbb{Q}(\sqrt{-3})$, Cyclic Cubic Extensions

Here $k=K_2=L=\mathbb{Q}(\sqrt{-3})$. By Lemma 1.5.5 we have $|(U(L)/U(L)^3)[T]|=3$, $[k:\mathbb{Q}]=2$, and if $\mathfrak{p}_3=\sqrt{-3}\mathbb{Z}_k$ is the unique ideal above 3, the possible ideals $\mathfrak{b}_z$ are $\mathfrak{p}_3^j$ for $j=0$, 1, 2 and 3, with corresponding ideals $\mathfrak{c}_z$ equal to $\mathbb{Z}_k$, $\mathfrak{p}_3$, $\mathfrak{p}_3$ and $\mathfrak{p}_3$. Thus, $|\mathfrak{c}_z/\mathfrak{b}_z|=1$, 1, 3, 9, so by Lemma 1.5.7 we have $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|=1$, 1, 3, 9. Since $e(\mathfrak{p}_3/3)=2$, $\mathfrak{r}^e(\mathfrak{b})$ is equal to $\mathfrak{p}_3$, $\mathbb{Z}_k$, $\mathbb{Z}_k$ and $\mathbb{Z}_k$, and we have respectively $\lceil\mathcal{N}\rceil(\mathfrak{b})^s=1$, $3^s$, $3^{2s}$, $3^{3s}$, $\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s=3^s$, 1, 1, 1, and $P_{\mathfrak{b}}(s)=1$, $1/3^s$, $1/3^s-1/3^{2s}$, $1-1/3^{2s}$. By Definition 1.2.9 we have $\mathcal{D}_3=\{\mathfrak{p}_3\}$, and $\mathcal{D}$ is the set of all primes $\mathfrak{p}$ of $k$, $\mathfrak{p}\nmid 3\mathbb{Z}_k$.

If $\chi=\chi_0$ is the trivial character, we thus have $F(\mathfrak{p}_3^j,\chi_0,s)=F(s)=\prod_{\mathfrak{p}\nmid 3\mathbb{Z}_k}(1+2/\mathcal{N}(\mathfrak{p})^s)$ for $j\geq 1$, while $F(\mathbb{Z}_{K_2},\chi_0,s)=2F(s)$. Thus the contribution of the trivial character is equal to

$$\begin{aligned}\Phi_0(s)&=\frac{3/2}{3^{3s}}\frac{(1,3^s,3^{2s},3^{3s})(2,1/3^s,1/3^s-1/3^{2s},1-1/3^{2s})}{(3^s,1,1,1)(1,1,3,9)}F(s)\\&=\frac{1}{6}\left(1+\frac{2}{3^{2s}}+\frac{6}{3^{3s}}+\frac{18}{3^{4s}}\right)\prod_{\mathfrak{p}\nmid 3\mathbb{Z}_k}\left(1+\frac{2}{\mathcal{N}(\mathfrak{p})^s}\right)\\&=\frac{1}{6}\left(1+\frac{2}{3^{2s}}+\frac{6}{3^{3s}}+\frac{18}{3^{4s}}\right)\prod_{\substack{p\in\mathbb{Z}\\ p\equiv 1\pmod 3}}\left(1+\frac{2}{p^s}\right)^2\prod_{\substack{p\in\mathbb{Z}\\ p\equiv 2\pmod 3}}\left(1+\frac{2}{p^{2s}}\right).\end{aligned}$$

An easy computation shows that the group $G_{\mathfrak{b}}$ is trivial for $\mathfrak{b}=\mathfrak{p}_3^j$ with $0\leq j\leq 2$, but has order 3 for $\mathfrak{b}=\mathfrak{p}_3^3$, Thus, we must simply add the contribution of the two conjugate nontrivial characters of order 3 of $G_{\mathfrak{p}_3^3}$. By definition, if $\chi$ is one of these characters we have

$$F(\mathfrak{p}_3^3,\chi,s)=\prod_{\mathfrak{p}\equiv x^3\pmod{\mathfrak{p}_3^3}}(1+2/\mathcal{N}(\mathfrak{p})^s)\prod_{\mathfrak{p}\not\equiv x^3\pmod{\mathfrak{p}_3^3}}(1-1/\mathcal{N}(\mathfrak{p})^s),$$

but the condition $\mathfrak{p} \equiv x^3 \pmod{\mathfrak{p}_3^3}$ is equivalent to $p \equiv \pm 1 \pmod 9$ for $p \in \mathbb{Q}$ below $\mathfrak{p}$. So we obtain

$$F(\mathfrak{p}_3^3, \chi, s) = \prod_{p \equiv 1 \pmod 9} (1 + 2/p^s)^2 \prod_{p \equiv -1 \pmod 9} (1 + 2/p^{2s}) \prod_{p \equiv 4,7 \pmod 9} (1 - 1/p^s)^2 \prod_{p \equiv 2,5 \pmod 9} (1 - 1/p^{2s}) ,$$

**Proposition 1.9.1.** *We have*

$$\sum_{K/k \text{ cyclic cubic}} \frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s} = -\frac{1}{2} + \frac{1}{6}\left(1 + \frac{2}{3^{2s}} + \frac{6}{3^{3s}} + \frac{18}{3^{4s}}\right) \prod_{\mathfrak{p} \nmid 3} \left(1 + \frac{2}{\mathcal{N}(\mathfrak{p})^s}\right) + \frac{1}{3}\left(1 - \frac{1}{3^{2s}}\right) \prod_{p \equiv 1 \pmod 9} (1 + 2/p^s)^2 \prod_{p \equiv -1 \pmod 9} (1 + 2/p^{2s}) \prod_{p \equiv 4,7 \pmod 9} (1 - 1/p^s)^2 \prod_{p \equiv 2,5 \pmod 9} (1 - 1/p^{2s}) .$$

**Corollary 1.9.2.** *If, as above, $M(k/k, X)$ denotes the number of cyclic cubic fields $K$ up to isomorphism with $\mathcal{N}(\mathfrak{f}(K/k)) \le X$, for all $\varepsilon > 0$ we have*

$$M(k/k, X) = C(k/k)X(\log(X) + D(k/k) - 1) + O(X^{\alpha+\varepsilon}) ,$$

*where*

$$C(\mathbb{Q}(k/k)) = \frac{1}{6} \prod_{\mathfrak{p} \subset k} \left(1 - \frac{3}{\mathcal{N}(\mathfrak{p})^2} + \frac{2}{\mathcal{N}(\mathfrak{p})^3}\right) (\mathrm{Res}_{s=1}\, \zeta_k(s))^2$$
$$= 0.05190499954455928914450029880481725 2\ldots$$
$$D(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) = 2\gamma_k - \log(3) + 12 \sum_{p \neq 3} \frac{\log(p)}{(p^{2r_3(p)} + p^{r_3(p)} - 2)}$$
$$= 1.44760703753609353771453588087483606 6\ldots ,$$

*where $r_3(p)$ is the class modulo 3 of $p$, i.e. 1 or 2, $\gamma_k = \lim_{s \to 1} \left(\frac{\zeta_k(s)}{\mathrm{Res}_{s=1}\, \zeta_k(s)} - \frac{1}{s-1}\right)$ and the sum is over all primes including $p = 3$.*

### 1.9.2 Case (3): $k = \mathbb{Q}(\sqrt{-3})$, $[K_2 : k] = 2$

Here $k = \mathbb{Q}(\sqrt{-3})$, $K_2 = L = \mathbb{Q}(\sqrt{-3}, \sqrt{D})$. By Lemma 1.5.5 we have $|(U(L)/U(L)^3)[T]| = 3$, $[k : \mathbb{Q}] = 2$, let $\mathfrak{p}_3 = \sqrt{-3}\mathbb{Z}_k$ be the unique ideal above 3, which is ramified, and $\mathfrak{P}_3$ an ideal of $L$ above $\mathfrak{p}_3$. Then $\mathfrak{p}_3$ can be inert or decomposed in $L/k$. The possible ideals $\mathfrak{b}_z$ are $(\mathfrak{p}_3\mathbb{Z}_L)^j$ for $j = 0$, 1, 2 and 3, with corresponding ideals $\mathfrak{c}_z$ equal to $\mathbb{Z}_L$, $\mathfrak{p}_3\mathbb{Z}_L$, $\mathfrak{p}_3\mathbb{Z}_L$ and $\mathfrak{p}_3\mathbb{Z}_L$. Thus, $|\mathfrak{c}_z/\mathfrak{b}_z| = 1$, 1, $3^2$, $3^4$, and $|\mathfrak{c}_z \cap k/\mathfrak{b}_z \cap k| = 1$, 1, 3, $3^2$ so by Lemma 1.5.7 we have $|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| = 1$, 1, 3, 9. Since $e(\mathfrak{p}_3/3) = 2$, $\mathfrak{r}^e(\mathfrak{b})$ is equal to $\mathfrak{P}_3$, $\mathbb{Z}_L$, $\mathbb{Z}_L$ and $\mathbb{Z}_L$, and we have respectively $\lceil \mathcal{N} \rceil(\mathfrak{b})^s = 1$, $3^s$, $3^{2s}$, $3^{3s}$, $\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s = 3^s$, 1, 1, 1, and $P_\mathfrak{b}(s) = 1$, $1/3^s$, $1/3^s - 1/3^{2s}$, $1 - 1/3^s$. But $\mathfrak{P}_3 \mid \mathfrak{d}_3$ if and only if $\mathfrak{p}_3$ is decomposed in $L/k$

So if $\mathfrak{p}_3$ is decomposed in $L/k$ we obtain that the contribution of the trivial character is

$$\begin{aligned}\Phi_0(s) &= \frac{3}{2\cdot 3^{3s}}\frac{(1,3^s,3^{2s},3^{3s})(2,1/3^s,1/3^s-1/3^{2s},1-1/3^{2s})}{(3^s,1,1,1)(1,1,3,9)}F(s)\\ &= \frac{1}{6}\left(1+\frac{2}{3^{2s}}+\frac{6}{3^{3s}}+\frac{18}{3^{4s}}\right)\prod_{\mathfrak{p}\in\mathcal{D}_3}\left(1+\frac{2}{\mathcal{N}(\mathfrak{p})^s}\right)\ .\end{aligned}$$

while if $\mathfrak{p}_3$ is inert in $L/k$ we obtain

$$\begin{aligned}\Phi_0(s) &= \frac{3}{2\cdot 3^{3s}}\frac{(3^s,3^{2s},3^{3s})(1/3^s,1/3^s-1/3^{2s},1-1/3^{2s})}{(1,1,1)(1,3,9)}F(s)\\ &= \frac{1}{6}\left(1+\frac{2}{3^{2s}}+\frac{6}{3^{3s}}\right)\prod_{\mathfrak{p}\in\mathcal{D}_3}\left(1+\frac{2}{\mathcal{N}(\mathfrak{p})^s}\right)\ .\end{aligned}$$

**Proposition 1.9.3.** *Let $k=\mathbb{Q}(\sqrt{-3})$, let $D$ be a fundamental discriminant with $D\neq -3$, let $K_2=L=\mathbb{Q}(\sqrt{-3},\sqrt{D})$. There exists a function $\phi_D(s)$ holomorphic for $\mathrm{Re}(s)>1/2$ such that*

$$\sum_{K\in\mathcal{F}(K_2)}\frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s}=\phi_D(s)+\frac{1}{6}L_3(s)\prod_{\mathfrak{p}\in\mathcal{D}_3}\left(1+\frac{2}{\mathcal{N}(\mathfrak{p})^s}\right)\ ,$$

*where*

$$L_3(s)=\begin{cases}1+2/3^{2s}+6/3^{3s}+18/3^{4s} & \text{if } \left(\frac{D}{3}\right)=1\\ 1+2/3^{2s}+6/3^{3s} & \text{if } \left(\frac{D}{3}\right)=-1.\end{cases}$$

**Corollary 1.9.4.** *If, as above, $M(K_2/k,X)$ denotes the number of cyclic cubic fields $K$ up to isomorphism with $\mathcal{N}(\mathfrak{f}(K/k))\le X$, for all $\varepsilon>0$ we have*

$$\begin{aligned}&M(K_2/k,X)=C(K_2/k)X+O(X^{\alpha+\varepsilon}) \quad \textit{with}\\ &C(K_2/k)=\ell_3\frac{1}{\zeta_k(2)}\prod_{\mathfrak{p}\mid D}\left(1-\frac{1}{\mathcal{N}(\mathfrak{p})+1}\right)\prod_{\mathfrak{p}\in\mathcal{D}}\left(1-\frac{2}{\mathcal{N}(\mathfrak{p})(\mathcal{N}(\mathfrak{p})+1)}\right)\ ,\end{aligned}$$

*where*

$$\ell_3=\begin{cases}5/18 & \text{if } \left(\frac{D}{3}\right)=1\\ 13/54 & \text{if } \left(\frac{D}{3}\right)=-1\end{cases}$$

### 1.9.3 Case (4): $k$ Imaginary Quadratic

As additional examples, we now assume that $k$ is an imaginary quadratic field of discriminant $D<0$, and we will in addition assume that 3 is inert in $k$, in other words that $\left(\frac{D}{3}\right)=-1$. It is of course not difficult to treat the other cases. Note that this assumption implies that $\rho\notin k$. In these examples, we will only compute $C(K_2/k)$.

Once again we have $3\mathbb{Z}_L = \mathfrak{p}_3^2$ with $\mathfrak{p}_3 = \sqrt{-3}\mathbb{Z}_L$, and the only possible ideals $\mathfrak{b}$ are $\mathfrak{p}_3^j$ with $0 \le j \le 3$. With standard notation we have $\mathrm{Res}_{s=1}\,\zeta_k(s) = 2\pi h(D)/(w(D)\sqrt{|D|})$, so

$$C(K_2/k) = \frac{\pi^2 h(D)^2}{66(w(D)/2)^2|D|} \prod_{\mathfrak{p}\subset k} \left(1 - \frac{3}{\mathcal{N}(\mathfrak{p})^2} + \frac{2}{\mathcal{N}(\mathfrak{p})^3}\right)(S_0 + S_1 + S_2 + S_3)\,,$$

where $S_j$ is the contribution of $\mathfrak{b} = \mathfrak{p}_3^j$. We have $S_0 = 2/3$, $S_1 = 1$, $S_2 = 9(1/3 - 1/9) = 2$, $S_3 = 27(1 - 1/9)/9 = 8/3$, so $S_0 + S_1 + S_2 + S_3 = 19/3$, so we obtain

$$\begin{aligned} C(K_2/k) &= \frac{19\pi^2 h(D)^2}{198(w(D)/2)^2|D|} \prod_{\mathfrak{p}\subset k} \left(1 - \frac{3}{\mathcal{N}(\mathfrak{p})^2} + \frac{2}{\mathcal{N}(\mathfrak{p})^3}\right) \\ &= \frac{19\pi^2 h(D)^2}{198(w(D)/2)^2|D|} \prod_{p\mid D} \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right) \\ &\quad \prod_{\left(\frac{D}{p}\right)=-1} \left(1 - \frac{3}{p^4} + \frac{2}{p^6}\right) \prod_{\left(\frac{D}{p}\right)=1} \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right)^2 . \end{aligned}$$

# Chapter 2

# An algorithm to compute relative cubic fields

## 2.1 General case

### 2.1.1 Introduction

Let $L/K$ be an extension of number fields. We define $\mathcal{F}_{K,n}(X)$ to be the set of isomorphism classes of extensions $L/K$ such that

$$[L:K] = n, \quad \text{and} \quad \mathcal{N}_{K/\mathbb{Q}}\mathfrak{d}(L/K) \leq X,$$

where $\mathfrak{d}(L/K)$ is the relative discriminant ideal of the extension $L/K$.

Our objective is to generalize Belabas's [2] algorithm for listing all representatives of $\mathcal{F}_{K,n}(X)$. In particular we consider the case when $K$ is an imaginary quadratic number field and $n = 3$, and we will solve it completely when $K$ has class number 1.

**Theorem 2.1.1.** *Let $K$ be an imaginary quadratic number field with class number $h_K = 1$. There exists an algorithm which lists all cubic extensions in $\mathcal{F}_{K,3}(X)$ in time $O_\varepsilon(X^{1+\varepsilon})$, for all $\varepsilon > 0$.*

[27, Theorem I.1] tells us that the number of such classes is of the order of $X$. So

**Corollary 2.1.2.** *The algorithm runs in time almost linear in the size of the output.*

We made an implementation in PARI/GP for the case $K = \mathbb{Q}(i)$ which can be easily adapted for any imaginary quadratic number field with class number 1.

### 2.1.2 Taniguchi's theorem

To generalize Belabas's algorithm we need a theorem by Taniguchi [50], adapting Davenport-Heilbronn [26] theory to cubic algebras.

**Definition 2.1.3.** *Let $\mathcal{O}$ be a Dedekind domain, and $K$ be its quotient field.*

- *Let $\mathcal{C}(\mathcal{O})$ be the set of "cubic algebras" that is, isomorphisms classes of $\mathcal{O}$-algebras that are projective of rank 3 as $\mathcal{O}$-modules.*

- *For every fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ we define*

$$\mathcal{C}(\mathcal{O},\mathfrak{a}) = \{R \in \mathcal{C}(\mathcal{O}) \mid \mathrm{St}(R) = \overline{\mathfrak{a}}\},$$

*where $\mathrm{St}(R) \in Cl(\mathcal{O})$ is the Steinitz class of $R$, thus $R$ will be of the form $\omega_1\mathcal{O} \oplus \omega_2\mathcal{O} \oplus \omega_3\mathfrak{a}$, for appropriate $\omega_1, \omega_2, \omega_3 \in \mathrm{Frac}(R) := R \otimes_{\mathcal{O}} K$. Let further*

$$G_{\mathfrak{a}} = \left\{ \begin{pmatrix} \alpha \in \mathcal{O} & \beta \in \mathfrak{a}^{-1} \\ \gamma \in \mathfrak{a} & \delta \in \mathcal{O} \end{pmatrix} \;\middle|\; \alpha\delta - \beta\gamma \in \mathcal{O}^{\times} \right\},$$

$$V_{\mathfrak{a}} = \{F = (a,b,c,d) \mid a \in \mathfrak{a}, b \in \mathcal{O}, c \in \mathfrak{a}^{-1}, d \in \mathfrak{a}^{-2}\}.$$

- *If $F \in V_{\mathfrak{a}}$, its discriminant $\mathrm{disc}(F) = b^2c^2 - 27a^2d^2 + 18abcd - 4ac^3 - 4b^3d$ belongs to $\mathfrak{a}^{-2}$.*

- *We consider elements of $V_{\mathfrak{a}}$ as binary cubic forms so $(a,b,c,d) = ax^3 + bx^2y + cxy^2 + dy^3$ and we define the action of $G_{\mathfrak{a}}$ on $V_{\mathfrak{a}}$ by*

$$M \cdot F = (\det M)^{-1} F(\alpha x + \gamma y, \beta x + \delta y),$$

*where $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G_{\mathfrak{a}}$.*

**Theorem 2.1.4** (Taniguchi)**.** *There exists a canonical bijection between $\mathcal{C}(\mathcal{O},\mathfrak{a})$ and $V_{\mathfrak{a}}/G_{\mathfrak{a}}$ such that the following diagram is commutative:*

$$\begin{array}{ccc} V_{\mathfrak{a}}/G_{\mathfrak{a}} & \longrightarrow & \mathcal{C}(\mathcal{O},\mathfrak{a}) \\ {\scriptstyle \mathrm{disc}}\downarrow & & \downarrow{\scriptstyle \mathfrak{d}} \\ \mathfrak{a}^{-2}/(\mathcal{O}^{\times})^2 & \xrightarrow{\times\mathfrak{a}^2} & \{ \textit{ integral ideals of } \mathcal{O}\} \end{array},$$

*where $\mathfrak{d}$ is the relative discriminant ideal map.*

**Remark**. Note that $\mathfrak{d}$ is well-defined since an $\mathcal{O}$-algebras isomorphism preserves the discriminant.

See Appendix A for a proof of this result.

**Remark**. In particular, when $\mathcal{O}$ is the maximal order of a number field $K$ with class number $h_K = 1$, then Taniguchi's bijection simplifies to a bijection between binary cubic forms with coefficients in $\mathcal{O}$ modulo $\mathrm{GL}_2(\mathcal{O})$ and cubic $\mathcal{O}$-algebras.

To enumerate relative cubic extensions $L/K$, we shall select only the cubic $\mathcal{O}$-algebras $R$ which are both integral domains (so that their ring of fractions is a field), and maximal orders : those maximal algebras are exactly the classes of the $\mathcal{O}_L$. $R$ is a domain if and only if $F$ is irreducible. Maximality is a local property, therefore we need to test $\mathfrak{p}$-maximality at all prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ such that $\mathfrak{p}^2 \mid \mathfrak{d}(R)$ and this can done with a generalization of Dedekind's criterion :

**Proposition 2.1.5** (relative Dedekind's criterion)**.** *[12, Theorem 2.4.8] Let $L/K$ be an extension of number fields, $L = K(\theta)$, $\theta$ an algebraic integer with minimal polynomial $T(x) \in \mathcal{O}_K[x]$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, let $\beta$ be a uniformizer of $\mathfrak{p}^{-1}$, i. e. $\beta \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$. Let $\overline{T(x)} = \prod_{1\leq i\leq k} \overline{T_i(x)}^{e_i}$ be the factorization of $\overline{T(x)} \in (\mathcal{O}_K/\mathfrak{p})[x]$, with $T_i(x)$ monic belonging to $\mathcal{O}_K[x]$. Let*

$$g(x) = \prod_{1\leq i\leq k} T_i(x), \quad h(x) = \prod_{1\leq i\leq k} T_i(x)^{e_i-1},$$

*then $g(x)h(x) - T(x) \in \mathfrak{p}[x]$. Let $f(x) = \beta(g(x)h(x) - T(x)) \in \mathcal{O}_K[x]$. Then $\mathcal{O} = \mathcal{O}_K[\theta]$ is $\mathfrak{p}$-maximal if and only if $\gcd(\overline{f}, \overline{g}, \overline{h}) = 1$ in $(\mathcal{O}_K/\mathfrak{p})[x]$.*

### 2.1.3 Reduction of binary cubic forms

Let $K$ be an imaginary quadratic field. Let $\mathcal{O}$ be its ring of integers.

We want a reduction theory for binary cubic forms of $(\mathrm{Sym}^3 \mathcal{O}^2)^*$, i.e.

$$F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3, \quad a, b, c, d \in \mathcal{O}$$

modulo the action of $\mathrm{SL}_2(\mathcal{O})$, given by:

$$M \cdot F = F(Ax + By, Cx + Dy), \quad \text{for each } M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}).$$

**Remark**. This is not, in general, the reduction asked by Taniguchi's Theorem, but we will see later, that it is sufficient for the case $h_K = 1$.

#### The covariant $H_F$

**Definition 2.1.6.** *Let $F$ be an irreducible binary cubic form (in particular its first coefficient $a \neq 0$). We associate to $F$ the positive definite binary Hermitian form*

$$H_F = t_1^2|x - \alpha_1 y|^2 + t_2^2|x - \alpha_2 y|^2 + t_3^2|x - \alpha_3 y|^2,$$

*where*

$$F(x, 1) = a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3), \text{ and}$$

$$t_i^2 = |a|^2|\alpha_j - \alpha_k|^2, \quad i, j, k \text{ pairwise distinct.}$$

**Lemma 2.1.7.** *We have*

$$(t_1t_2t_3)^2 = |a|^2|\operatorname{disc}(F)| \tag{2.1}$$

*Proof.* Straightforward from definition 2.1.6 and the definition of discriminant of a polynomial. □

The following two lemmas also follow from a direct computation:

**Lemma 2.1.8.** *We have*

$$H_F(x, y) = P|x|^2 + Qx\overline{y} + \overline{Q}\overline{x}y + R|y|^2,$$

*where*

$$\begin{cases} P = t_1^2 + t_2^2 + t_3^2 \in \mathbb{R}^+ \\ Q = -(\alpha_1 t_1^2 + \alpha_2 t_2^2 + \alpha_3 t_3^2) \in \mathbb{C} \\ R = |\alpha_1|^2 t_1^2 + |\alpha_2|^2 t_2^2 + |\alpha_3|^2 t_3^2 \in \mathbb{R}^+. \end{cases}$$

**Lemma 2.1.9.** *Let* $\Delta = -\operatorname{disc}(H_F) = PR - |Q|^2$ *and* $D = \operatorname{disc}(F)$. *Then*

$$\Delta = 3|D|. \tag{2.2}$$

**Definition 2.1.10.** *We define* $[H_F]$ *to be the matrix :*

$$[H_F] = \begin{pmatrix} P & Q \\ \overline{Q} & R \end{pmatrix}.$$

*The group* $\mathrm{GL}_2(\mathbb{C})$ *acts on the space of binary Hermitian forms over* $\mathbb{C}$ *via:*

$$M \cdot [H_F] = M^* \times [H_F] \times M,$$

*where* $M^* = (\overline{M})^t$.

In particular, if $M \in \mathrm{GL}_2(\mathcal{O})$, then the discriminant of $H_F$ is preserved by this action.

**Proposition 2.1.11.** *The application which sends* $F$ *to* $H_F$ *is covariant, i. e.*

$$H_{M \cdot F} = M \cdot H_F.$$

*Proof.*
Just verify on generators of $\mathrm{SL}_2(\mathbb{C})$: $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, $\alpha \in \mathbb{C}$. □

Thanks to this property we can translate our problem of defining a unique reduced $F$ to the problem of finding a unique reduced covariant $H_F$ plus some extra conditions as we will see in Section 2.2.3.

**Definition 2.1.12.** *Let* $F = (a, b, c, d) \in (\mathrm{Sym}^3 \mathcal{O}^2)^*$ *be a binary cubic form with coefficients in* $\mathcal{O}$. *We say that* $F$ *is reduced if its covariant* $H_F$ *is reduced.*

In the rest of this section we will then define reduction for positive definite binary hermitian forms, and we will se that this notion is completely explicit in the case of imaginary quadratic number fields with class number 1.

### Hyperbolic 3-space

Let

$$\begin{aligned} \mathcal{H}_3 &= \{z + tj \mid z \in \mathbb{C}, t \in \mathbb{R}^+\} \\ &= \{h = z + tj \mid h \in \mathbb{H}, \text{ such that the } k - \text{component is } 0, t > 0\}, \end{aligned}$$

where $\mathbb{H}$ is the quaternions ring.

We define the action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathcal{H}_3$ by $M \cdot (z + tj) = (z' + t'j)$, with

$$\begin{cases} z' = \dfrac{\rho^2 A\overline{C} + zA\overline{D} + \overline{z}B\overline{C} + B\overline{D}}{\rho^2|C|^2 + zC\overline{D} + \overline{z}\overline{C}D + |D|^2} \\ t' = \dfrac{t}{\rho^2|C|^2 + zC\overline{D} + \overline{z}\overline{C}D + |D|^2}, \end{cases}$$

where $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$ and $\rho^2 = |z|^2 + t^2$. With the quaternion notations (and operations), this translates to the neater formula

$$M \cdot (h) = (Ah + B)(Ch + D)^{-1}.$$

Let

$$\begin{aligned} \mathscr{P} &= \{ \text{ positive definite binary quadratic Hermitian forms in } \mathbb{C}\} \\ &= \left\{ P|x|^2 + Qx\overline{y} + \overline{Q}\overline{x}y + R|y|^2 \,\middle|\, \begin{array}{l} P, R \in \mathbb{R}^+, Q \in \mathbb{C} \\ |Q|^2 - PR < 0 \end{array} \right\}, \end{aligned}$$

and let $\widetilde{\mathscr{P}} = \mathscr{P}/\mathbb{R}^+$ where $\mathbb{R}^+$ acts on $\mathscr{P}$ by multiplication.

Let, finally, $\Phi : \mathscr{P} \to \mathcal{H}_3$ defined by:

$$\Phi\left( \begin{pmatrix} P & Q \\ \overline{Q} & R \end{pmatrix} \right) = -\frac{Q}{P} + \frac{\sqrt{\Delta}}{P} j. \tag{2.3}$$

We have

$$\Phi(M \cdot H) = M \cdot (\Phi(H)), \qquad \text{for each } H \in \mathscr{P}, M \in \mathrm{SL}_2(\mathbb{C}).$$

More precisely, $\Phi$ induces a bijection $\widetilde{\Phi} : \widetilde{\mathscr{P}} \to \mathcal{H}_3$, wich commutes with the action of $\mathrm{SL}_2(\mathbb{C})$.

So, in particular, there is a bijection between orbits of $\mathcal{H}_3/\mathrm{SL}_2(\mathcal{O})$ and $\widetilde{\mathscr{P}}/\mathrm{SL}_2(\mathcal{O})$. As fundamental domains $\mathcal{F}$ for $\mathcal{H}_3$ modulo $\mathrm{SL}_2(\mathcal{O})$ are known, we can say:

$$H_F \text{ is reduced modulo } \mathrm{SL}_2(\mathcal{O}) \Leftrightarrow \Phi(H_F) \in \mathcal{F}.$$

From [31] we have an explicit description of fundamental domains of $\mathcal{H}_3$ modulo $\mathrm{PSL}(2, \mathcal{O})$:

**Definition 2.1.13.** *Let $K = \mathbb{Q}(\sqrt{D_K})$ with $D_K < 0$ a squarefree integer and $d_K$ the discriminant of $K$. We define*

$$\begin{aligned} \mathcal{F}_{\mathbb{Q}(i)} &= \left\{ z + tj \in \mathcal{H}_3 \colon 0 \le |\operatorname{Re}(z)| \le \frac{1}{2}, 0 \le \operatorname{Im}(z) \le \frac{1}{2}, |z|^2 + t^2 \ge 1 \right\}, \\ \mathcal{F}_{\mathbb{Q}(\sqrt{-3})} &= \left\{ z + tj \in \mathcal{H}_3 \colon z \in F_{\mathbb{Q}(\sqrt{-3})}, |z|^2 + t^2 \ge 1 \right\}, \end{aligned}$$

*where*

$$\begin{aligned} F_{\mathbb{Q}(\sqrt{-3})} &= \left\{ z \in \mathbb{C} \colon 0 \le \operatorname{Re}(z), \frac{\sqrt{3}}{3} \operatorname{Re}(z) \le \operatorname{Im}(z), \operatorname{Im}(z) \le \frac{\sqrt{3}}{3}(1 - \operatorname{Re}(z)) \right\} \\ &\quad \cup \left\{ z \in \mathbb{C} \colon 0 \le \operatorname{Re}(z) \le \frac{1}{2}, -\frac{\sqrt{3}}{3} \operatorname{Re}(z) \le \operatorname{Im}(z) \le \frac{\sqrt{3}}{3} \operatorname{Re}(z) \right\}. \end{aligned}$$

*And for $D \neq -3, -1$,*

$$\begin{aligned} \mathcal{F}_K &= \{ z + tj \in \mathcal{B}_K \colon z \in F_K \}, \textit{where} \\ \mathcal{B}_K &= \left\{ z + tj \in \mathcal{H}_3 \colon \begin{array}{l} |cz + d|^2 + |c|^2 t^2 \ge 1 \textit{ for all } c, d \in \mathcal{O} \\ \textit{with } \langle c, d \rangle = \mathcal{O} \end{array} \right\}, \\ F_K &= \left\{ z \in \mathbb{C} \colon 0 \le \operatorname{Re}(z) \le 1, 0 \le \operatorname{Im}(z) \le \sqrt{|d_K|}/2 \right\}. \end{aligned}$$

**Lemma 2.1.14.** *For all number fields $K$ we have*

$$[\mathrm{PGL}(2,\mathcal{O}_K):\mathrm{PSL}(2,\mathcal{O}_K)] = 2^{\dim_{\mathbb{F}_2}\left(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2\right)} = 2.$$

*Proof.* The exact sequence

$$1 \to \mathrm{SL}_2(\mathcal{O}) \to \mathrm{GL}_2(\mathcal{O}) \to \mathcal{O}^\times \to 1$$

induced by the determinant, gives rise to the exact sequence

$$1 \to \left\langle \mathcal{O}^\times \cdot \mathrm{Id}, \mathrm{SL}_2(\mathcal{O})\right\rangle \to \mathrm{GL}_2(\mathcal{O}) \to \mathcal{O}^\times/(\mathcal{O}^\times)^2 \to 1.$$

and, since for imaginary quadratic number field $K$, we have $\dim_{\mathbb{F}_2}\left(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2\right) = 1$, we can conclude. □

**Remark**. So when we consider fundamental domains of $\mathcal{H}_3$ modulo $\mathrm{GL}_2(\mathcal{O})$, we can take half of the fundamental domains above.

### 2.1.4 Bounds for the $t$-component of a reduced point in $\mathcal{H}_3$

Fundamental domains as given in the previous paragraph, give obvious bounds for the $z$-component of $(z,t) \in \mathcal{H}_3$.

Now we want to bound the $t$-component from below.

For that we need the following Proposition ([49],[31]):

**Proposition 2.1.15.** *There is a constant $\kappa \in ]0,\infty[$ only depending on $K$, such that for any $z \in \mathbb{C}\setminus K$ there are infinitely many $\lambda,\mu \in \mathcal{O}$ with*

$$\left|z - \frac{\lambda}{\mu}\right| \le \frac{\kappa}{|\mu|^2} \quad \text{and } \langle \mu,\lambda\rangle = \mathcal{O}$$

So for "big" $|\mu|$ we have $\frac{\kappa}{|\mu|} < 1$ and so $|z\mu - \lambda| \le \frac{\kappa}{|\mu|} < 1$.

But we know that if $z + tj \in \mathcal{F}_K$ we have $|z\mu-\lambda|^2 + t^2|\mu|^2 \ge 1$ and so we obtain $t \ge t_K$, for some $t_K$ depending only on $K$.

It remains to treat points $z + tj \in \mathcal{F}_K$, $z \in K$.

Let us define

$$S_K = \{z \in K \mid |z\mu+\lambda| \ge 1 \text{ for all } \langle\lambda,\mu\rangle = \mathcal{O}\}.$$

This set of *singular points* is finite modulo addition of an element of $\mathcal{O}$ (see [49, 31]). The $z + tj \in \mathcal{F}_K$ for $z \in S_K$ are the only points in $\mathcal{F}_K$ where there is no lower bound for $t$.

Fortunately, if $h_K = 1$, then $S_K = \emptyset$ : in fact if $z = \frac{\alpha}{\beta}$ with $\alpha,\beta$ coprime elements of $\mathcal{O}$ we just need to take $\mu = \beta$ and $\lambda = \alpha$ to get $|\mu z - \lambda| = 0$ with $\langle\lambda,\mu\rangle = \mathcal{O}$.

So when $h_K = 1$ we have always $t \ge t_K > 0$ for some $t_K$ depending only on $K$.

**Proposition 2.1.16.** *Let $K$ be an imaginary quadratic number field with class number $h_k = 1$. Then there exists a constant $t_K$, only depending on $K$, such that $t \ge t_K$ for every $(z,t) \in \mathcal{F}_K$.*

So from now on we will restrict to $K$ imaginary quadratic number field with class number $h_K = 1$.

## 2.2 Computing $t_K$ for all $K$ imaginary quadratic with $h_K = 1$

As we saw in section 2.1.4, when $h_K = 1$ it is possible to bound $|t|^2 \geq t_K^2$.

Let us give explicitly those $t_K^2$ for all the imaginary quadratic number fields with class number one.

**Theorem 2.2.1.** *Let $K = \mathbb{Q}(\sqrt{-D})$, for $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.*

*Then the value of $t_K^2$ is given in the following tables :*

| $D$ | 1 | 2 | 3 | 7 | 11 |
|---|---|---|---|---|---|
| $t_K^2$ | 1/2 | 1/4 | 2/3 | 3/7 | 2/11 |

| $D$ | 19 | 43 | 67 | 163 |
|---|---|---|---|---|
| $t_K^2$ | 2/19 | 2/43 | 2/67 | 2/163 |

*Proof.* The first table describes the Euclidean fields. In this case the computation of $t_K$ is very easy and we sketch it here (but it can also be found in more detail in [22]).

In fact, we only need to find the intersection of the three unit spheres centered in 0, 1 and $\omega$ where

$$\omega = \begin{cases} \sqrt{-D} & \text{when } -D \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{-D}}{2} & \text{when } -D \equiv 1 \pmod 4 \end{cases}$$

So we find that the intersection point $x = z + it$ has

$$z = \begin{cases} \frac{1+\sqrt{-D}}{2} & \text{when } -D \equiv 2, 3 \pmod 4 \\ \frac{1}{2} + \frac{(1-D)}{4\sqrt{-D}} & \text{when } -D \equiv 1 \pmod 4 \end{cases}$$

and we obtain $t_K$ from $t_K^2 = 1 - |z|^2$.

The second table concerns the non-Euclidean fields. For these we just refer to [53]. □

### 2.2.1 Bounds for a reduced binary Hermitian form

Once we know $t \geq t_K$ we can bound $P, Q$ and $R$:

**Lemma 2.2.2.** *Let $(P, Q, R) = P|x|^2 + Qx\overline{y} + \overline{Q}\overline{x}y + R|y|^2$ be a reduced Hermitian form in $\mathscr{P}$, with discriminant $\Delta = |Q|^2 - PR$. We have*

$$P \leq \frac{\sqrt{\Delta}}{t_K}. \tag{2.4}$$

$$|Q|^2 \leq c_K P^2, \tag{2.5}$$

*for a constant $c_K$ depending only on the number field $K$, and*

$$PR \leq \left(1 + \frac{c_K}{t_K^2}\right)\Delta \tag{2.6}$$

*Proof.* For (2.4) just recall that $t = \sqrt{\Delta}/P$ by the definition of $\Phi$ in (2.3) and $t \geq t_K$.

Thanks to the bounds on $\mathrm{Re}\,(z)$ and $\mathrm{Im}\,(z)$ given in the description of the fundamental domain $\mathcal{F}$ (in Definition 2.1.13) we get

- $0 \leq |\mathrm{Re}(Q)| \leq P/2$, $0 \leq \mathrm{Im}(-Q) \leq 1/2$, and so $|Q|^2 \leq P^2/2$ when $K = \mathbb{Q}(i)$;
- $0 \leq \mathrm{Re}(-Q) \leq P/2$, $-\sqrt{3}/6P \leq \mathrm{Im}(-Q) \leq \sqrt{3}/3P$ and then $|Q|^2 \leq 7/12P^2$, when $K = \mathbb{Q}(\sqrt{-3})$
- $0 \leq \mathrm{Re}(-Q) \leq P/2, 0 \leq \mathrm{Im}(-Q)| \leq \frac{\sqrt{|d_K|}}{2} P$ and then $|Q|^2 \leq \left(\frac{1+|d_K|}{4}\right) P^2$

So in all the cases we have

$$|Q|^2 \leq c_K P^2 \leq c_K \frac{\Delta}{t_K^2},$$

for $c_K = \left(\frac{1+|d_K|}{4}\right)$ Finally, we have

$$PR - |Q|^2 = \Delta,$$

so we obtain

$$PR \leq \left(1 + \frac{c_K}{t_K^2}\right) \Delta$$

□

### 2.2.2 Bounds for reduced binary cubic forms

In this section, we are going to give bounds for the coefficients of reduced binary cubic forms, which allow us to loop on all reduced binary cubic forms in time $\widetilde{O}(X)$. Let $K$ be an imaginary quadratic fields of class number 1 and $\mathcal{O} = \mathcal{O}_K$.

**Theorem 2.2.3.** *Let $F = (a, b, c, d)$ be an irreducible binary cubic form with coefficients in $\mathcal{O}$ which is reduced modulo $\mathrm{SL}_2(\mathcal{O})$. Let $|\mathrm{disc}(F)| \leq D$. Then*

$$|a| \leq \left(\frac{\alpha}{\sqrt{3}}\right)^{3/2} D^{1/4}; \quad |b| \leq 3\gamma^{1/2} D^{1/4}$$

$$|ad| \leq \beta^{3/2} D^{1/2}; \quad |bc| \leq 9(3\beta)^{3/2} D^{1/2}; \quad |ac| \leq 3\gamma D^{1/2}.$$

*Where $\alpha = 1/t_K$, $\beta = \left(1 + \frac{c_K}{t_K^2}\right)$, $\gamma = \frac{\alpha\beta\sqrt{27}}{4}$.*

*Proof.* Let $H = (P, Q, R) \in \mathscr{P}$ be a reduced (positive definite) binary hermitian form. Then

$$\begin{cases} P \leq R \\ |\mathrm{Re}(Q)| \leq P/2 \\ |\mathrm{Im}(Q)| \leq \sqrt{|d_K|} P/2. \end{cases}$$

(remark that reduction conditions may be stricter than these ones, so $(P, Q, R)$ satisfying this bounds is not always a reduced Hermitian form). Using the results of Lemma 2.2.2 we obtain:

$$P \leq \alpha\sqrt{\Delta} \text{ and } PR \leq \beta\Delta. \tag{2.7}$$

where $\alpha = 1/t_K$ and $\beta = \left(1 + \frac{c_K}{t_K^2}\right)$. Moreover

$$t_i^2|\alpha_i|^2 \leq R, \quad \text{and} \quad t_j t_k \leq \frac{1}{2}(t_j^2 + t_k^2) \leq \frac{P}{2}. \tag{2.8}$$

It follows that

$$|\alpha_i|^2 \leq \left(\frac{P}{2}\right)^2 R\frac{1}{t_1^2 t_2^2 t_3^2}, \text{ for all } i \in \{1, 2, 3\}. \tag{2.9}$$

From (2.7) and (2.8) we obtain

$$|\alpha_i|^2 \leq \frac{\alpha\beta\sqrt{27}}{4}\frac{\sqrt{D}}{|a|^2}$$

So we have

$$|\alpha_i| \leq \gamma^{1/2}\frac{D^{1/4}}{|a|}, \tag{2.10}$$

where $\gamma = \frac{\alpha\beta\sqrt{27}}{4}$. Thanks to the last formula, we can bound $|b|$:

$$|b| = |a(-\alpha_1 - \alpha_2 - \alpha_3)| \leq 3\gamma^{1/2}D^{1/4}. \tag{2.11}$$

In the same way

$$|c| = |a|\,|\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3| \leq 3\gamma\frac{\sqrt{D}}{|a|}$$

so

$$|ac| \leq 3\gamma\sqrt{D} \tag{2.12}$$

We can also bound $|a|$. In fact, using the AGM inequality we have

$$3(a^2D)^{1/3} = 3(t_1^2t_2^2t_3^2)^{1/3} \leq t_1^2 + t_2^2 + t_3^2 = P. \tag{2.13}$$

We know that $P \leq \sqrt{3}\alpha\sqrt{D}$ and $t_1^2t_2^2t_3^2 = |a|^2D$ so we obtain

$$|a| \leq \left(\frac{\alpha}{\sqrt{3}}\right)^{3/2} D^{1/4}.$$

Now we need to bound $|ad|$ and $|bc|$. From (2.13) we obtain

$$|a|^2 \leq \frac{P^3}{3^3D}.$$

Then

$$|a|^2R^3 \leq \frac{P^3R^3}{3^3D} \leq \frac{\beta^3\Delta^3}{3^3D} = \beta^3D^2.$$

Moreover,

$$|d^2D| = \left|\frac{d}{a}\right|^2 |a|^2 D = |\alpha_1|^2|\alpha_2|^2|\alpha_3|^2 t_1^2 t_2^2 t_3^2 \leq R^3,$$

so

$$|a^2 d^2| \leq \frac{|a|^2 R^3}{D} \leq \beta^3 D,$$

and we conclude

$$|ad| \leq \beta^{3/2} |D|^{1/2}. \tag{2.14}$$

Finally we study $|bc|$:

$$|bc| \leq |a|^2 \left(\sum_i |\alpha_i|\right)\left(\sum_{i\neq j} |\alpha_i \alpha_j|\right).$$

so we have a sum of 9 terms of the form $|a|^2\alpha_i\alpha_j\alpha_k$ with $i,j,k$ not all equal. Thanks to the formula

$$|\alpha_i|^2 t_i^2 (t_1^2 + t_2^2 + t_3^2) \leq PR \tag{2.15}$$

we get

$$|\alpha_i|^2 \leq \frac{PR}{t_i^2 t_j^2} \text{ for every } j \in \{1,2,3\}. \tag{2.16}$$

Choosing properly the $j$'s appearing in the formula above, we have, for $i,j,k$ not all equal

$$|a|^4 |\alpha_i|^2 |\alpha_j|^2 |\alpha_k|^2 \leq |a|^4 \frac{(PR)^3}{t_1^4 t_2^4 t_3^4} = \frac{(PR)^3}{D^2} \leq \beta^3 3^3 |D|,$$

which implies

$$|a|^2 |\alpha_i||\alpha_j||\alpha_k| \leq (3\beta)^{3/2} D^{1/2} \tag{2.17}$$

So

$$|bc| \leq 9(3\beta)^{3/2} D^{1/2}. \tag{2.18}$$

and we can conclude. □

**Remark**. Reduction modulo $\mathrm{SL}_2(\mathcal{O})$ is weaker than reduction modulo $\mathrm{GL}_2(\mathcal{O})$, in particular the bounds we have found for $a,b,c,d$ still hold for forms reduced modulo $\mathrm{GL}_2(\mathcal{O})$.

**Corollary 2.2.4.** *It is possible to list all the binary cubic forms $(a,b,c,d)$ modulo $\mathrm{SL}_2(\mathcal{O})$, with $\mathcal{N}(\mathrm{disc}(F)) \leq X$ (i.e. $X = D^2$, with the notation of Theorem 2.2.3) in time $O(X^{1+\varepsilon})$, for all $\varepsilon > 0$.*

*Proof.* The number of quadruples $(a,b,c,d)$ satisfying all the conditions given in Theorem 2.2.3 is

$$N = \left(\sum_{|a|\ll D^{1/4}} \sum_{|d|\ll D^{1/2}/|a|} 1\right) \cdot \left(\sum_{0<|b|\ll D^{1/4}} \sum_{|c|\ll D^{1/2}/|b|} 1\right)$$
$$+ \sum_{|a|\ll D^{1/4}} \left(\sum_{|d|\ll D^{1/2}/|a|} \sum_{|c|\ll D^{1/2}/|a|} 1\right),$$

where the second term corresponds to $b = 0$. Thus

$$N \ll \sum_{|a| \ll D^{1/4}} \frac{D}{|a|^2} \sum_{\substack{|b| \ll |D|^{1/4} \\ b \neq 0}} \frac{D}{|b|^2} + \sum_{|a| \ll D^{1/4}} \frac{D^2}{|a|^4}$$

For simplicity we will focus on the last sum of this formula, but the first one can be treated in the same way.

$$\sum_{|a| \ll D^{1/4}} \frac{D^2}{|a|^4} \ll D^2 \cdot \sum_{n=1}^{D} \frac{\#\{a \in \mathcal{O} \colon |a|^4 = n\}}{n}.$$

Now, since $\#\{a \in \mathcal{O} \colon |a|^4 = n\} = O(n^\varepsilon) = O(D^\varepsilon)$, for all $\varepsilon > 0$ and $\sum_{n=1}^{D} \frac{1}{n}$ is $O(\log(D))$. So we can conclude. □

### 2.2.3 Automorphisms and morphisms

As we already said, the problem of reducing $F$ modulo $\mathrm{GL}_2(\mathcal{O})$ reduces "nearly" to the problem of reducing $H_F$ modulo $\mathrm{GL}_2(\mathcal{O})$. We are going to explain the meaning of this "nearly".

**Proposition 2.2.5.** *Let $F_1 \neq F_2 \in (\mathrm{Sym}^3 \mathcal{O}^2)^*$, $F_2 = M \cdot F_1$ for some $M \in \mathrm{GL}_2(\mathcal{O})$. Suppose that $H_{F_1}$ and $H_{F_2}$ are both reduced Hermitian forms. Then only two cases are possible:*

(1) *$H_{F_1} = H_{F_2} = H$ and $M \in \mathrm{Aut}(H)$ (i.e. $M \cdot H = H$);*

(2) *$H_{F_1} \neq H_{F_2}$ but they are both on the boundary of the fundamental domain $\mathcal{F}$ and they are in the same orbit modulo $\mathrm{GL}_2(\mathcal{O})$.*

We need to study these two cases to avoid counting more than once the same orbit of $(\mathrm{Sym}^3 \mathcal{O}^2)^*$.

For the first case, we can list the finitely many automorphisms $\{M_i\}$ of $H_F$ and choose only one of the $M_i \cdot F$ (for example the smallest $F = (a, b, c, d)$ in lexicographical order).

For the second case, we have to do the same thing but with the matrices $\{N_j\}$ (we will call them "morphisms"), which send $H_F$ on the boundary to another point of the boundary.

Finally, we have to put the two conditions together to get only one representative for each orbit.

**Proposition 2.2.6.** *Let $F = (a, b, c, d)$, $F$ reduced modulo $\mathrm{GL}_2(\mathcal{O})$, $\mathcal{N}(\mathrm{disc}(F)) \leq X^2$. Let $H = H_F$, and $\Delta = PR - |Q|^2$.*

*Let $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O})$ such that $M \cdot H_F = H_F$. Then we have the following bounds on the coefficients of $M$:*

$$|A|^2 \leq \frac{PR}{\Delta}, \quad |B| \leq \frac{P}{\sqrt{\Delta}}, \quad |D|^2 \leq \frac{PR}{\Delta}. \tag{2.19}$$

*Proof.* Let us write $H(x,y) = P|x|^2 + Q\overline{x}y + \overline{Q}\overline{x}y + R|y|^2$. We have

$$PH(x,y) = |xP + yQ|^2 + \Delta|y|^2, \quad \text{and} \tag{2.20}$$

$$RH(x,y) = |Ry + \overline{Q}x|^2 + \Delta|x|^2. \tag{2.21}$$

Thanks to the formula (2.20) we can give upper bounds for $|A|, |B|$, and $|D|$.

Let we write more explicitly the relation $M \cdot H = H$:

$$\begin{aligned} M \cdot H &= \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} P & Q \\ \overline{Q} & R \end{pmatrix} \begin{pmatrix} \overline{A} & \overline{C} \\ \overline{B} & \overline{D} \end{pmatrix} \\ &= \begin{pmatrix} |A|^2P + \overline{A}B\overline{Q} + A\overline{B}Q + |B|^2R & A\overline{C}P + B\overline{C}\overline{Q} + A\overline{D}Q + B\overline{D}R \\ \overline{A}CP + \overline{A}D\overline{Q} + \overline{B}CQ + \overline{B}DR & |C|^2P + \overline{C}D\overline{Q} + C\overline{D}Q + |D|^2R \end{pmatrix} \\ &= \begin{pmatrix} H(A,B) & \dots \\ \dots & H(C,D) \end{pmatrix} \end{aligned} \tag{2.22}$$

By imposing this matrix to be equal to $M$ we have

$$\begin{aligned} |AP + BQ|^2 + \Delta|B|^2 = P^2 &\quad \Rightarrow \quad |B| \leq \frac{P}{\sqrt{\Delta}}, \\ |CP + DQ|^2 + \Delta|D|^2 = PR &\quad \Rightarrow \quad |D|^2 \leq \frac{PR}{\Delta}, \\ |BR + A\overline{Q}|^2 + \Delta|A|^2 = PR &\quad \Rightarrow \quad |A|^2 \leq \frac{PR}{\Delta}. \end{aligned}$$

□

The bounds of the previous Proposition are completely explicit when $h_K = 1$, since we know $t_K$ and $c_K$.

So we can just loop on all $A, B, C, D$ satisfying these bounds, then select only the matrices with discriminant $|AD - BC| = 1$. The following algorithm needs to be run only once for each of our 9 imaginary quadratic fields of class number 1: it lists the finite set of possibilities for $\mathrm{Aut}\, H$.

**Algorithm 1.** *Lists all possible automorphism matrices $M$ such that $M \cdot H_F = H_F$ (same hypothesis as in Proposition 2.2.6).*

For each triple $(A, B, D)$ satisfying the given bounds, do the following:

(1) Solve $|AD - BC| = 1$, for $C \in \mathcal{O}$: $AD - BC$ belongs to the finite set $\mathcal{O}^*$, and we can solve for $C$.

(2) Consider the following $4 \times 4$ matrix, with coefficients in $\mathcal{O}$:

$$W = \begin{pmatrix} (|A|^2 - 1) & A\overline{B} & \overline{A}B & |B|^2 \\ A\overline{C} & (A\overline{D} - 1) & B\overline{C} & B\overline{D} \\ \overline{A}C & \overline{B}C & (\overline{A}D - 1) & \overline{B}D \\ |C|^2 & C\overline{D} & \overline{C}D & (|D|^2 - 1) \end{pmatrix}.$$

(3) Compute the rank $r$ of $W$ (over the field $K$).

(4) **If** $r = 1$ or $r = 4$, **skip** to the following quadruple $(A, B, C, D)$.

(5) **If** $r = 0$ **output** $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ ($M$ is an automorphism acting on all $F \in \mathcal{F}$)

(6) **If** $r = 2$ or $r = 3$ **output** $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ ($M$ is an automorphism acting only on a boundary subspace).

**Remark**. We could also loop only on $A, D$ and replace step (1) by :

(1) Solve $|AD - BC| = 1$ for $B, C \in \mathcal{O}$. This time $BC$ belongs to an explicit finite set, and we enumerate divisors.

**Proposition 2.2.7.** *Let* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ *belong to* $\mathrm{Aut}\, H_F$*, where* $H_F$ *is the Hessian of some reduced cubic form* $F$*. If* $r$ *is the rank of the matrix* $W$ *constructed in the above algorithm, then*

- $r = 0$ *if and only if* $B = C = 0$ *and* $A = D$ *are units. Then* $M$ *is an automorphism for* all *Hermitian quadratic forms in* $\mathcal{F}$*.*
- $r = 1$ *is impossible*
- $r = 2$ *or* $r = 3$ *then* $M$ *is an automorphism for some linear subspace of* $\mathcal{F}$*, defined by explicit equations in the variables* $(P, Q, \overline{Q}, R)$*.*
- $r = 4$ *is impossible.*

*Proof.* The condition $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Aut}(P|x|^2 + Q\bar{x}y + \overline{Q}\bar{x}y + R|y|^2)$ translates to the linear system $WX = 0$, with $X = (P, Q, \overline{Q}, R)^t$.

- If $r = 4$, the only solution of the system is $(0, 0, 0, 0)$ but this is not allowed since $P, R > 0$.
- Assume that $r \leq 1$ : the matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ has rank 2 so the two 2 by 2 matrices on the lower-left and upper-right corners of $W$ have rank 2 unless $B = C = 0$. In this case $W$ is diagonal

$$\begin{pmatrix} |A|^2 - 1 & & & \\ & A\overline{D} - 1 & & \\ & & \overline{A}D - 1 & \\ & & & |D|^2 - 1 \end{pmatrix}.$$

Since $B = C = 0$, and $AD - BC$ is a unit, we must have $|A| = |D| = 1$, so this matrix has either rank 2 or 0 (when $\overline{A}D = A\overline{D} = 1$).

□

## 2.3 The algorithm

**Algorithm 2.** *Given a bound* $X = D^2$*, output the list of reduced binary cubic forms modulo* $\mathrm{GL}_2(\mathcal{O})$*, such that* $\mathcal{N}(\mathrm{disc}(F)) \leq X$*.*

For each quadruple $F = (a, b, c, d) \in \mathcal{O}^4$ satisfying all the inequalities in Theorem 2.2.3 do the following

(1) Approximate the complex roots of $F$, $(\alpha_1, \alpha_2, \alpha_3)$ to a sufficient accuracy. Then approximate $H_F = (P, Q, R)$ the associated Hermitian form.

(2) Check if $H_F$ is reduced (in particular if $H_F$ is "near" to the boundary of the fundamental domain use Algorithm 3 (see below) to check exactly the boundary condition). If not **skip** to the following $F$.

(3) Check whether $F$ is irreducible in $K[x, y]$. If not **skip** to the following $F$.

(4) Apply Dedekind criterion to check whether $F$ describes a maximal ring. If not **skip** to the following $F$.

(5) Compute the set of all automorphisms $M_i$ of $H_F$ and compute all the images $M_i \cdot F$. Check if $F$ is the minimal element (for some order, for instance the lexicographic one) in this set: if yes, **print** $F$.

**Remarks**.

- For the precision needed in step (1) refer to Appendix C.
- In step (5), we compute a list of automorphs for $F$ to decide whether $F$ is the minimal in lexicographic order (in this case $F$ should be keeped, otherwise no). Another way to deal with this problem could be "stocking" all those $F$ and then checking $\mathrm{GL}_2(\mathcal{O})$-equivalence once we have all the forms with a fixed discriminant $D$. The problem is that our algorithm, does not assure that the output forms are ordered by discriminant, so we could apply this test only at the end, and this would mean a lot more space used for stocking all the automorphic forms. Moreover, this would imply a double loop on the list which will make also the complexity grow. That's why we preferred to apply immediately automorphism matrices so that we don't have to keep anything in memory (recall that we just output the "good" binary cubic form each time we find one, so we are not even obliged to keep in memory the list of representatives of cubic extensions).

## 2.4 The case $K = \mathbb{Q}(i)$

When $K = \mathbb{Q}(i)$ the fundamental domain for positive definite binary Hermitian forms is given by

$$\begin{cases} P \leq R \\ -P/2 \leq \mathrm{Re}(Q) \leq P/2 \\ 0 \leq \mathrm{Im}(Q) \leq P/2. \end{cases}$$

We now specialize Theorem 2.2.3:

**Theorem 2.4.1.** *Let $F$ be an irreducible binary cubic form with coefficients in $\mathbb{Z}[i]$ which is reduced modulo $\mathrm{SL}_2(\mathbb{Z}[i])$ and with discriminant $D$. Then*

$$|a| \leq \left(\frac{2}{3}\right)^{3/4} |D|^{1/4}; \quad |b| \leq 3\left(\frac{27}{2}\right)^{1/4} |D|^{1/4}$$

$$|ad| \leq 2\sqrt{2}|D|^{1/2}; \quad |bc| \leq 9 \cdot 6\sqrt{6}|D|^{1/2}, \quad |ac| \leq 3\left(\frac{27}{2}\right)^{1/2} |D|^{1/2}.$$

As explained in Corollary 2.2.4, we can loop on all $(a,b,c,d)$ given in Theorem 2.4.1 in time $O(X^{1+\varepsilon})$, for any $\varepsilon > 0$.

**Proposition 2.4.2.** *Let* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}[i])$*, such that*

$$M \cdot H = H,$$

*then*

$$|A| \leq 1, |B| \leq 1, |D| \leq 1, |C|^2 \leq 2.$$

*Proof.* Bounds on $|A|, |B|$ and $|D|$ directly come from Proposition 2.2.6. The bound on $C$ then follows from Algorithm 1. □

**Proposition 2.4.3.** *If*

$$H = \begin{pmatrix} P & Q \\ \overline{Q} & R \end{pmatrix}$$

*is not on the boundary of the fundamental domain, then its only automorphisms are the ones in the following set:*

$$\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}[i])} \begin{pmatrix} P & Q \\ \overline{Q} & R \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} \right\}$$

*Proof.* This follows from Proposition 2.2.7. □

### 2.4.1 Loops on $a, b, c, d$

When $K = \mathbb{Q}(i)$ we have seen that multiplication by $i$ and $-i$ give automorphisms on all cubic forms. So, in Algorithm 2, instead of looping over all $a \in \mathbb{Z}[i]$ satisfying $|a| \leq a_{max}$, where

$$a_{max} := \left(\frac{2}{3}\right)^{3/4} |D|^{1/4},$$

we can just restrict to just one quadrant, for example

$$\{a \colon |a| \leq a_{max}, \mathrm{Re}(a) \geq 1, \mathrm{Im}(a) \geq 0, a \neq 0\}$$

Moreover we noticed that $[\mathrm{PGL}_2(\mathcal{O}) : \mathrm{PSL}_2(\mathcal{O})] = 2$, and a representative for the nontrivial coset is $\sigma = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$. It sends an Hermitian form $(P,Q,R)$ to $(P,iQ,R) = (P, -\mathrm{Im}(Q) + i\,\mathrm{Re}(Q), R)$, so we can restrict to binary Hermitian forms such that $\mathrm{Re}(Q) \geq 0$ (with a border condition for $\mathrm{Re}(Q) = 0$). This new condition translates to a condition on the coefficient $c$ of the binary cubic form $F = (a,b,c,d)$. We can for example restrict $c$ to the upper half plane:

$$\{c \colon |c| \leq c_{max}, \mathrm{Im}(c) \geq 1 \text{ if } \mathrm{Re}(c) < 0, \mathrm{Im}(c) \geq 0 \text{ otherwise } \}.$$

From now on let us call $\phi$ the function which takes a cubic form $(a,b,c,d)$ to an equivalent one $(a',b',c',d')$ in the good quadrants.

## 2.5 Implementation problems

### 2.5.1 Checking rigorously the boundary conditions

As the computation of $P, Q, R$ involves floating point approximations of the complex roots of a polynomial in $\mathcal{O}_K[X]$, it will not give, of course, exact results. Those floating point computations will in general be sufficient to test whether the Hermitian form is strictly inside or outside the fundamental domain. But if it is very near the boundary (or worse *on* the boundary), this approach fails.

For that we use the following formulas:

$$P = -\frac{|b|^2}{|a|^2} + 3(|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2) \tag{2.23}$$

$$Q = \frac{\overline{b}c}{|a|^2} + 3(\overline{\alpha_1}\alpha_2\alpha_3 + \alpha_1\overline{\alpha_2}\alpha_3 + \alpha_1\alpha_2\overline{\alpha_3}) \tag{2.24}$$

$$R = -\frac{|c|^2}{|a|^2} + 3(|\alpha_1|^2|\alpha_2|^2 + |\alpha_1|^2|\alpha_3|^2 + |\alpha_2|^2|\alpha_3|^2) \tag{2.25}$$

Now we consider $\alpha_1, \alpha_2, \alpha_3, \overline{\alpha_1}, \overline{\alpha_2}, \overline{\alpha_3}$ as algebraic numbers, and we let $S$ be the set of the six permutations fixing the $\alpha_i$, and acting as $S_3$ on the $\overline{\alpha_i}$. The polynomial

$$g_P = \prod_{\sigma \in S} (X - \sigma(\alpha_1\overline{\alpha_1} + \alpha_2\overline{\alpha_2} + \alpha_3\overline{\alpha_3}))$$

vanishes at $|\alpha_1|^2+|\alpha_2|^2+|\alpha_3|^2$, and its coefficients are symmetric in $(\alpha_1, \alpha_2, \alpha_3)$ and $(\overline{\alpha_1}, \overline{\alpha_2}, \overline{\alpha_3})$ independently. They can thus be expressed in terms of $(b/a, c/a, d/a)$ and $(\overline{b/a}, \overline{c/a}, \overline{d/a})$. The polynomial $f_P(X) = g_P\left(\frac{X}{3} - \frac{|b|^2}{3|a|^2}\right)$ vanishes at $P$ and belongs to $K[X]$.

In the same way we can compute polynomials in $K[X]$ vanishing at $Q$, $R$, $\mathrm{Re}(Q)$ or $\mathrm{Im}(Q)$. Such polynomials are easily computed using a computer algebra system like Maple (and it is sufficient to compute them once for all); the polynomials $g_P$, $g_Q$, $g_R$ and so on are given in Appendix D — before the trivial linear change of variable yielding $f_P$, $f_Q$, $f_R$, etc.

We want to verify rigorously boundary conditions, for instance $P = R$: if $f_P$ and $f_R$ have no common factor in $K[X]$, then $P \neq R$. But this is not enough: we also want to check whether $P < R$ or $P > R$, i.e. if the point we are testing is "inside" or "outside" the fundamental domain.

The following theorem of Mahler [41] provides the accuracy we need for our floating point computations:

**Theorem 2.5.1** (Mahler). *Let $f = a_0x^m + a_1x^{m-1} + \cdots + a_m = a_0(x - \alpha_1)\cdots(x - \alpha_m)$ be a separable polynomial of degree $m \geq 2$, and let*

$$\Delta(f) = \min_{1 \leq i < j \leq m} |\alpha_i - \alpha_j|$$

*be the minimal distance between two distinct roots of $f$. Then*

$$\Delta(f) > \sqrt{3}m^{-(m+2)/2}|\operatorname{disc}(f)|^{1/2}M(f)^{-(m-1)},$$

*where* $\operatorname{disc}(f)$ *is the discriminant of $f$, and $M(f) = |a_0|\prod_{h=1}^{m}\max(1, |\alpha_h|)$.*

This translates to the following algorithm:

**Algorithm 3** (Checking an algebraic identity)**.** *Let $\alpha$ and $\beta \in \mathbb{R}$ be two algebraic numbers, and let $A$ and $B \in K[X] \setminus 0$ that vanish at $\alpha$, and $\beta$ respectively. Assume we can compute floating point approximations $\hat{\alpha}$ and $\hat{\beta}$ such that $|\alpha - \hat{\alpha}| < \varepsilon$, $\left|\beta - \hat{\beta}\right| < \varepsilon$, for any fixed $\varepsilon > 0$.*

*We want to decide whether $\alpha < \beta$, $\alpha > \beta$ or $\alpha = \beta$.*

(1) Let $C = AB$ and $f = C/\gcd(C, C')$.

(2) If the degree of $f$ is 1, then **answer** $\alpha = \beta$.

(3) Compute a good approximation $\hat{\Delta}$ of

$$\Delta(f) = \sqrt{3} m^{-(m+2)/2} |\operatorname{disc}(f)|^{1/2} M(f)^{-(m-1)},$$

where $\operatorname{disc}(f)$ and $M(f)$ are defined in Theorem 2.5.1 such that $\hat{\Delta} \leq \Delta(f)$.

(4) Compute $\alpha$ and $\beta$ at precision $\varepsilon = \hat{\Delta}/4$, i.e. $\hat{\alpha}$ and $\hat{\beta}$ such that

$$|\alpha - \hat{\alpha}| < \varepsilon, \quad \left|\beta - \hat{\beta}\right| < \varepsilon.$$

(5) If $|\hat{\alpha} - \hat{\beta}| < 2\varepsilon$, **answer** $\alpha = \beta$.

(6) If $\hat{\alpha} < \hat{\beta}$, **answer** $\alpha < \beta$.

(7) If $\hat{\alpha} > \hat{\beta}$, **answer** $\alpha > \beta$.

*Proof.* The polynomial $f$ is non constant and has $\alpha$ and $\beta$ among its roots. If its degree is 1, then $\alpha = \beta$. Otherwise, assume first that $|\hat{\alpha} - \hat{\beta}| < 2\varepsilon$. Then

$$|\alpha - \beta| \leq |\alpha - \hat{\alpha}| + \left|\beta - \hat{\beta}\right| + \left|\hat{\alpha} - \hat{\beta}\right| < 4\varepsilon \leq \Delta(f).$$

Hence $\alpha = \beta$ by Mahler's theorem in this case, proving (5).

We now assume that $|\hat{\alpha} - \hat{\beta}| \geq 2\varepsilon$; since

$$\alpha - \beta = \hat{\alpha} - \hat{\beta} + (\alpha - \hat{\alpha}) - (\beta - \hat{\beta})$$

and

$$\left|(\alpha - \hat{\alpha}) - (\beta - \hat{\beta})\right| < 2\varepsilon,$$

$\alpha - \beta$ and $\hat{\alpha} - \hat{\beta}$ have the same sign. □

**Proposition 2.5.2.** *The smallest $\varepsilon$ that we can obtain in step (4) of the above algorithm (i.e. the maximal precision needed) is $\gg X^{-\beta}$, for some positive constant $\beta$.*

**Remark**. That means that for our computation we will need at most $\Omega(\log X)$ significant digits.

*Proof.* Our algorithm loops over reduced integral cubic forms $F = (a, b, c, d) \in (\mathcal{O}_K)^4$ with discriminant $\operatorname{disc}(F)$ satisfying $|\operatorname{disc}(F)|^2 \leq X$. In particular, Theorem 2.2.3 implies that $|a| \ll X^{1/8}$.

For each such form, we may compute various separable polynomials $f$ with coefficients in $a^{-u}\mathcal{O}_K$, for some bounded integer $u$. Then $\mathrm{disc}(f)$ is non zero, in $a^{-4u}\mathcal{O}_K$. Its norm is a non-zero rational integer divided by $|a|^{-8u}$, hence $\gg X^{-u}$. Thus $\mathrm{disc}(f) \gg X^{-u/2}$.

Landau's theorem (see [4, Proof of Theorem 13.1] for example) tells us that

$$M(f) \leq \|f\|_2$$

and the coefficients of $f$ are monomials in $e_1, e_2, e_3, f_1, f_2, f_3$ (see Appendix D). Each one of these is bounded by $c \cdot X^{\alpha}$, for an appropriate constant $c$ and exponent $\alpha$.

We have

$$\Delta(f) \gg M(f)^{-(m-1)}.$$

So we obtain

$$\|f\|_2 \ll X^{\beta},$$

but then we can conclude that $\Delta(f) \gg X^{-\beta}$. □

### 2.5.2 An idea to count only half of the extensions

It is easy to remark that if $H = (P, Q, R)$ is in the fundamental domain, then also $H' = (P, -\overline{Q}, R)$ is. And, in general,these two Hermitian forms are not equivalent modulo $\mathrm{GL}_2(\mathcal{O})$.

In particular, if $F = (a, b, c, d)$ has $H_F = H$, then $F' = (\overline{a}, -\overline{b}, \overline{c}, -\overline{d})$ gives $H_{F'} = H'$.

This allow us to loop only on half of the $c$ satisfying the given bounds.

Then construct both the forms $F = (a, b, c, d)$ and $F' = (\overline{a}, -\overline{b}, \overline{c}, -\overline{d})$ and we check if they are equivalent (comparing $F'$ with the list of automorphic functions to $F$). If not we verify also the list of automorphic functions to $F'$ to see if one of them will be found in our loops, and if both the answers are no, we add this second form $F'$ to our output list.

### 2.5.3 Loop on $d$

Once we have fixed $(a, b, c)$, we could loop on $|d| \leq d_{max}$ but this will be very slow.

The idea is to consider the formula of the discriminant of the cubic form $F$ :

$$D = Ad^2 + Bd + C,$$

with $A = -27a^2, B = 18abc - 4b^3$ and $C = b^2c^2 - 4ac^3$. Next we can find the solutions $x_1, x_2$ of the polynomial $Ax^2 + Bx + C$ so that $D = A(d - x_1)(d - x_2)$. As we know that $|D| \leq X$, then we get $|d - x_1||d - x_2| \leq X/|A|$. Now let us suppose that $|d - x_1|$ and $|d - x_2|$ are $\geq 1/2$. Then we obtain

$$\begin{cases} |d - x_1| \leq 2X/|A| \\ |d - x_2| \leq 2X/|A| \end{cases},$$

and the set of the solutions $d$ is given by the intersection of the two circles of centre $x_1$ and $x_2$ and ray $2X/|A|$.

On the other case, if $|d - x_i| < 1/2$ for $i = 1$ or 2, then we just need to consider as possible $d$ the two points $\lceil x_1 \rfloor$ and $\lceil x_2 \rfloor$.

Now let us consider

$$|x_1 - x_2| = \frac{\sqrt{|\Delta|}}{|A|},$$

where $\Delta = B^2 - 4AC$. If $|x_1 - x_2| > 4X/|A|$, then the two circles described above have no intersection, so the only possible $d$ are $\lceil x_1 \rfloor$ and $\lceil x_2 \rfloor$. In the other case, if the two circles have intersection, we have to consider both their intersection and $\lceil x_1 \rfloor$ and $\lceil x_2 \rfloor$.

This method allows us to make a much smaller loop on $d$.

### 2.5.4 Another kind of reduction

After personal conversation with J. Cremona, I tried to apply a different kind of reduction, which can be found in [23, 54, 24].

Let us consider the subgroup $S$ of $\mathrm{GL}_2(\mathcal{O})$ of unimodular substitutions of the kind

$$\tau_k : \begin{cases} x \to x + k \\ y \to y \end{cases},$$

that is the set matrices of the form $\tau_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, with $k \in \mathcal{O}$.

This transformations send

$$(a, b, c, d) \to (a, b + 3ak, 3ak^2 + 2bk + c, ak^3 + bk^2 + ck + d).$$

So it is always possible to replace a cubic form $F_0 = (a_0, b_0, c_0, d_0)$ by an equivalent one, $F = (a, b, c, d)$ obtained by applying an element of $S$ and such that $b$ is reduced modulo $3a$ (after we have chosen a fundamental parallelotope for the lattice generated by $3a$ and $3a\omega$, where $\langle 1, \omega \rangle$ is a fixed basis for $\mathcal{O}_K$).

**Definition 2.5.3.** *Let $F_0 = (a_0, b_0, c_0, d_0) \in (\mathrm{Sym}^3 \mathcal{O}^2)^*$ be a binary cubic form. And let us fix once and for all a choice of a fundamental parallelotope $\mathcal{P}_{u,v}$ for the lattice generated by two elements $u, v \in \mathcal{O}_K$. We associate to $F_0$ the equivalent form $F = (a, b, c, d) \in (\mathrm{Sym}^3 \mathcal{O}^2)^*$ such that $F = \tau_K(F_0)$, for some $k \in \mathcal{O}_K$ and that the second component of $F$, $b$ is in the fundamental parallelotope $\mathcal{P}_{3a,3a\omega}$ We will call such form $F$ $\tau$-reduced.*

**Remark**. This $F$ is unique if we fix a unique choice for points on the border of $\mathcal{P}$.

In particular, we can apply this new reduction to Julia-reduced forms. On the way back, if we have a $\tau$-reduced form $F = (a, b, c, d)$ which comes from a Julia-reduced form, then the unimodular transformation $\tau_k$ which sends it back to the Julia reduced one is given by $k = \lceil Q/P \rfloor$, where $(P, Q, R)$ is the covariant $H_F$ associated to $F$. In fact, unimodular transformations in $S$ leave $P$ unchanged and send $Q \to Q - kP$, so $\tau_k$ will send $(P, Q, R)$ to $(P, Q_0, R_0)$ such that $|\mathrm{Re}(Q)| \leq P/2$ and $|\mathrm{Im}(Q)| \leq P/2$, and can only increase $R$, so $P \leq R_0$.

Moreover, elements of $S$ leave unchanged $P_H = b^2 - 3ac$ (this is the first coefficient of the Hessian of our cubic form, but it is not true in general that it is the first coefficient of our covariant $H_F$!)and $U_H = 2b^3 + 27a^2d - 9abc$ and, as is shown in Womack's thesis [54] we have

$$|a| \leq 3^{-3/4} t_K^{-3/2} D^{1/4}$$

and

$$|U| \leq 3^{3/4} t_K^{-3/2} D^{3/4}$$

so from the sygyzy

$$4P^3 = U^2 + 27Da^2$$

we obtain

$$P_H \leq c_H D^{1/2}, \tag{2.26}$$

where $c_H = 3^{1/2} 2^{-1/3} t_K^{-1}$. In particular when $K = \mathbb{Q}(i)$, we get $c_H = 1,944...$ so we get

**Proposition 2.5.4.** *Let $F = (a, b, c, d)$ be a $\tau$-reduced binary cubic form then*

$$|c| \leq \frac{|b|^2 + c_H |D|^{1/2}}{3|a|}.$$

*Proof.* Immediate from (2.26). □

**Remark**. This different kind of reduction does not change the complexity of the algorithm, which is still in $O_\varepsilon(X^{1+\varepsilon})$ but it changes the constant implied in this complexity. In fact, the algorithm goes more than 6 times faster, wich is not negligible in practice.

**Algorithm 4** ($\tau$-reduction)**.** *Let $K$ be an imaginary quadratic number field of class number* 1*. This algorithm loops over all the binary cubic forms $F' = (a', b', c', d')$ with $\mathcal{N}\,\mathrm{disc}(F) \leq X^2$, which are $\tau$-reduced, and associates the corresponding Julia reduced binary cubic form $F = (a, b, c, d)$.*

For each $a', b', c', d'$ in $\mathcal{O}$ satisfying the following properties:

- $|a'| \leq a_{max} = \left(\frac{1}{t_K\sqrt{3}}\right)^{3/2} X^{1/8}$,
- $b'$ belongs to $\mathcal{P}_{3a',3a'\omega}$
- $|c'| \leq \frac{|b'|^2 + c_H X^{1/4}}{3|a'|}$,
- $\mathcal{N}\left(\mathrm{disc}(a', b', c', d')\right) \leq X^2$. (This last condition bounds $d'$.)

Do the following:

(1) compute the first two coefficients $P', Q'$ of the covariant $H_{F'}$ of the cubic form $F' = (a', b', c', d')$.

(2) Set $k$ the closest point to $Q/P$ in $\mathcal{O}$; select a fixed rounding rule to break ties (for instance, select the lexically smallest point).

(3) Compute $F = (a, b, c, d) = \tau_k(a', b', c', d')$.

(4) Continue from step (2) of Algorithm 2.

## 2.6 Results

We programmed the algorithm for the case $K = \mathbb{Q}(i)$ in Pari/GP.

Here are some results we got on an Intel Xeon 5160 dual core, 3.0 GHz.

$X$ is the bound on $\mathfrak{d}(L/K)$, $N(X)$ is the number of isomorphism classes of cubic extensions of $\mathbb{Q}(i)$ up to that bound, and $t$ is the running time of the algorithm. Finally $t'$ is the time needed to do the same computation but using the version of ray class field algorithm that we describe in Appendix B.1.

| $X$ | $N(X)$ | $t$ | $t'$ |
|---|---|---|---|
| $10^4$ | 276 | 5 s | 16s |
| $4 \cdot 10^4$ | 1339 | 19 s | 1mn 18s |
| $9 \cdot 10^4$ | 3305 | 56 s | 3mn 45s |
| $10^6$ | 42692 | 24 mn 1 s | 2h 52mn 9s |
| $4 \cdot 10^6$ | 181944 | 2 h 49 mn | 34h 24 mn 8s |
| $9 \cdot 10^6$ | 421559 | 9 h 37 mn | $> 134$ h |
| $10^8$ | 4990974 | 359 h 25 mn | $> 2720$ h |

### 2.6.1 List of cubic extensions of $\mathbb{Q}(i)$ up to $\mathcal{N}\mathfrak{d}(L/\mathbb{Q}(i)) \leq 10^4$

| $\mathcal{N}\mathfrak{d}(L/\mathbb{Q}(i))$ | $P(X)$ |
|---|---|
| 169 | $x^3 + (1+2i)\,x^2 + 2ix + i$ |
| 169 | $x^3 + (2+i)\,x^2 + 2ix - 1$ |
| 353 | $x^3 + (2+2i)\,x^2 + 3ix - 1$ |
| 353 | $x^3 + (2+2i)\,x^2 + 3ix + i$ |
| 484 | $x^3 + (2+2i)\,x^2 + 4ix + (-1+i)$ |
| 529 | $x^3 + 2x^2 + x + 1$ |
| 745 | $x^3 + 2ix^2 - x - 1$ |
| 745 | $x^3 + 2x^2 + x + i$ |
| 772 | $x^3 + 2ix^2 - 2x + (1-i)$ |
| 772 | $x^3 + 2x^2 + 2x + (1-i)$ |
| 841 | $x^3 + (2+2i)\,x^2 + (-1+i)\,x - i$ |
| 932 | $x^3 + (1+2i)\,x^2 + ix + 1$ |
| 932 | $x^3 + (2+i)\,x^2 + ix - i$ |
| 953 | $x^3 + (2+2i)\,x^2 + (-1+2i)\,x - i$ |
| 953 | $x^3 + (2+2i)\,x^2 + (1+2i)\,x + 1$ |
| 961 | $x^3 + 2x^2 + x - 1$ |
| 1025 | $x^3 + (2+2i)\,x^2 + ix - i$ |
| 1025 | $x^3 + (2+2i)\,x^2 + ix + 1$ |
| 1289 | $x^3 + (2+2i)\,x^2 + 2ix - i$ |
| 1289 | $x^3 + (2+2i)\,x^2 + 2ix + 1$ |
| 1369 | $x^3 + (2+2i)\,x^2 + (-2+3i)\,x + (-2-i)$ |
| 1369 | $x^3 + (2+2i)\,x^2 + (2+3i)\,x + (1+2i)$ |
| 1444 | $x^3 + (1+i)\,x^2 + (1-i)$ |

| | |
|---|---|
| 1508 | $x^3 + 2ix^2 + (-1-i)\,x + (1+i)$ |
| 1508 | $x^3 + 2x^2 + (1-i)\,x + (-1-i)$ |
| 1513 | $x^3 + (2+2i)\,x^2 + 3ix + (-2+i)$ |
| 1513 | $x^3 + (2+2i)\,x^2 + 3ix + (-1+2i)$ |
| 1665 | $x^3 + (1+2i)\,x^2 + (-2+2i)\,x - i$ |
| 1665 | $x^3 + (2+i)\,x^2 + (2+2i)\,x + 1$ |
| 1696 | $x^3 + (2+2i)\,x^2 + (-2+3i)\,x - 2$ |
| 1696 | $x^3 + (2+2i)\,x^2 + (2+3i)\,x + 2i$ |
| 1700 | $x^3 + (1+2i)\,x^2 + (-2+i)\,x + (-1-2i)$ |
| 1700 | $x^3 + (2+i)\,x^2 - + (2+i)\,x + (2+i)$ |
| 1721 | $x^3 + 2ix^2 - 2x + 1$ |
| 1721 | $x^3 + 2x^2 + 2x - i$ |
| 1753 | $x^3 + ix^2 + x + (-1+i)$ |
| 1753 | $x^3 + x^2 - x + (-1+i)$ |
| 1825 | $x^3 + 2ix^2 + (-1-i)\,x + i$ |
| 1825 | $x^3 + 2x^2 + (1-i)\,x - 1$ |
| 2017 | $x^3 + 2ix^2 + (-3+i)\,x - i$ |
| 2017 | $x^3 + 2x^2 + (3+i)\,x + 1$ |
| 2036 | $x^3 + ix^2 + 2ix + (-1-i)$ |
| 2036 | $x^3 + x^2 + 2ix + (1+i)$ |
| 2180 | $x^3 + (-1-i)\,x + (1+i)$ |
| 2180 | $x^3 + (1-i)\,x + (-1-i)$ |
| 2257 | $x^3 + (2+2i)\,x^2 + (-1+3i)\,x + (-2-i)$ |
| 2257 | $x^3 + (2+2i)\,x^2 + (1+3i)\,x + (1+2i)$ |
| 2297 | $x^3 + (1+2i)\,x^2 - 2x + (1-2i)$ |
| 2297 | $x^3 + (2+i)\,x^2 + 2x + (2-i)$ |
| 2305 | $x^3 + (1+2i)\,x^2 - 2x + 1$ |
| 2305 | $x^3 + (2+i)\,x^2 + 2x - i$ |
| 2401 | $x^3 + 2x^2 - x - 1$ |
| 2404 | $x^3 + (1+2i)\,x^2 + 3ix + (-1+2i)$ |
| 2404 | $x^3 + (2+i)\,x^2 + 3ix + (-2+i)$ |
| 2417 | $x^3 + ix^2 + (-2+i)\,x - 2i$ |
| 2417 | $x^3 + x^2 + (2+i)\,x + 2$ |
| 2512 | $x^3 + 2ix^2 + (-2+i)\,x - 2i$ |
| 2512 | $x^3 + 2x^2 + (2+i)\,x + 2$ |
| 2516 | $x^3 + 2ix^2 - x + (-1-i)$ |
| 2516 | $x^3 + 2x^2 + x + (1+i)$ |
| 2704 | $x^3 + (2+2i)\,x^2 + 5ix + (-2+2i)$ |
| 2809 | $x^3 + (1+i)\,x^2 + 2x + (2+i)$ |
| 2916 | $x^3 + (1+i)$ |
| 2932 | $x^3 - x + (1+i)$ |
| 2932 | $x^3 + x + (-1-i)$ |
| 3028 | $x^3 + (1+2i)\,x^2 + (1-i)$ |
| 3028 | $x^3 + (2+i)\,x^2 + (1-i)$ |
| 3104 | $x^3 + (2+2i)\,x^2 + 3ix - 2$ |
| 3104 | $x^3 + (2+2i)\,x^2 + 3ix + 2i$ |
| 3161 | $x^3 + (1+2i)\,x^2 - 2x + (-1-2i)$ |
| 3161 | $x^3 + (2+i)\,x^2 + 2x + (2+i)$ |
| 3172 | $x^3 + (2+2i)\,x^2 + 2ix + (-1-i)$ |
| 3172 | $x^3 + (2+2i)\,x^2 + 2ix + (1+i)$ |

| | |
|---|---|
| 3209 | $x^3 + 2ix^2 + (-2-i)\,x + (2-i)$ |
| 3209 | $x^3 + 2x^2 + (2-i)\,x + (1-2i)$ |
| 3257 | $x^3 + (1+i)\,x^2 + (-1-i)\,x + (1-2i)$ |
| 3257 | $x^3 + (1+i)\,x^2 + (1-i)\,x + (2-i)$ |
| 3313 | $x^3 + (2+2i)\,x^2 + (-1+2i)\,x + (-1-2i)$ |
| 3313 | $x^3 + (2+2i)\,x^2 + (1+2i)\,x + (2+i)$ |
| 3412 | $x^3 + 2ix^2 + (-1+2i)\,x + (-1-i)$ |
| 3412 | $x^3 + 2x^2 + (1+2i)\,x + (1+i)$ |
| 3460 | $x^3 + 2ix^2 - 2ix + (1+i)$ |
| 3460 | $x^3 + 2x^2 - 2ix + (-1-i)$ |
| 3481 | $x^3 + x^2 - x - 2$ |
| 3601 | $x^3 + (1+i)\,x^2 - ix + (1-2i)$ |
| 3601 | $x^3 + (1+i)\,x^2 - ix + (2-i)$ |
| 3716 | $(1+i)\,x^3 + 4ix^2 + (-3+3i)\,x + (-2-i)$ |
| 3716 | $(1+i)\,x^3 + 4ix^2 + (-3+3i)\,x + (-2+i)$ |
| 3721 | $x^3 + ix^2 + (-2+2i)\,x + (-1-2i)$ |
| 3721 | $x^3 + x^2 + (-1+2i)\,x + (-1+i)$ |
| 3721 | $x^3 + x^2 + (2+2i)\,x + (2+i)$ |
| 3737 | $x^3 + (2+2i)\,x^2 + (-1+3i)\,x - 3$ |
| 3737 | $x^3 + (2+2i)\,x^2 + (1+3i)\,x + 3i$ |
| 3793 | $x^3 + (2+2i)\,x^2 + (-2+2i)\,x + (-1-2i)$ |
| 3793 | $x^3 + (2+2i)\,x^2 + (2+2i)\,x + (2+i)$ |
| 3809 | $x^3 + 2ix^2 + (-3-i)\,x - 3i$ |
| 3809 | $x^3 + 2x^2 + (3-i)\,x + 3$ |
| 3908 | $x^3 + (-1-i)\,x + (-1+i)$ |
| 3908 | $x^3 + (1-i)\,x + (-1+i)$ |
| 3940 | $x^3 - 2x + (1+i)$ |
| 3940 | $x^3 + 2x + (-1-i)$ |
| 4036 | $x^3 + (1+i)\,x^2 + 2ix + (-1-i)$ |
| 4036 | $x^3 + (1+i)\,x^2 + 2ix + (1+i)$ |
| 4052 | $x^3 + (-1-2i)\,x + (-1+i)$ |
| 4052 | $x^3 + (1-2i)\,x + (-1+i)$ |
| 4084 | $x^3 + (1+i)\,x^2 - x - 2i$ |
| 4084 | $x^3 + (1+i)\,x^2 + x + 2$ |
| 4196 | $x^3 + (1+2i)\,x^2 + (-2+3i)\,x - 3$ |
| 4196 | $x^3 + (2+i)\,x^2 + (2+3i)\,x + 3i$ |
| 4217 | $(1+i)\,x^3 + (1+4i)\,x^2 + (-1+4i)\,x + (-2+i)$ |
| 4217 | $(1+i)\,x^3 + (2+i)\,x^2 + x - 1$ |
| 4304 | $x^3 + 2ix^2 + (-2-i)\,x + 2$ |
| 4304 | $x^3 + 2x^2 + (2-i)\,x - 2i$ |
| 4432 | $x^3 + (1+2i)\,x^2 + (-3+i)\,x + (1-i)$ |
| 4432 | $x^3 + (2+i)\,x^2 + (3+i)\,x + (1-i)$ |
| 4537 | $x^3 + 2ix^2 + (-1+i)\,x + (-2-i)$ |
| 4537 | $x^3 + 2x^2 + (1+i)\,x + (1+2i)$ |
| 4777 | $x^3 + ix^2 + (1+i)\,x + (-2+i)$ |
| 4777 | $x^3 + x^2 + (-1+i)\,x + (-1+2i)$ |
| 4825 | $x^3 + (1+2i)\,x^2 + (-1-i)\,x + (1-2i)$ |
| 4825 | $x^3 + (2+i)\,x^2 + (1-i)\,x + (2-i)$ |
| 4900 | $x^3 + (2+2i)\,x^2 + 2ix + (1-i)$ |
| 4932 | $x^3 + 2ix^2 + (1+i)\,x + (-1+i)$ |

| | |
|---|---|
| 4932 | $x^3 + 2x^2 + (-1+i)\,x + (-1+i)$ |
| 5057 | $x^3 + ix^2 + ix - 2$ |
| 5057 | $x^3 + x^2 + ix + 2i$ |
| 5065 | $x^3 + 2ix^2 + (-3-i)\,x + (-1-2i)$ |
| 5065 | $x^3 + 2x^2 + (3-i)\,x + (2+i)$ |
| 5105 | $x^3 + (1+2i)\,x^2 - 2x - 3i$ |
| 5105 | $x^3 + (2+i)\,x^2 + 2x + 3$ |
| 5113 | $x^3 + (1+2i)\,x^2 - x - 2i$ |
| 5113 | $x^3 + (2+i)\,x^2 + x + 2$ |
| 5161 | $x^3 + 2ix^2 + (-3-2i)\,x + (2-i)$ |
| 5161 | $x^3 + 2x^2 + (3-2i)\,x + (1-2i)$ |
| 5329 | $x^3 + 2ix^2 + (-4+i)\,x - 3i$ |
| 5329 | $x^3 + 2x^2 + (4+i)\,x + 3$ |
| 5364 | $x^3 + 2ix^2 + (-3-2i)\,x + (1-i)$ |
| 5364 | $x^3 + 2x^2 + (3-2i)\,x + (1-i)$ |
| 5449 | $x^3 + (1+2i)\,x^2 + (-2+2i)\,x + (-2+i)$ |
| 5449 | $x^3 + (2+i)\,x^2 + (2+2i)\,x + (-1+2i)$ |
| 5465 | $x^3 + (1+i)\,x^2 - 2ix + (1-2i)$ |
| 5465 | $x^3 + (1+i)\,x^2 - 2ix + (2-i)$ |
| 5476 | $x^3 + (2+2i)\,x^2 + (1-i)$ |
| 5569 | $x^3 + ix^2 + (1+i)\,x + (-1+2i)$ |
| 5569 | $x^3 + x^2 + (-1+i)\,x + (-2+i)$ |
| 5729 | $x^3 + (2+2i)\,x^2 + 4ix + (-3+2i)$ |
| 5729 | $x^3 + (2+2i)\,x^2 + 4ix + (-2+3i)$ |
| 5776 | $x^3 + (2+2i)\,x^2 + 3ix + (-2+2i)$ |
| 5792 | $x^3 + 2ix^2 + (-4+i)\,x + (-2-2i)$ |
| 5792 | $x^3 + 2x^2 + (4+i)\,x + (2+2i)$ |
| 5849 | $x^3 + 2ix^2 + (-1-2i)\,x + (2+i)$ |
| 5849 | $x^3 + 2x^2 + (1-2i)\,x + (-1-2i)$ |
| 5956 | $x^3 + (1+2i)\,x^2 + (-2+i)\,x + 1$ |
| 5956 | $x^3 + (2+i)\,x^2 + (2+i)\,x - i$ |
| 5972 | $x^3 + 2ix^2 + x + (-1+i)$ |
| 5972 | $x^3 + 2x^2 - x + (-1+i)$ |
| 6065 | $x^3 + ix^2 + x + (-1-i)$ |
| 6065 | $x^3 + x^2 - x + (1+i)$ |
| 6100 | $(1+i)\,x^3 + (1+5i)\,x^2 + (-3+6i)\,x + (-2+2i)$ |
| 6100 | $(1+i)\,x^3 + (2+2i)\,x^2 + (1+2i)\,x + 1$ |
| 6241 | $(1+i)\,x^3 + 5ix^2 + (-4+5i)\,x - 2$ |
| 6304 | $x^3 + (2+2i)\,x^2 + ix - 2i$ |
| 6304 | $x^3 + (2+2i)\,x^2 + ix + 2$ |
| 6553 | $x^3 + (1+2i)\,x^2 + (-2+i)\,x - 2$ |
| 6553 | $x^3 + (2+i)\,x^2 + (2+i)\,x + 2i$ |
| 6561 | $x^3 + 3ix + (-2-i)$ |
| 6561 | $x^3 + 3ix + (1+2i)$ |
| 6561 | $x^3 + 3x - i$ |
| 6561 | $(1+i)\,x^3 + 3ix^2 + 3ix + 2i$ |
| 6569 | $x^3 + 2ix^2 + (-1-i)\,x + (2+i)$ |
| 6569 | $x^3 + 2x^2 + (1-i)\,x + (-1-2i)$ |
| 6625 | $x^3 + (1+2i)\,x^2 + (2-i)$ |
| 6625 | $x^3 + (2+i)\,x^2 + (1-2i)$ |

| | |
|---|---|
| 6889 | $x^3 + 2x^2 + 2x - 1$ |
| 6928 | $x^3 + 2ix^2 - ix + 2i$ |
| 6928 | $x^3 + 2x^2 - ix - 2$ |
| 7072 | $(1+i)\,x^3 + 4ix^2 + (-3+2i)\,x - 2$ |
| 7072 | $(1+i)\,x^3 + 4ix^2 + (-2+3i)\,x - 2$ |
| 7200 | $x^3 + ix^2 + (1-i)\,x + (-1-i)$ |
| 7200 | $x^3 + x^2 + (-1-i)\,x + (1+i)$ |
| 7265 | $x^3 + (1+2i)\,x^2 + (-2-i)\,x - 2i$ |
| 7265 | $x^3 + (2+i)\,x^2 + (2-i)\,x + 2$ |
| 7328 | $x^3 + (1+2i)\,x^2 + (-3+3i)\,x + (-3-i)$ |
| 7328 | $x^3 + (2+i)\,x^2 + (3+3i)\,x + (1+3i)$ |
| 7345 | $x^3 + (1+2i)\,x^2 + (-3+i)\,x + (1-2i)$ |
| 7345 | $x^3 + (2+i)\,x^2 + (3+i)\,x + (2-i)$ |
| 7345 | $x^3 + (2+2i)\,x^2 + (1-2i)$ |
| 7345 | $x^3 + (2+2i)\,x^2 + (2-i)$ |
| 7396 | $x^3 + 2ix + (1-i)$ |
| 7460 | $x^3 + 2ix^2 + (-3+i)\,x + (-1-3i)$ |
| 7460 | $x^3 + 2x^2 + (3+i)\,x + (3+i)$ |
| 7529 | $x^3 + ix^2 + (-1-2i)\,x + 2$ |
| 7529 | $x^3 + x^2 + (1-2i)\,x - 2i$ |
| 7569 | $x^3 + 2x^2 + 3x + 3$ |
| 7684 | $x^3 + 2ix^2 - 4x + (1-3i)$ |
| 7684 | $x^3 + 2x^2 + 4x + (3-i)$ |
| 7760 | $x^3 + (1+2i)\,x^2 + (-3+i)\,x + (-1-3i)$ |
| 7760 | $x^3 + (2+i)\,x^2 + (3+i)\,x + (3+i)$ |
| 7801 | $x^3 + ix^2 - 2x + (1-2i)$ |
| 7801 | $x^3 + x^2 + 2x + (2-i)$ |
| 7888 | $x^3 + (1+2i)\,x^2 + (-3+3i)\,x + (-1-i)$ |
| 7888 | $x^3 + (2+i)\,x^2 + (3+3i)\,x + (1+i)$ |
| 7921 | $(1+i)\,x^3 + (2+i)\,x^2 + x + (1-i)$ |
| 7988 | $(1+i)\,x^3 + (1+5i)\,x^2 + (-1+6i)\,x + (-2+2i)$ |
| 7988 | $(1+i)\,x^3 + (2+2i)\,x^2 + x - 1$ |
| 8065 | $x^3 + ix^2 + (-1+i)\,x + (-1-2i)$ |
| 8065 | $x^3 + x^2 + (1+i)\,x + (2+i)$ |
| 8080 | $x^3 + 2ix^2 + (-4+i)\,x - 2i$ |
| 8080 | $x^3 + 2x^2 + (4+i)\,x + 2$ |
| 8081 | $x^3 + 2ix^2 + (-4-i)\,x + (1-2i)$ |
| 8081 | $x^3 + 2x^2 + (4-i)\,x + (2-i)$ |
| 8185 | $x^3 + (1+2i)\,x^2 + (-2+i)\,x + (-2-2i)$ |
| 8185 | $x^3 + (2+i)\,x^2 + (2+i)\,x + (2+2i)$ |
| 8212 | $(1+i)\,x^3 + (1+5i)\,x^2 + (-2+5i)\,x + (-2+2i)$ |
| 8212 | $(1+i)\,x^3 + (2+2i)\,x^2 + (2+i)\,x - i$ |
| 8324 | $x^3 + (1+2i)\,x^2 + (-2+3i)\,x + (-1-2i)$ |
| 8324 | $x^3 + (2+i)\,x^2 + (2+3i)\,x + (2+i)$ |
| 8420 | $x^3 + ix^2 + x + (-1+2i)$ |
| 8420 | $x^3 + x^2 - x + (-2+i)$ |
| 8480 | $(1+i)\,x^3 + (1+2i)\,x^2 + 2ix + (1+i)$ |
| 8480 | $(1+i)\,x^3 + (2+5i)\,x^2 + (-1+7i)\,x + (-1+2i)$ |
| 8489 | $x^3 + ix^2 + (-2-2i)\,x + i$ |
| 8489 | $x^3 + x^2 + (2-2i)\,x - 1$ |

| | |
|---|---|
| 8545 | $x^3 + (1+2i)\,x^2 + x + 2$ |
| 8545 | $x^3 + (2+i)\,x^2 - x - 2i$ |
| 8577 | $x^3 + 2ix^2 + (-2+2i)\,x + (-2+i)$ |
| 8577 | $x^3 + 2x^2 + (2+2i)\,x + (-1+2i)$ |
| 8585 | $x^3 + ix^2 + (-1-3i)\,x + (1-2i)$ |
| 8585 | $x^3 + x^2 + (1-3i)\,x + (2-i)$ |
| 8585 | $x^3 + (1+2i)\,x^2 + (-3+i)\,x + (-2-3i)$ |
| 8585 | $x^3 + (2+i)\,x^2 + (3+i)\,x + (3+2i)$ |
| 8608 | $x^3 + 2ix^2 + (-2+i)\,x + (-2-2i)$ |
| 8608 | $x^3 + 2x^2 + (2+i)\,x + (2+2i)$ |
| 8705 | $x^3 + 2ix^2 + (-4-i)\,x + (-1-2i)$ |
| 8705 | $x^3 + 2x^2 + (4-i)\,x + (2+i)$ |
| 8713 | $x^3 + (2+2i)\,x^2 + (-1+5i)\,x + (-4+i)$ |
| 8713 | $x^3 + (2+2i)\,x^2 + (1+5i)\,x + (-1+4i)$ |
| 8852 | $x^3 + ix^2 + 2x + (-1-i)$ |
| 8852 | $x^3 + x^2 - 2x + (1+i)$ |
| 8980 | $x^3 + (1+2i)\,x^2 + (-2+4i)\,x + (-3+i)$ |
| 8980 | $x^3 + (2+i)\,x^2 + (2+4i)\,x + (-1+3i)$ |
| 9065 | $x^3 + (1+2i)\,x^2 + (1+i)\,x + (2+i)$ |
| 9065 | $x^3 + (2+i)\,x^2 + (-1+i)\,x + (-1-2i)$ |
| 9113 | $x^3 + ix^2 + (-1+i)\,x + (-2-i)$ |
| 9113 | $x^3 + x^2 + (1+i)\,x + (1+2i)$ |
| 9161 | $x^3 + 2ix^2 - 3x + (-2-i)$ |
| 9161 | $x^3 + 2x^2 + 3x + (1+2i)$ |
| 9169 | $x^3 + (2+2i)\,x^2 - x + (1-2i)$ |
| 9169 | $x^3 + (2+2i)\,x^2 + x + (2-i)$ |
| 9248 | $x^3 + 2ix^2 + (-2+3i)\,x + (-2-2i)$ |
| 9248 | $x^3 + 2x^2 + (2+3i)\,x + (2+2i)$ |
| 9297 | $x^3 + ix^2 - 2ix + (2+i)$ |
| 9297 | $x^3 + x^2 - 2ix + (-1-2i)$ |
| 9409 | $x^3 + (2+2i)\,x^2 + (-3+4i)\,x + (-6+i)$ |
| 9409 | $x^3 + (2+2i)\,x^2 + (3+4i)\,x + (-1+6i)$ |
| 9425 | $x^3 + (-2+i)\,x + (-2+i)$ |
| 9425 | $x^3 + (2+i)\,x + (-1+2i)$ |
| 9505 | $x^3 + (1+2i)\,x^2 + (-4+i)\,x + (-2-2i)$ |
| 9505 | $x^3 + (2+i)\,x^2 + (4+i)\,x + (2+2i)$ |
| 9521 | $x^3 + (1+2i)\,x^2 + (-3+i)\,x + (-3-2i)$ |
| 9521 | $x^3 + (2+i)\,x^2 + (3+i)\,x + (2+3i)$ |
| 9540 | $x^3 + 2ix^2 + (-3+i)\,x + (1-i)$ |
| 9540 | $x^3 + 2x^2 + (3+i)\,x + (1-i)$ |
| 9593 | $x^3 + ix^2 + (-1+3i)\,x + (-2-i)$ |
| 9593 | $x^3 + x^2 + (1+3i)\,x + (1+2i)$ |
| 9649 | $x^3 + (1+i)\,x^2 + (-2-i)\,x - 3i$ |
| 9649 | $x^3 + (1+i)\,x^2 + (2-i)\,x + 3$ |
| 9700 | $x^3 + ix^2 + ix + (-2+i)$ |
| 9700 | $x^3 + x^2 + ix + (-1+2i)$ |
| 9760 | $x^3 + (1+i)\,x^2 + 3ix + (-1-i)$ |
| 9760 | $x^3 + (1+i)\,x^2 + 3ix + (1+i)$ |
| 9764 | $x^3 + ix^2 - 3x + (1-2i)$ |
| 9764 | $x^3 + x^2 + 3x + (2-i)$ |

| | |
|---|---|
| 9972 | $x^3 + (1+2i)\,x^2 + (-2+2i)\,x + (-3-i)$ |
| 9972 | $x^3 + (2+i)\,x^2 + (2+2i)\,x + (1+3i)$ |
| 10000 | $x^3 + (1+i)\,x^2 - ix + (-1+i)$ |

# Appendix A

## A.1 Taniguchi's theorem

**Definition A.1.1.** *Let $\mathcal{O}$ be a Dedekind domain.*

- *Let $\mathcal{C}(\mathcal{O})$ be the set of "cubic algebras" that is, isomorphism classes of $\mathcal{O}$-algebras that are projective of rank 3 as $\mathcal{O}$-modules.*
- *For every fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ we define*

$$\mathcal{C}(\mathcal{O},\mathfrak{a}) = \{R \in \mathcal{C}(\mathcal{O}) \mid \mathrm{St}(R) = \overline{\mathfrak{a}}\},$$

*where $\mathrm{St}(R) \in Cl(\mathcal{O})$ is the Steinitz class of $R$. Let further*

$$G_{\mathfrak{a}} = \left\{ \begin{pmatrix} \alpha \in \mathcal{O} & \beta \in \mathfrak{a}^{-1} \\ \gamma \in \mathfrak{a} & \delta \in \mathcal{O} \end{pmatrix} \;\middle|\; \alpha\delta - \beta\gamma \in \mathcal{O}^{\times} \right\},$$

$$V_{\mathfrak{a}} = \{F = (a,b,c,d) \mid a \in \mathfrak{a}, b \in \mathcal{O}, c \in \mathfrak{a}^{-1}, d \in \mathfrak{a}^{-2}\}.$$

- *If $F \in V_{\mathfrak{a}}$, its discriminant $\mathrm{disc}(F) = b^2c^2 - 27a^2d^2 + 18abcd - 4ac^3 - 4b^3d$ belongs to $\mathfrak{a}^{-2}$.*
- *We consider elements of $V_{\mathfrak{a}}$ as binary cubic forms so $(a,b,c,d) = ax^3 + bx^2y + cxy^2 + dy^3$ and we define the action of $G_{\mathfrak{a}}$ on $V_{\mathfrak{a}}$ by*

$$M.F = (\det M)^{-1} F(\alpha x + \gamma y, \beta x + \delta y),$$

*where $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G_{\mathfrak{a}}$ (this twisted action makes the representation faithful, the usual one has kernel $\mu_3$).*

**Theorem A.1.2** (Taniguchi)**.** *There exists a canonical bijection between $\mathcal{C}(\mathcal{O},\mathfrak{a})$ and $V_{\mathfrak{a}}/G_{\mathfrak{a}}$ such that the following diagram is commutative:*

$$\begin{array}{ccc} V_{\mathfrak{a}}/G_{\mathfrak{a}} & \longrightarrow & \mathcal{C}(\mathcal{O},\mathfrak{a}) \\ {\scriptstyle \mathrm{disc}}\downarrow & & \downarrow{\scriptstyle \mathfrak{d}} \\ \mathfrak{a}^{-2}/(\mathcal{O}^{\times})^2 & \xrightarrow{\times \mathfrak{a}^2} & \{\textit{integral ideals of } \mathcal{O}\} \end{array}$$

*where $\mathfrak{d}$ is the relative discriminant ideal map.*

*Proof.* For the sake of completeness, we reprove this theorem in this Appendix.

We will not strictly follow Taniguchi's proof, but we will also take some elements from previous proofs of the result over $\mathbb{Z}$ ([28], [34], [5] and [7]).

Let $R \in \mathcal{C}(\mathcal{O}, \mathfrak{a})$. Let us choose a representative of an element $R \in \mathcal{C}(\mathcal{O}, \mathfrak{a})$ in the form

$$R = 1_R \cdot \mathcal{O} + \omega_1 \cdot \mathcal{O} + \omega_2 \cdot \mathfrak{a},$$

for appropriate $\omega_1, \omega_2, \omega_3 \in \mathrm{Frac}(R) := R \otimes_{\mathcal{O}} K$.

Let us write

$$\omega_1\omega_2 = \alpha + \beta\omega_1 + \gamma\omega_2;$$

since $\omega_1(\mathfrak{a}\omega_2) \subset R$, we have $\alpha, \beta \in \mathfrak{a}^{-1}$ and $\gamma \in \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$.

Hence we can normalize our basis $\omega_1, \omega_2$ by replacing it by $\omega_1 - \gamma$ and $\omega_2 - \beta$, if needed, to obtain $\mathfrak{a}\omega_1\omega_2 \in \mathcal{O} \cdot 1_R$

We know that a cubic ring with a normalized basis is determined up to isomorphism by the products

$$\begin{cases} \omega_1^2 = j - b\omega_1 + a\omega_2 \\ \omega_2^2 = l - d\omega_1 + c\omega_2 \\ \omega_1\omega_2 = m \end{cases} \tag{A.1}$$

By associativity of the product (in particular $\omega_1 \cdot (\omega_2^2) = (\omega_1\omega_2) \cdot \omega_2$) we obtain

$$\begin{cases} l = -bd \\ m = -ad \\ j = -ac \end{cases}, \tag{A.2}$$

so $R$ is determined up to isomorphism by $(a, b, c, d)$, and since $\mathcal{O}\omega_1^2, \mathfrak{a}^2\omega_2^2 \subset R$ we have

$$a \in \mathfrak{a}, \quad b \in \mathcal{O}, \quad c \in \mathfrak{a}^{-1}, \quad d \in \mathfrak{a}^{-2},$$

So we define $\phi : \mathcal{C}(\mathcal{O}, \mathfrak{a}) \longrightarrow V_{\mathfrak{a}}$, which associates to a representative $R \in \mathcal{C}(\mathcal{O}, \mathfrak{a})$ the element $(a, b, c, d) \in V_{\mathfrak{a}}$ given by the product laws (A.1) and we define $\psi : V_{\mathfrak{a}} \longrightarrow \mathcal{C}(\mathcal{O}, \mathfrak{a})$ which associates to an element $(a, b, c, d) \in V_{\mathfrak{a}}$ the $\mathcal{O}$-module $\mathcal{O} \oplus \mathcal{O} \oplus \mathfrak{a}$ provided by the multiplication law given by (A.1) and (A.2), which makes it an $\mathcal{O}$-algebra.

Now $\mathcal{C}(\mathcal{O}, \mathfrak{a})$ is defined modulo isomorphism, so we have to take into account basis changes. Let us consider matrices $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_2(K)$ $(K = Fr(\mathcal{O}))$, with discriminant $ad - bc \in \mathcal{O}^\times$. It is easy to prove that the subgroup which fixes $R/\mathcal{O} = \mathcal{O} \oplus \mathfrak{a}$ by left multiplication is exactly $G_{\mathfrak{a}}$.

Moreover, once we apply this basis change, computations will show that the binary cubic form $(a', b', c', d') \in V_{\mathfrak{a}}$ corresponding to $\langle \omega_1', \omega_2' \rangle$ will be obtained by the action of $M$ on $(a, b, c, d)$. So we have finished the proof of the bijection.

Let us prove that the diagram is commutative.

Is is sufficient to prove it locally, so we can assume that $\mathcal{O}$ is a discrete valuation ring, so we are in the case of a principal ideal domain. First of all remark that $\mathfrak{d}$ is well-defined since an $\mathcal{O}$-algebras isomorphism preserves the discriminant.

Since $\langle 1, \omega_1, \omega_2 \rangle$ is a basis of $R$ we have that the discriminant of the ring is

$$\begin{aligned} D_R = D\langle 1, \omega_1, \omega_2 \rangle &= \begin{vmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\omega_1) & \mathrm{Tr}(\omega_2) \\ \mathrm{Tr}(\omega_1) & \mathrm{Tr}(\omega_1^2) & \mathrm{Tr}(\omega_1\omega_2) \\ \mathrm{Tr}(\omega_2) & \mathrm{Tr}(\omega_1\omega_2) & \mathrm{Tr}(\omega_2^2) \end{vmatrix} \\ &= \begin{vmatrix} 3 & -b & c \\ -b & b^2 - 2ac & -3ad \\ c & -3ad & c^2 - 2bd \end{vmatrix} \\ &= b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2 = \mathrm{disc}(a, b, c, d). \end{aligned}$$

Finally, since $R = 1 \cdot \mathcal{O} \oplus \omega_1 \cdot \mathcal{O} \oplus \omega_2 \cdot \mathfrak{a}$ and this is a pseudo-basis, then the formula for the relative discriminant ideal is

$$\mathfrak{d}(R) = \mathrm{disc}(a, b, c, d) \cdot \mathfrak{a}^2,$$

and we conclude. □

# Appendix B

## B.1 Another algorithm to enumerate cubic extensions

Another way to list cubic extensions of a given number field $K$ is given by class field theory.

In fact we know there is a bijection between Abelian extensions $L/K$ (modulo isomorphism) and equivalence classes of congruence subgroups $(\mathfrak{m}, A_{\mathfrak{m}}(L/K))$ where $\mathfrak{m}$ is a suitable modulus for the extension $L/K$ and $A_{\mathfrak{m}}$ denotes the Artin group associated to the modulus $\mathfrak{m}$ and the extension $L/K$ [12, Theorem 3.5.1].

### B.1.1 Quadratic extensions

Let $K$ be a number field. Since quadratic extensions are all Abelian, we can just apply the bijection to list all the extensions $K_2/K$ of degree 2.

**Algorithm 5** (List of relative quadratic extensions)**.** [12, Algorithm 9.2.4] *Given a number field $K$ and a bound $B$, this algorithm outputs a list of all relative extensions $K_2/K$ of degree 2, modulo isomorphism such that $\mathcal{N}(\mathfrak{d}(K_2/K)) \leq B$.*

(1) Compute the list $\mathcal{L}_0$ of all the ideals $\mathfrak{m}_0$ of norm $\leq B$ which are conductors at 2 (i.e. for all $\mathfrak{p} \mid \mathfrak{m}_0$, $v_{\mathfrak{p}}(\mathfrak{m}_0) = 1$ if $\mathfrak{p} \nmid 2$, while $2 \leq v_{\mathfrak{p}}(\mathfrak{m}_\circ) \leq 2e(\mathfrak{p}/2) + 1$ if $\mathfrak{p} \mid 2$).

(2) Compute the list $\mathcal{L}$ of all moduli of the form $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, with $\mathfrak{m}_0 \in \mathcal{L}_0$ and $\mathfrak{m}_\infty$ ranges through all the subsets of the real places of $K$.

(3) For $i = 1,\ldots,|\mathcal{L}|$, let $\mathfrak{m}$ the $i$-th modulus of the list $\mathcal{L}$. If $\mathfrak{m}$ is not a conductor of $(\mathfrak{m}, P_{\mathfrak{m}})$ or $h_{\mathfrak{m}}$ odd, go to step 3.

(4) Compute the list $\mathcal{C}$ of all subgroups $C$ of index 2 of $Cl_{\mathfrak{m}}$.

(5) For $j = 1,\ldots,|\mathcal{C}|$, let $C$ be the $j$-th element of $\mathcal{C}$. Check if $\mathfrak{m}$ is a conductor of $(\mathfrak{m}, C)$, otherwise go to step 5.

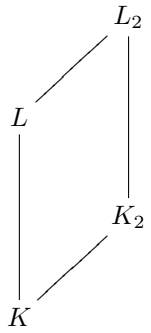
(6) Compute the defining polynomial of the extension $K_2/K$ corresponding to the equivalence class of $(\mathfrak{m}, C)$.

### B.1.2 Cubic extensions

The algorithm listing cyclic cubic extensions is analogous to Algorithm 5 and it is given in [12, Algorithm 9.2.5], so we will omit it here.

So let us consider only the noncyclic case.

Let $K$ be a number field, $L/K$ a noncyclic extension, $N$ the Galois closure of this extension (so $\mathrm{Gal}(N/K)$ is isomorphic to $D_3$) and $K_2$ the only quadratic extension of $K$ contained in $N$.




Theorem 9.2.6 ([12]) give us properties of this kind of extensions (more generally for dihedral extensions $L_2/K$ with Galois group $D_n$).

In particular, when $n = 3$, we know that the conductor of the extension $L_2/K_2$ is of the form $\mathfrak{a}\mathcal{O}_{K_2}$, for some ideal $\mathfrak{a}$ of $\mathcal{O}_K$ and that $\mathfrak{d}(L/K) = \mathfrak{d}(K_2/K)\mathfrak{a}^2$,. The following algorithm lists all cubic noncyclic extensions of $K$ of bounded relative discriminant:

**Algorithm 6.** *[List of relative noncyclic cubic extensions]*

*Given a number field $K$, and a bound $B$, this algorithm outputs a list of all relative extensions $L/K$ of degree 3, modulo isomorphism, such that $\mathcal{N}\mathfrak{d}(L/K) \leq B$.*

(1) Compute the list $\mathcal{L}_0$ of all the ideals $\mathfrak{a}$ of $K$ of norm $\leq B^{1/2}$ which are conductors at 3, except that we allow $v_{\mathfrak{p}}(\mathfrak{a}) = 1$ for $\mathfrak{p} \mid 3$.

(2) Compute the list $\mathcal{Q}$ of quadratic extensions $K_2/K$ up to $K$-isomorphism such that $\mathcal{N}(\mathfrak{d}(K_2/K)) \leq B$.

(3) For $i = 1, \ldots, |\mathcal{Q}|$ let $K_2$ be the $i$-th element of $\mathcal{Q}$, let $\mathfrak{d} = \mathfrak{d}(K_2/K)$, and let $\tau$ be the generator of $\mathrm{Gal}(K_2/K)$.

(4) Let $\mathcal{L}_1$ be the sublist of the ideals $\mathfrak{a}$ of $\mathcal{L}_0$ such that

$$\mathcal{N}(\mathfrak{a}) \leq \left(\frac{B}{\mathcal{N}\mathfrak{d}(K_2/K)}\right)^{1/2},$$

and such that if $\mathfrak{p} \nmid 3$ and $\mathfrak{p} \mid \mathfrak{a}$ then $\mathfrak{p} \nmid \mathfrak{d}$; if $\mathfrak{p} \mid 3$ and $v_{\mathfrak{p}}(\mathfrak{a}) = 1$ , then $\mathfrak{p} \mid \mathfrak{d}$; and finally if $\mathfrak{p} \mid 3$, $e(\mathfrak{p}/3)$ is even and $v_{\mathfrak{p}}(\mathfrak{a}) = \lfloor 3e(\mathfrak{p}/3)/2 \rfloor + 1$, then $\mathfrak{p} \nmid \mathfrak{d}$. Compute the list $\mathcal{L}_2$ of ideals $\mathfrak{m}_0$ of $K_2$ of the form $\mathfrak{m}_0 = \mathfrak{a}\mathbb{Z}_{K_2}$, with $\mathfrak{a} \in \mathcal{L}_1$.

(5) For $j = 1, \ldots, |\mathcal{L}_2|$ let $\mathfrak{m}$ be the modulus whose finite part $\mathfrak{m}_0$ is the $j$-th element of $\mathcal{L}_2$ and with $\mathfrak{m}_\infty = \emptyset$. Check whether $\mathfrak{m}$ is the conductor of $(\mathfrak{m}, P_{\mathfrak{m}})$. If not go to step 5.

(6) Compute the list $\mathcal{C}$ of all the congruence subgroups $C$ of $I_{\mathfrak{m}}(K_2)$ of index 3.

(7) For $c = 1, \dots, |\mathcal{C}|$ let $C$ be the $c$-th congruence subgroup of $\mathcal{C}$, check if $\mathfrak{m}$ is the conductor of $(\mathfrak{m}, C)$. If not or if $\tau(C) \neq C$, go to step 7.

(8) Test if $\tau(I) = I^{-1}$ in $Cl_{\mathfrak{m}}(K_2)/C$ i.e. test if $\mathcal{N}_{K_2/K} I = 1$ in $Cl_{\mathfrak{m}}(K_2)/C$.

(9) $(\mathfrak{m}, C)$ is the conductor of a suitable cyclic cubic extension of $K_2$. Using Kummer theory, compute a defining polynomial $P(X) \in K_2[X]$ for the cubic extension $L_2/K_2$ corresponding to $(\mathfrak{m}, C)$.

(10) Let $P_c = P^{\tau}(X)$ be the polynomial obtained by applying $\tau$ to all the coefficients of $P$. Set $Q(X) = \mathcal{R}_Y(P_c(Y), P(X - Y))$, where $\mathcal{R}_Y$ denotes the resultant in the variable $Y$. Then $Q(X) \in K[X]$. Factor $Q(X)$ in $K[X]$, output one of the irreducible factors of $Q(X)$ of degree 3 in $K[X]$ (it will have one) as a defining polynomial for $L/K$, and go to step 7.

**Remarks**. We took the previous algorithms from [12], fixing some small mistakes in the algorithm for noncyclic cubic extensions

(1) In step 4 the conditions on $\mathfrak{p} \mid \mathfrak{a}$ are not clear: [12] says "...and finally if $\mathfrak{p} \mid 3$ and $v_{\mathfrak{p}}(\mathfrak{a}) = 3e(\mathfrak{p}/3)/2 + 1$, then $\mathfrak{p} \nmid \mathfrak{d}$" in fact, the equality implies that $e(\mathfrak{p}/3)$ is even, so when it is odd we can just skip the test. Moreover, when $\mathfrak{p} \nmid 3$, there should be a condition saying that $v_{\mathfrak{p}}(\mathfrak{a}) = 1$, but in fact this was already tested on step 1.

(2) In step 5 "terminate the algorithm" must be replaced by "go to step 3"

(3) In steps $7-8$. In fact for each $C \in \mathcal{C}$ it is not sufficient to test wether $\mathfrak{m}$ is the conductor of $(\mathfrak{m}, C)$, but we need to check also if $\tau(C) = C$. Thanks to [12, Theorem 9.2.6]it is sufficient to test the condition $\tau(\overline{I}) = \overline{I^{-1}}$, where

$$Cl_{\mathfrak{m}}(K_2)/\overline{C} = \left\langle \overline{I} \right\rangle .$$

(4) In the original algorithm in [12], to get the lists $\mathcal{L}, \mathcal{L}_0$, and so on, you first construct the list of all ideals up to some bound $B$ and then select the ones satisfying the given conditions (by factoring them). It is much more straightforward to construct directly those ideals, and it make a big gain of time and space in the algorithm. The first thing to remark is that for all prime ideals $\mathfrak{p}$ in $\mathbb{Z}_K$, apart from the ones above 2 and 3 the only possible exponent is 1. So we can directly make the list of all these ideals (just using a loop on prime ideals over $\mathbb{Z}$, factoring them over $\mathbb{Z}_K$ and making all the possible products), then we multiply for the allowed powers of $\mathfrak{p}_2$ and $\mathfrak{p}_3$ (which depend on the step of the algorithm we are : quadratic extensions, cubic extensions,...).

(5) We can also avoid to factor the ideals of $\mathcal{L}_0$ to test the condition in step (4) of Algorithm 6. Indeed, we can define $\mathfrak{a}_3 = \mathrm{lcm}(\mathfrak{a}, 3^2)$ and $\mathfrak{a}_0 = \mathfrak{a}/\mathfrak{a}_0$. Then we just need to test if $\mathrm{lcm}(\mathfrak{a}_0, \mathfrak{d}) = 1$ and if $\mathfrak{a}_3 = \mathfrak{p}_3$ then $\mathrm{lcm}(\mathfrak{d}, \mathfrak{p}_3) \neq 1$.

# Appendix C

## C.1 Approximation errors in Algorithm 2

**Proposition C.1.1.** *Let $F(x) = ax^3 + bx^2 + cx + d$ be our cubic polynomial. If we compute its roots $\alpha_1, \alpha_2, \alpha_3$ with relative precision $\varepsilon$, that is*

$$|\alpha_i - \hat{\alpha}_i| < \varepsilon |\alpha_i|, \tag{C.1}$$

*for $i = 1, 2, 3$, and we suppose that we are working with exact arithmetic (i.e. computing operations does not add any error term to our expressions) then we have*

$$\max\left\{|P - \hat{P}|, |Q - \hat{Q}|, |R - \hat{R}|\right\} \leq \frac{1971}{2} \cdot X \cdot \varepsilon, \tag{C.2}$$

*where $\hat{P}$, $\hat{Q}$ and $\hat{R}$ are the values computed for $P, Q, R$ respectively, using the approximations $\hat{\alpha}_i$ instead of the $\alpha_i$.*

*Proof.* Let us recall that $t_i^2 = |a|^2 |\alpha_j - \alpha_k|^2$, with $\{i, j, k\} = \{1, 2, 3\}$. Now

$$||\alpha_j - \alpha_k| - |\hat{\alpha}_j - \hat{\alpha}_k|| \leq |\alpha_j - \hat{\alpha}_j| + |\alpha_k - \hat{\alpha}_k| \leq \varepsilon(|\alpha_j| + |\alpha_k|)),$$

so

$$|t_i - \hat{t}_i| \leq \varepsilon |a| (|\alpha_j| + |\alpha_k|). \tag{C.3}$$

Moreover

$$|t_i^2 - \hat{t}_i^2| \leq |t_i + \hat{t}_i||t_i - \hat{t}_i| \leq (2t_i + \varepsilon|a|(|\alpha_j| + |\alpha_k|)) \cdot \varepsilon |a| (|\alpha_j| + |\alpha_k|)$$

and $t_i \leq |a| \left(|\alpha_j| + |\alpha_k|\right)$ so we get

$$|t_i^2 - \hat{t}_i^2| \leq \varepsilon |a|^2 (2 + \varepsilon)(|\alpha_j| + |\alpha_k|)^2. \tag{C.4}$$

Now we develop $P$

$$\begin{aligned} |P - \hat{P}| &\leq |t_1^2 - \hat{t}_1^2| + |t_2^2 - \hat{t}_2^2| + |t_3^2 - \hat{t}_3^2| \\ &\leq \varepsilon |a|^2 (2 + \varepsilon) \left((|\alpha_2| + |\alpha_3|)^2 + (|\alpha_1| + |\alpha_3|)^2 + (|\alpha_1| + |\alpha_2|)^2\right) \\ &\leq 2 \cdot \varepsilon |a|^2 (2 + \varepsilon) \left(|\alpha_1| + |\alpha_2| + |\alpha_3|\right)^2. \end{aligned}$$

Now we can bound $|\alpha_i|$

$$|\alpha_i| \leq \gamma^{1/2} \frac{X^{1/4}}{|a|},$$

and in particular when $K = \mathbb{Q}(i)$ we have

$$|\alpha_i| \leq \frac{1}{|a|}\left(\frac{27X}{2}\right)^{1/4}.$$

Let us call

$$c_\alpha = \gamma^{1/2} X^{1/4},$$

(remark that $c_\alpha > 1$ for every $X > 1$) so that

$$|\alpha_i| \leq \frac{c_\alpha}{|a|}. \tag{C.5}$$

So

$$\left(|\alpha_1| + |\alpha_2| + |\alpha_3|\right)^2 \leq \frac{9}{|a|^2} c_\alpha^2.$$

And finally

$$|P - \hat{P}| \leq 2 \cdot \varepsilon |a|^2 (2+\varepsilon) \cdot \frac{9}{|a|^2} \cdot c_\alpha^2$$

so

$$|P - \hat{P}| \leq 18 \cdot \varepsilon \cdot (2+\varepsilon) \cdot c_\alpha^2 \tag{C.6}$$

Let us call

$$c_P = 18 \cdot \varepsilon \cdot (2+\varepsilon) \cdot c_\alpha^2 \tag{C.7}$$

for simplicity.

When we look at $Q$ we have

$$|Q - \hat{Q}| \leq |\alpha_1 t_1^2 - \hat{\alpha}_1 \hat{t}_1^2| + |\alpha_2 t_2^2 - \hat{\alpha}_2 \hat{t}_2^2| + |\alpha_3 t_3^2 - \hat{\alpha}_3 \hat{t}_3^2|$$

Now for each triple $i, j, k$ with $\{i, j, k\} = \{1, 2, 3\}$, we have

$$\begin{aligned}
|\alpha_i t_i^2 - \hat{\alpha}_i \hat{t}_i^2| &\leq |\alpha_i t_i^2 - (\alpha_i \pm \varepsilon\alpha_i)\hat{t}_i^2| \\
&\leq |\alpha_i t_i^2 - \alpha_i \hat{t}_i^2| + |\varepsilon \alpha_i \hat{t}_i^2| \\
&\leq |\alpha_i||t_i^2 - \hat{t}_i^2| + \varepsilon|\alpha_i| \left(t_i^2 + \varepsilon\,|a|^2\,(2+\varepsilon)(|\alpha_j| + |\alpha_k|)^2\right)
\end{aligned}$$

So

$$\begin{aligned}
|Q - \hat{Q}| &\leq \frac{c_\alpha}{|a|} c_P + \varepsilon \frac{c_\alpha}{|a|}(1 + (2+\varepsilon)\varepsilon)\,|a|^2 \cdot 2(|\hat{\alpha}_1| + |\hat{\alpha}_2| + |\hat{\alpha}_3|)^2 \\
&\leq \frac{c_\alpha}{|a|} c_P + \varepsilon \frac{c_\alpha}{|a|}(1 + (2+\varepsilon)\varepsilon) \cdot 18 c_\alpha^2.
\end{aligned}$$

Finally for $R$ we have

$$|R - \hat{R}| \leq \left||\alpha_1|^2 t_1^2 - |\hat{\alpha}_1|^2 \hat{t}_1^2\right| + \left||\alpha_2|^2 t_2^2 - |\hat{\alpha}_2|^2 \hat{t}_2^2\right| + \left||\alpha_3|^2 t_3^2 - |\hat{\alpha}_3|^2 \hat{t}_3^2\right|.$$

Now, since $|\hat{\alpha}_i|^2 \leq |\alpha_i|^2 + 2 \cdot \varepsilon |\alpha_i|^2 + \varepsilon^2 |\alpha_i|^2$,

$$\begin{aligned}
\left||\alpha_i|^2 t_i^2 - |\hat{\alpha}_i|^2 \hat{t}_i^2\right| &\leq \left||\alpha_i|^2 t_i^2 - \left(|\alpha_i|^2 \pm (2 \cdot \varepsilon + \varepsilon^2)|\alpha_i|^2\right) \hat{t}_i^2\right| \\
&\leq |\alpha_i|^2 |t_i^2 - \hat{t}_i^2| + (2 \cdot \varepsilon + \varepsilon^2)|\alpha_i|^2 |\hat{t}_i|^2 \\
&\leq |\alpha_i|^2 |t_i^2 - \hat{t}_i^2| + (2 \cdot \varepsilon + \varepsilon^2)|\alpha_i|^2 (t_i^2 + \varepsilon(2+\varepsilon)\,|a|^2\,(|\alpha_j| + |\alpha_k|)^2).
\end{aligned}$$

So

$$\begin{aligned} |R - \hat{R}| &\leq \frac{c_\alpha^2}{|a|^2} c_P + (2 \cdot \varepsilon + \varepsilon^2) \frac{c_\alpha^2}{|a|^2} |a|^2 (1 + \varepsilon(2+\varepsilon)) 2(|\alpha_1| + |\alpha_2| + |\alpha_2|)^2 \\ &\leq \frac{c_\alpha^2}{|a|^2} c_P + 18 \cdot (2 \cdot \varepsilon + \varepsilon^2)(1 + \varepsilon(2+\varepsilon)) \cdot \frac{c_\alpha^4}{|a|^4}. \end{aligned}$$

Putting rougher bounds we get

$$\begin{aligned} |P - \hat{P}| &\leq 37 c_\alpha^2 \cdot \varepsilon \\ |Q - \hat{Q}| &\leq 55 c_\alpha^3 \cdot \varepsilon \\ |R - \hat{R}| &\leq 73 c_\alpha^4 \cdot \varepsilon, \end{aligned}$$

and we can conclude. □

**Corollary C.1.2.** *Let us suppose $K = Q(i)$, $X \leq 10^5$, $\varepsilon = 10^{-38}$ and that we are working with exact arithmetic, then the error that appears when we test border conditions is bounded by $\varepsilon \leq 2 \cdot 10^{-30}$.*

Up to now, we assumed exact arithmetic, and the error comes only from the $\alpha_i$ which are approximate values. In reality, we have also to take into account the error coming from floating point computations. For all basic operations $+$, $\times$, $-$, $/$, let us note $\oplus$ $\otimes$, $\ominus$, $\oslash$ the corresponding machine operation. For all $* \in \{+, -, \times, /\}$, we suppose that

$$|(a * b) - (a \circledast b)| \leq \varepsilon |a * b|$$

for any $a$ and $b$ in $\mathbb{R}$.

By induction we obtain the following proposition

**Proposition C.1.3.** *Let $x = (x_1, \ldots, x_k) \in \mathbb{C}^k$, and define*

$$S_k = x_1 \oplus x_2 \oplus \cdots \oplus x_k,$$

$$P_k = x_1 \otimes x_2 \otimes \cdots \otimes x_k.$$

*Then*

$$\left| S_k - \sum_{i=1}^{k} x_i \right| \leq \left( \frac{(1+\varepsilon)^k - (1+\varepsilon)}{\varepsilon} - (k-1) \right) \|x\|_\infty \tag{C.8}$$

*and*

$$\left| P_k - \prod_{i=1}^{k} x_k \right| \leq \left( (1+\varepsilon)^{k-1} - 1 \right) \|x\|_\infty^k . \tag{C.9}$$

**Corollary C.1.4.**

$$\left| S_k - \sum_{i=1}^{k} x_i \right| \leq \left( \frac{k^2}{2} \right) \varepsilon \|x\|_\infty \tag{C.10}$$

$$\left| P_k - \prod_{i=1}^{k} x_k \right| \leq k\varepsilon \|x\|_\infty^k \tag{C.11}$$

*Proof.* Apply Newton formula to $(1+\varepsilon)^k$ and $(1+\varepsilon)^{k-1}$ in (C.8) and (C.9) respectively. For (C.8) we get

$$S_k \leq \left( \binom{k}{2}\varepsilon + \sum_{i=3}^{k} \binom{k}{i}\varepsilon^{i-1} \right).$$

It is sufficient to choose $\varepsilon$ sufficiently small (for example $\varepsilon \leq \frac{1}{k^4}$) to bound the sum by $\varepsilon$, so that

$$S_k \leq \left( \binom{k}{2} + 1 \right) \varepsilon \left\| x \right\|_\infty \leq \frac{k^2}{2}\varepsilon \left\| x \right\|_\infty,$$

for all $k \geq 2$. The proof of (C.11) is similar but easier so it is left to the reader. □

**Proposition C.1.5.** *If we drop off the hypothesis that we are working with exact arithmetic and consider also the error given by machine operations, we get*

$$\max\left\{ |P - \hat{P}'|, |Q - \hat{Q}'|, |R - \hat{R}'| \right\} \leq 179 c_\alpha^4 \cdot \varepsilon. \tag{C.12}$$

*Proof.* When we look at the operations used to compute $P$, $Q$ and $R$, the most complicated one is $R$ which is computed in 14 simple operations on the $\alpha_i$, and it involves the product of only 4 of these $\alpha_i$. Using (C.10) and (C.11), we see that

$$|R' - R| \leq \left( \begin{pmatrix} 15 \\ 2 \end{pmatrix} + 1 \right) \frac{c_\alpha^4}{|a|^4}\varepsilon \leq 106 c_\alpha^4 \varepsilon$$

So putting together the two kinds of error we get

$$|R - \hat{R}'| \leq 73 \cdot c_\alpha^4 \cdot \varepsilon + 106 c_\alpha^4 \cdot \varepsilon = 179 \cdot c_\alpha^4 \cdot \varepsilon.$$

Analogous (smaller) bounds hold for $|P - \hat{P}'|$ and $|Q - \hat{Q}'|$. □

**Corollary C.1.6.** *If we suppose $K = \mathbb{Q}(i)$, $X \leq 10^5$ and $\varepsilon = 10^{-38}$, the error term that we obtain testing the borders is bounded by $10^{-28}$.*

### C.1.1 Error when computing $k$

Let $F = (a_0, b_0, c_0, d_0)$ be a Cremona-reduced binary cubic form, and let $H_F = (P, Q, R)$ be the associated binary hermitian form. Finally let $G = (a, b, c, d)$ be the corresponding Julia-reduced binary cubic form. When we compute $k = k_1 + ik_2 = \left\lfloor \frac{Q}{P} \right\rceil$ (we round separately imaginary part and real part) we only have a problem when $\left\lfloor \frac{Q_i}{P} \right\rceil = k_i + \frac{1}{2}$, for $i = 1$ or 2, where we set $Q_1 = \mathrm{Re}(Q), Q_2 = \mathrm{Im}(Q)$.

But to detect it with approximate values we need again to estimate the possible error $\delta$.

Let us suppose for example

$$Q_i/P = k_i + \omega$$

where $0 \leq \omega \leq 1$, and

$$\hat{Q}_i/\hat{P} = k_i + \omega + \delta.$$

**Proposition C.1.7.** *Let $K = \mathbb{Q}(i)$. The error $\delta$ for $k_i$ (with exact arithmetics) is bounded by*

$$|\delta| \leq 10^3 \cdot X^{3/4} \cdot \varepsilon. \tag{C.13}$$

*Proof.* We have

$$\left|(Q_i - (k_i + \omega)\, P) - \left(\hat{Q}_i - (k_i + \omega)\, \hat{P}\right)\right| = \delta \hat{P}.$$

So we obtain

$$\delta \leq \hat{P}\delta \leq |Q_i - \hat{Q}_i| + (k_i + \omega)|P - \hat{P}|.$$

(since $P > 1$, and it is sufficient to take the error on $P$ sufficiently small to get $\hat{P} < 1$ too).

Now we need to bound $k$ but since $b_0 = 3ak + b$, we get

$$|k| \leq \frac{|b| + |b_0|}{3}.$$

Now we know that $|b| \leq 3 \cdot c_\alpha$ and

$$|b_0| \leq \max\{\mathrm{Re}(3a), \mathrm{Im}(3a)\} \leq |3a| \leq 3\left(\frac{\alpha}{\sqrt{3}}\right)^{3/4} X^{1/4},$$

with $\alpha = 1/t_K$ so

$$k_i \leq |k| \leq \frac{|b_0| + |b|}{3} \leq c_\alpha + \left(\frac{\alpha}{\sqrt{3}}\right)^{3/4} X^{1/4}.$$

In particular, when $K = \mathbb{Q}(i)$, with rough approximations we get

$$k_i + \omega \leq 4X^{1/4}$$

then

$$\delta \leq 55 \cdot \varepsilon \cdot c_\alpha^3 + 37 \cdot \varepsilon \cdot c_\alpha^2 \cdot 4X^{1/4}$$

In particular for $K = \mathbb{Q}(i)$

$$\delta \leq 10^3 \cdot X^{3/4} \cdot \varepsilon.$$

□

**Corollary C.1.8.** *If we suppose $K = \mathbb{Q}(i)$, $X \leq 10^5$, $\varepsilon = 10^{-38}$ and exact arithmetic we get*

$$\delta \leq 10^{-30}.$$

**Proposition C.1.9.** *If we suppose machine operations, we have to add to the previous error $\delta$, an error $\delta' \leq (3\tau + 2\varepsilon)(4X^{1/4} + 1)$, where $\tau = 106 \cdot c_\alpha^4 \varepsilon$.*

*Proof.* Recall that

$$\max\left\{\left|\hat{P} - \hat{P}'\right|, \left|\hat{Q} - \hat{Q}'\right|\right\} \leq 106 \cdot c_\alpha^4 \varepsilon,$$

and that we suppose that the error given by a single machine operation is

$$\hat{P}' \oslash \hat{Q}'_i \leq \hat{P}'/\hat{Q}'_i \cdot (1 + \varepsilon).$$

Now $\hat{P}'/\hat{Q}' \leq \frac{\hat{P}(1+\tau)}{\hat{Q}(1-\tau)} \leq \frac{\hat{P}}{\hat{Q}}(1+3\tau)$ where $\tau = 106 \cdot c_\alpha^4 \varepsilon$.

So $\hat{P}' \oslash \hat{Q}' \leq \frac{\hat{P}}{\hat{Q}}(1+3\tau)(1+\varepsilon) \leq \frac{\hat{P}}{\hat{Q}}(1+2\varepsilon+3\tau)$, if we suppose $|\tau| \leq 1/3$ so

$$\left|\hat{P}' \oslash \hat{Q}' - \hat{P}/\hat{Q}\right| \leq (3\tau + 2\varepsilon)\left|\hat{P}/\hat{Q}\right| \tag{C.14}$$

$$\leq (3 \cdot 106 c_\alpha^4 \cdot \varepsilon + 2\varepsilon)(4X^{1/4}+1) \tag{C.15}$$

In particular when $K = \mathbb{Q}(i)$ we have $\delta' \leq (4295 \cdot \varepsilon \cdot X)(4X^{1/4}+1)$ □

**Corollary C.1.10.** *If we suppose $X \leq 10^5$, $\varepsilon = 10^{-38}$ and machine arithmetic we get*

$$\delta \leq 10^{-27}.$$

### C.1.2 Error when computing $|d-x_1||d-x_2|$

Let $F = (a,b,c,d)$. Set $A = -27a^2, B = 18abc - 4b^3, C = b^2c^2 - 4ac^3$. We consider the polynomial $Ax^2 + Bx + C$; $\Delta = B^2 - 4AC$ is an exact value, so

$$|\hat{\sqrt{\Delta}} - \sqrt{\Delta}| \leq \varepsilon|\sqrt{\Delta}|.$$

Recall that $x_1 = \frac{-B+\sqrt{\Delta}}{2A}$ and $x_2 = \frac{-B-\sqrt{\Delta}}{2A}$

**Proposition C.1.11.** *We have that*

$$||d-x_1||d-x_2| - |d-\hat{x}_1||d-\hat{x}_2|| \leq 4 \cdot X \cdot \tau + \tau^2,$$

*with $\tau = \gamma_K \cdot \varepsilon X^{3/4}$, and $\gamma_K$ is constant depending only on the number field $K$. In particular $\gamma_{\mathbb{Q}(i)} \leq 10^4$*

*Proof.* For $i = 1$ or 2, we have

$$|x_i - \hat{x}_i| = \left|\frac{\sqrt{\Delta}}{2A} - \frac{\hat{\sqrt{\Delta}}}{2A}\right| \leq |\sqrt{\Delta} - \hat{\sqrt{\Delta}}| \leq \tau,$$

where $\tau = \varepsilon|\sqrt{\Delta}|$. Hence,

$$||d-x_i| - |d-\hat{x}_i|| \leq |x_i - \hat{x}_i| \leq \tau.$$

Now

$$\begin{aligned}
||d-x_1||d-x_2| - |d-\hat{x}_1||d-\hat{x}_2|| &\leq |d-x_2|\,||d-x_1| - |d-\hat{x}_1|| + |d-\hat{x}_1|\,||d-x_2| - |d-\hat{x}_2|| \\
&\leq |d-x_2|\tau + |d-\hat{x}_1|\tau \\
&\leq \frac{2X}{|A|} \cdot \tau + |d-\hat{x}_1|\tau \\
&\leq \frac{4X}{|A|}\tau + \tau^2,
\end{aligned}$$

since $|d-\hat{x}_i| \leq |d-x_i| + |\hat{x}_i - x_i| \leq \frac{2X}{|A|} + \tau$. Now we need to bound $\Delta$, but looking at the polynomial expression for $A$, $B$ and $C$, and applying the bounds given in Theorem 2.2.3 we get

$$\Delta \leq \gamma_K^2 \cdot X^{3/2},$$

for a constant $\gamma_K$ depending only on the number field $K$; so

$$\sqrt{\Delta} \leq \gamma_K \cdot X^{3/4},$$

then we can replace $\tau$ by the upper bound $\gamma_K \cdot \varepsilon \cdot X^{3/4}$. In particular, when $K = \mathbb{Q}(i)$ it is easy to see that $\gamma_K \leq 10^4$ □

**Corollary C.1.12.** *If we suppose $K = \mathbb{Q}(i)$, $X \leq 10^5$, $\varepsilon = 10^{-38}$ and exact arithmetic we get*

$$||d - x_1||d - x_2| - |d - \hat{x}_1||d - \hat{x}_2|| \leq 10^{-24}.$$

**Proposition C.1.13.** *Let $\lambda = 2Ad + B$. The additional error $\delta$ given by machine operations is*

$$\delta \leq 3 \cdot \varepsilon \cdot \left(|\lambda| + \hat{\sqrt{\Delta}}\right)^2$$

*where $\varepsilon$ is the machine error for one simple operation.*

*Proof.* Since $A, B$ and $C$ are exact numbers, we just need to take into account the operations involving $\sqrt{\Delta}$. let us write

$$\begin{aligned} |d - x_1|\,|d - x_2| &= \frac{|2Ad - 2Ax_1|\,|2Ad - 2Ax_2|}{4A^2} \\ &= \frac{\left|\lambda - \sqrt{\Delta}\right|\left|\lambda + \sqrt{\Delta}\right|}{4A^2} \end{aligned}$$

Now

$$\left|\left(\lambda \ominus \hat{\sqrt{\Delta}}\right) - \left(\lambda - \hat{\sqrt{\Delta}}\right)\right| \leq \varepsilon \left(|\lambda| + \hat{\sqrt{\Delta}}\right)$$

And

$$\left|\left(\lambda \oplus \hat{\sqrt{\Delta}}\right) - \left(\lambda + \hat{\sqrt{\Delta}}\right)\right| \leq \varepsilon \left(|\lambda| + \hat{\sqrt{\Delta}}\right)$$

So

$$(\lambda \ominus \hat{\sqrt{\Delta}}) \times (\lambda \oplus \hat{\sqrt{\Delta}}) \leq (1+\varepsilon)^2(|\lambda| + \hat{\sqrt{\Delta}})^2$$

$$\begin{aligned} &\left|(\lambda \ominus \hat{\sqrt{\Delta}}) \otimes (\lambda \oplus \hat{\sqrt{\Delta}}) - (\lambda - \hat{\sqrt{\Delta}}) \times (\lambda + \hat{\sqrt{\Delta}})\right| \\ &\leq \varepsilon(1+\varepsilon)^2(|\lambda| + \hat{\sqrt{\Delta}})^2 + 2\varepsilon(|\lambda| + \hat{\sqrt{\Delta}}) + \varepsilon^2(|\lambda| + \hat{\sqrt{\Delta}}) =: err \end{aligned}$$

Finally the machine error obtained after the division by $4A^2$ is

$$\begin{aligned} &||d \ominus \hat{x}_1'| \otimes |d \ominus \hat{x}_2'| - |d - \hat{x}_1|\,|d - \hat{x}_2||| \\ &\leq \frac{(1+\epsilon)err + (|\lambda| + \hat{\sqrt{\Delta}})^2\epsilon}{4 \cdot 27} \\ &\leq 2\varepsilon(|\lambda| + \hat{\sqrt{\Delta}})^2 + \varepsilon^2 \cdot f(\lambda, \Delta, \varepsilon), \end{aligned}$$

and it is easy to see that for sufficiently small $\varepsilon$, we can bound

$$\varepsilon^2 \cdot f(\lambda, \Delta, \varepsilon) \leq \varepsilon \left(\left|\lambda + \hat{\sqrt{\Delta}}\right|\right)^2,$$

so we conclude. □

**Corollary C.1.14.** *If we suppose $K = \mathbb{Q}(i)$, $X \leq 10^5$, $\varepsilon = 10^{-38}$ and machine operations, we get*

$$\delta \leq 10^{-22}.$$

*Proof.* Recall that

$$\hat{\sqrt{\Delta}} \leq \gamma_K \cdot (1 + \varepsilon) \cdot X^{3/4}.$$

In the same way we can prove

$$|\lambda| \leq \delta_K X^{3/4},$$

for a constant $\delta_K$ depending only on $K$. In particular if $K = \mathbb{Q}(i)$ we obtain

$$\hat{\sqrt{\Delta}} \leq 10^4 X^{3/4}$$

and

$$|\lambda| \leq 3000 X^{3/4}.$$

So

$$|\lambda| + \hat{\sqrt{\Delta}} \leq 13000 X^{3/4},$$

and we conclude. □

# Appendix D

This appendix gives the polynomials used in §2.5.1 to check rigorously the boundary conditions in the reduction inequalities.

Section D.1 gives the Maple code used to compute the polynomial `gP` associated to the binary cubic form

$$F = ax^3 + bx^2y + cxy^2 + dy^3 = a(x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y).$$

It belongs to $K[X]$ and vanishes at

$$|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 .$$

Similarly `gR` vanishes at

$$(|\alpha_1|^2|\alpha_2|^2 + |\alpha_1|^2|\alpha_3|^2 + |\alpha_2|^2|\alpha_3|^2),$$

`gQ` vanishes at

$$z = \overline{\alpha_1}\alpha_2\alpha_3 + \alpha_1\overline{\alpha_2}\alpha_3 + \alpha_1\alpha_2\overline{\alpha_3}.$$

Finally, `gReQ`, `gImQ` vanish at $2\mathrm{Re}(z)$ and $2\mathrm{Im}(z)$ respectively.

The resulting expressions are polynomials in $\mathbb{Z}[e_1, e_2, e_3, f_1, f_2, f_3, X]$, where the $e_i$ stand for the elementary symmetric functions:

$$\begin{aligned} e_1 &= \alpha_1 + \alpha_2 + \alpha_3 = -b/a, \\ e_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = c/a, \\ e_3 &= \alpha_1\alpha_2\alpha_3 = -d/a. \end{aligned}$$

The $f_i$ stand for their conjugates.

These polynomials are used by the GP functions in §D.2, with numeric arguments for $a, b, c, d \in \mathcal{O}_K$, yielding univariate polynomials in $K[X]$.

## D.1 Maple code

```
#############################################################################
# ai corresponds to \alpha_i, bi to \overline{\alpha_i}
Sa := a1+a2+a3=e1, a1*a2+a1*a3+a2*a3=e2, a1*a2*a3=e3:
Sb := b1+b2+b3=f1, b1*b2+b1*b3+b2*b3=f2, b1*b2*b3=f3:

# sigma = [123, 132, 213, 231, 312, 321]
sigma[1]:= e -> e:
sigma[2]:= e -> subs({       b2=b3, b3=b2}, e):
sigma[3]:= e -> subs({b1=b2, b2=b1       }, e):
sigma[4]:= e -> subs({b1=b2, b2=b3, b3=b1}, e):
sigma[5]:= e -> subs({b1=b3, b2=b1, b3=b2}, e):
sigma[6]:= e -> subs({b1=b3,        b3=b1}, e):

# expand \prod (X-\sigma_i(s))
# then substitute the elementary symmetric functions
POL := proc (s) local P, Q;
  P := mul(X-sigma[i](s), i=1..6);
  Q := simplify(P, {Sa,Sb}, [a1,a2,a3,b1,b2,b3]);
  sort(collect(Q,X), X);
end:
#############################################################################

gP := POL(a1*b1 + a2*b2 + a3*b3);
gR := POL(a1*a2*b1*b2 + a1*a3*b1*b3 + a2*a3*b2*b3);
gQ := POL(b1*a2*a3 + a1*b2*a3 + a1*a2*b3);
gReQ := POL(b1*a2*a3 + a1*b2*b3 + a1*b2*a3 + b1*a2*b3 + a1*a2*b3 + b1*b2*a3);
gImQ := POL(-a1*b2*b3 + b1*a2*a3 - b1*a2*b3 + a1*b2*a3 - b1*b2*a3 + a1*a2*b3);
```

## D.2 GP code

```
gP(a,b,c,d)=
{ my(e1 = -b/a, e2 = c/a, e3 = -d/a);
  my(f1 = conj(e1), f2 = conj(e2), f3 = conj(e3));

X^6
-2*f1*e1*X^5
+(f1^2*e1^2+2*f2*e1^2+2*f1^2*e2-6*f2*e2)*X^4+
(-2*f1^3*e3-27*f3*e3+9*f3*e2*e1-2*f3*e1^3-2*f1*f2*e1^3+9*f2*f1*e3+ 5*f1*f2*e2*e1-2*f1^3*e1*e2)*X^3+
(-6*f2^2*e2*e1^2-9*f3*f1*e2*e1^2+f1^4*e2^2-6*f1^2*f2*e2^2+2*f1^4*e3*e1+
  27*f3*f1*e3*e1+f2^2*e1^4+2*f3*f1*e1^4+9*f2^2*e2^2+3*f1^2*f2*e1^2*e2
  -9*f1^2*f2*e3*e1)*X^2+
(15*f1^3*f2*e3*e2-f2^2*f1*e1^3*e2-2*f1^5*e2*e3+81*f3*f2*e3*e2+3*f2^2*f1*e2^2*e1
  -f1^3*f2*e2^2*e1-27*f3*f2*e2^2*e1+9*f3*f1^2*e2^2*e1-27*f2^2*f1*e3*e2-27*f3*f1^2*e3*e2
  -2*f3*f2*e1^5-2*f3*f1^2*e1^3*e2+9*f2^2*f1*e3*e1^2-27*f3*f2*e3*e1^2+15*f3*f2*e2*e1^3
  -2*f1^3*f2*e3*e1^2)*X+
f1^6*e3^2+f2^2*f1^2*e1^3*e3+f3*f2*f1*e1^4*e2-27*f2^3*e3^2-27*f3^2*e2^3+f1^4*f2*e1*e2*e3
  +27*f2^2*f1^2*e3^2-4*f2^3*e2^3-9*f2*f1*f3*e2^2*e1^2+27*f3^2*e2^2*e1^2-4*f2^3*e3*e1^3
  +9*f3*f2*f1*e3*e1^3-2*f3*f1^3*e3*e1^3+f3^2*e1^6+f1^3*f3*e2^2*e1^2+18*f2*f1*f3*e2^3
  -9*f3^2*e2*e1^4+18*f2^3*e3*e2*e1-9*f1^4*f2*e3^2-27*f3*f2*f1*e3*e2*e1+9*f3*f1^3*e3*e2*e1
  -9*f2^2*f1^2*e3*e2*e1+f2^2*f1^2*e2^3+f2^3*e2^2*e1^2-4*f1^3*f3*e2^3;
};

gR(a,b,c,d)=
{ my(e1 = -b/a, e2 = c/a, e3 = -d/a);
  my(f1 = conj(e1), f2 = conj(e2), f3 = conj(e3));
```

```
X^6-2*f2*e2*X^5+(2*f3*f1*e2^2-6*f3*f1*e3*e1+2*f2^2*e3*e1+f2^2*e2^2)*X^4+
(9*f3*f2*f1*e3^2-2*f3^2*e2^3-2*f2^3*e3^2-27*f3^2*e3^2+9*f3^2*e3*e2*e1+5*f3*f2*f1*e3*e2*e1
-2*f2*f1*f3*e2^3-2*f2^3*e3*e2*e1)*X^3+(27*f3^2*f2*e3^2*e2-9*f3^2*f2*e3*e2^2*e1
+9*e3^2*f3^2*f1^2*e1^2+f3^2*f1^2*e2^4-6*f3^2*f1^2*e3*e2^2*e1+2*f3^2*f2*e2^4+2*e3^2*f2^4*e2
-6*f2^2*f1*f3*e3^2*e1^2-9*e3^2*f3*f2^2*f1*e2+f2^4*e1^2*e3^2+3*f3*f2^2*f1*e2^2*e1*e3)*X^2+
(9*f3^2*f2^2*e2*e3^2*e1^2-2*f2^5*e3^3*e1-f3^2*f2*f1^2*e2^3*e1*e3-2*f3^3*f1*e2^5
+3*f3^2*f1^2*f2*e2*e3^2*e1^2+9*e3^2*f3^2*f2*f1^2*e2^2-f2^3*f1*f3*e3^2*e2*e1^2
-27*f3^3*f1*e3^2*e2*e1^2+15*f3^3*f1*e3*e2^3*e1-2*f3^2*f2^2*e2^3*e1*e3
-27*f3^2*f1^2*f2*e3^3*e1+81*f3^3*f1*e3^3*e1+15*f3*f1*f2^3*e3^3*e1-27*f3^3*f1*e3^2*e2^2
-27*f3^2*f2^2*e3^3*e1-2*e3^2*f3*f2^3*f1*e2^2)*X+f2^6*e3^4-27*f3^3*f1^3*e3^4
+f3^3*e1^2*f1^3*e3^2*e2^2+f3^3*f2*f1*e2^4*e1*e3-4*e3^2*f3^3*f1^3*e2^3
+27*f3^2*f2^2*f1^2*e3^4-4*f3^3*f1^3*e3^3*e1^3-27*f3^4*e3^3*e1^3
+18*f3^3*f1*f2*e3^3*e1^3+f3^4*e2^6+9*f3^2*f2^3*e3^3*e2*e1
+18*f3^3*f1^3*e3^3*e2*e1-9*f3^4*e3*e2^4*e1+f3^2*f2^2*f1^2*e3^3*e1^3
-9*f3^2*f2^2*f1^2*e3^3*e2*e1+f3^2*e3^2*f2^3*e2^2*e1^2
-2*e3^2*f3^2*f2^3*e2^3-9*f3*f2^4*f1*e3^4-4*f3^2*f2^3*e3^3*e1^3
+e3^2*f3^2*f2^2*f1^2*e2^3+9*e3^2*f3^3*f2*f1*e2^3+f3*f2^4*f1*e3^3*e2*e1
-9*f3^3*e3^2*f1*f2*e2^2*e1^2-27*f3^3*f1*f2*e3^3*e2*e1+27*f3^4*e3^2*e2^2*e1^2;
};

gQ(a,b,c,d)=
{ my(e1 = -b/a, e2 = c/a, e3 = -d/a);
  my(f1 = conj(e1), f2 = conj(e2), f3 = conj(e3));

X^6-2*f1*e2*X^5+(f1^2*e2^2+2*f1^2*e3*e1+2*f2*e2^2-6*f2*e3*e1)*X^4
+(9*f2*f1*e3^2-2*f1^3*e3^2-2*f1*f2*e2^3+9*f3*e3*e2*e1-27*f3*e3^2-2*f3*e2^3
+5*f2*f1*e3*e2*e1-2*f1^3*e1*e2*e3)*X^3+(-6*f1^2*f2*e3^2*e1^2+2*f3*f1*e2^4
+9*e3^2*f2^2*e1^2+3*f1^2*f2*e2^2*e1*e3+f2^2*e2^4+27*f3*f1*e3^2*e2+f1^4*e3^2*e1^2
-6*f2^2*e3*e2^2*e1+2*e3^2*f1^4*e2-9*f3*f1*e3*e2^2*e1-9*e3^2*f2*f1^2*e2)*X^2
+(9*f3*f1^2*e3^2*e2*e1^2-2*e3^2*f1^3*f2*e2^2+15*f1^3*f2*e3^3*e1+15*f3*f2*e3*e2^3*e1
-f1*f2^2*e2^3*e1*e3-27*f2^2*f1*e3^3*e1-27*f3*f1^2*e3^3*e1-27*f3*f2*e3^2*e2*e1^2
-2*f3*f1^2*e2^3*e1*e3-f1^3*f2*e3^2*e2*e1^2-2*f1^5*e3^3*e1+9*e3^2*f2^2*f1*e2^2
-27*f3*f2*e3^2*e2^2+81*f3*f2*e3^3*e1+3*f2^2*f1*e3^2*e2*e1^2-2*f2*f3*e2^5)*X
-2*e3^2*f1^3*f3*e2^3+9*f1^3*f3*e3^3*e2*e1-9*e3^2*f3*f2*f1*e2^2*e1^2+f1^4*f2*e3^3*e2*e1
-27*f3*f2*f1*e3^3*e2*e1-9*f2^2*f1^2*e3^3*e2*e1+e3^2*f2^3*e2^2*e1^2+18*f3*f2*f1*e3^3*e1^3
+f2^2*f1^2*e3^3*e1^3+f1^6*e3^4-4*f2^3*e3^3*e1^3+27*f2^2*f1^2*e3^4-9*f1^4*f2*e3^4
+e3^2*f1^3*f3*e2^2*e1^2+18*f2^3*e3^3*e2*e1+f2*f1*f3*e2^4*e1*e3+27*f3^2*e3^2*e2^2*e1^2
-9*f3^2*e3*e2^4*e1+9*e3^2*f3*f2*f1*e2^3+f3^2*e2^6+e3^2*f2^2*f1^2*e2^3
-4*f1^3*f3*e3^3*e1^3-27*f3^2*e3^3*e1^3-4*e3^2*f2^3*e2^3-27*f2^3*e3^4;
};


gImQ(a,b,c,d)=
{ my(e1 = -b/a, e2 = c/a, e3 = -d/a);
  my(f1 = conj(e1), f2 = conj(e2), f3 = conj(e3));

X^6
+ (-2*f1*e2+2*f2*e1)*X^5
+ (-3*e3*f1*f2+2*e2^2*f2+2*f2^2*e2-3*e1*e2*f3+e2^2*f1^2+27*e3*f3-6*e3*f2*e1 -
  6*f3*f1*e2+2*e1^2*f3*f1-3*e1*e2*f1*f2+2*e3*f1^2*e1+e1^2*f2^2)*X^4+(-2*e3^2*f1^3 -
  27*e3^2*f3-2*e2^3*f3-4*e3*e1^2*f2^2+4*e2^2*f1^2*f3-2*e2^2*f1*f2^2+6*e2^2*f2*f3 +
  2*e1*e2^2*f2^2-6*e3*f2^2*e2-2*e2^3*f1*f2+9*e3^2*f1*f2+9*e2*e3*f3*e1+2*e3*e1^2*f2*f1^2 +
  6*e3*f1^2*f3*e1-5*e3*f1*f2^2*e1-6*e3*e1^2*f1*f3+27*e3*f2*f3*e1-e1^2*f1*f2^2*e2 -
  2*e1^2*f1^2*f3*e2-5*e1^2*f2*f3*e2+5*e3*f2*f1^2*e2-27*e3*f1*f3*e2+5*e1*e2^2*f1*f3 +
  e1*e2^2*f2*f1^2-2*e1*e2*f1^3*e3+5*e2*e3*f1*f2*e1+2*e1^3*f3^2+2*e1^3*f2*f1*f3 -
  5*e2*e1*f2*f1*f3+2*e3*f2^3+27*e3*f3^2+2*e2*e1*f2^3-9*e2*e1*f3^2-9*e3*f2*f1*f3)*X^3
+ (e2^4*f2^2-2*e1^3*e3*f2^3+9*e3^2*f1^2*f2^2+6*e1*e2*e3*f2^3+e1^3*e3*f1^2*f2^2 -
  72*e1*e2*e3*f1*f2*f3+3*e1*e2*e3*f1^2*f2^2+6*e1*e2*e3*f1^3*f3+6*e1^3*e3*f1*f2*f3 -
  2*e1^3*e3*f1^3*f3+9*e1^2*e2^2*f3^2-2*e2^3*f1^3*f3+e2^3*f1^2*f2^2+e1^2*e2^2*f2^3 -
  27*e3^2*f2^3-27*e2^3*f3^2-2*e2^3*f2^3+e1^2*e2^2*f1^3*f3+6*e2^3*f1*f2*f3 +
  3*e1^2*e2^2*f1*f2*f3+9*e3^2*e1^2*f2^2+2*e2^4*f3*f1+e3^2*e1^2*f1^4+2*e2*e3^2*f1^4 -
  6*e2^2*e3*f2^2*e1+27*e3^2*f3*f1^2*e1+18*e3^2*f2^2*f1*e1-108*e3^2*f2*f3*e1-e2^3*e1*f2^2*f1 -
  2*e2^3*e1*f3*f1^2-5*e2^3*e1*f2*f3+27*e2^2*e3*f2*f3+3*e2^2*e3*f2^2*f1+27*e3^2*f3*f1*e2 -
  9*e2*e3^2*f2*f1^2-5*e3^2*e1*f2*f1^3-6*e3^2*e1^2*f2*f1^2-2*e2^2*f2*f1^3*e3-9*e2^2*e3*f3*f1*
  e1+18*e2*e3*e1^2*f2*f3+3*e2*e3*e1^2*f3*f1^2-e2*e1^2*f2*f1^3*e3+3*e2^2*e1*f2*f1^2*e3 -
  27*e3*e1^3*f3^2+2*e1*e3*f2^4-27*e3^2*f1^3*f3+81*e3^2*f2*f1*f3+3*e3*e1^2*f2*f1^2*f3 +
  27*e1*e3*f2*f3^2+81*e1*e2*e3*f3^2-2*e3*e1^2*f1*f2^3+27*e1^2*e3*f1*f3^2+27*e3*e2*f3*f2^2 -
  5*e3*e2*f1*f2^3-9*e1*e3*f2^2*f1*f3+18*e3*e2*f2*f1^2*f3-108*e2*e3*f1*f3^2+9*e2^2*f1^2*f3^2 +
  18*e1*e2^2*f1*f3^2-9*e2*e1^2*f2*f3^2-6*e2*e1^2*f1^2*f3^2-5*e2*e1^3*f1*f3^2+2*e1^4*f2*f3^2 +
  e1^4*f1^2*f3^2+3*e2^2*e1*f3*f2^2-e2^2*e1*f1*f2^3-2*e2*e1^3*f3*f2^2-6*e2^2*f2^2*f1*f3 +
  e2^2*f2^4+3*e2*e1^2*f2^2*f1*f3-e2*e1^3*f2*f1^2*f3)*X^2
+ (- 33*e2*e3^2*e1*f1^3*f3-6*e2*e1*e3^2*f1^2*f2^2+3*e2*e3*e1^3*f3*f2^2+18*e2*e3*e1^3*f1*f3^2 -
  2*e2^5*f2*f3-6*e3^2*e1*f2^4-2*e1*e3^3*f1^5+2*e1^5*f1*f3^3+81*e3^3*f2*f3*e1 -
  27*e2^2*e3^2*f2*f3+9*e3^2*e2^2*f2^2*f1-2*e3^2*e2^2*f2*f1^3-27*e1*e3^3*f1^2*f3 -
```

```
  27*e1*e3^3*f2^2*f1+15*e1*e3^3*f2*f1^3+15*e3*e2^3*f2*f3*e1-27*e2*e1^2*e3^2*f2*f3 -
  e1*e2^3*f2^2*f1*e3+9*e2*e3^2*e1^2*f1^2*f3+3*e2*e3^2*e1^2*f2^2*f1-e2*e3^2*e1^2*f2*f1^3 -
  2*e1*e2^3*f1^2*f3*e3+e2^2*e1^2*f2^2*f1^2*e3+54*e3^3*f2^3-54*e2^3*f3^3-33*e3*e2^3*f2*f1*f3 -
  2*e3*e1*e2^2*f1^4*f3-e3*e2^2*e1*f1^3*f2^2-3*e2*e1^4*f3^3+2*e2*e3*f2^5-3*e3*e2^2*f2*f1^3*f3 +
  6*e2^2*e1^2*f2*f1*f3^2-3*e2^2*e1*f2*f1^2*f3^2+27*e2*e3*f3^2*f2^2+2*e2*e3*e1^2*f2^4 +
  27*e3*e2^3*f3^2+2*e3*e2^3*f2^3-5*e2*e3^2*f1^3*f2^2+6*e2*e3^2*f1^4*f3-81*e2*e3*f1*f3^3 -
  18*e2*e3^2*e1*f2^3-81*e2*e3^2*e1*f3^2-4*e3*e2^2*f2^4+81*e2*e3^2*f1*f3^2-108*e2*e3^2*f3*f2^2
 +18*e2*e3^2*f1*f2^3+3*e2^4*e1*f3^2+81*e2*e3*e1*f3^3+27*e2^2*e1^2*f3^3-15*e2*e1^3*f1*f3^3 +
  2*e2*e1^3*f3^2*f2^2-15*e2*e3*f3*f1*f2^3+27*e2*e3*f2*f1^2*f3^2+8*e3*e2^3*f1^3*f3 -
  27*e3*e2^2*e1^2*f3^2-27*e3*e2^2*f1^2*f3^2+2*e3*e2^2*f1^2*f2^3+108*e3*e2^2*f2*f3^2 -
  9*e1*e2^2*f3^2*f2^2+18*e2*e1*e3*f1^3*f3^2+27*e1*e2^2*f1*f3^3-3*e2*e1*e3*f1*f2^4 +
  33*e2*e1*e3*f3*f2^3-5*e1^2*e2^3*f1*f3^2+3*e2*e3^2*e1*f2*f1^4-18*e2^3*e1*f2*f3^2 -
  3*e2^3*e1*f1^2*f3^2+5*e2^2*e1^3*f2*f3^2-3*e2*e1^4*f2*f1*f3^2+e2*e1^3*f2*f1^2*f3^2 +
  2*e1^3*e3^2*f1^3*f3+3*e3^3*f1^4*f2+2*e1^3*e3^2*f2^3-27*e3^3*f1^2*f2^2-81*e3^3*f2*f1*f3 +
  27*e3^3*f1^3*f3-27*e3^2*f3*f2^3-54*e3^2*f1^3*f3^2-3*e3^2*f1*f2^4+54*e3^2*e1^3*f3^2 +
  27*e3*e1^2*f1*f3^3-81*e1*e3^2*f2*f3^2+108*e1*e3^2*f1^2*f3^2-27*e3*e1^3*f3^3-108*e1^2*
  e3^2*f1*f3^2+4*e1^2*e3^2*f1^4*f3-9*e3*e1^2*f2*f1^2*f3^2-2*e3^2*e1^2*f1^3*f2^2 +
  27*e3^2*e1^2*f3*f2^2+3*e3^2*e1^2*f1*f2^3+81*e3^2*f2*f1*f3^2+27*e3^2*f3*f1^2*f2^2 +
  33*e3*e1^3*f2*f1*f3^2-18*e1*e3^2*f2*f1^3*f3-4*e3*e1^4*f1^2*f3^2-6*e3*e1^4*f2^3 -
  2*e3*e1^3*f1^3*f3^2-8*e3*e1^3*f3*f2^3+2*e3*e1^4*f2^2*f1*f3+2*e3*e1^2*f3*f1*f2^3 -
  18*e3^2*e1^3*f2*f1*f3+5*e1*e3^2*f1^2*f2^3-6*e3*e2^2*e1^2*f2*f1*f3+15*e3*e2^2*e1*f2*f1^2*f3 -
  15*e2*e3*e1^2*f2^2*f1*f3+135*e2*e3^2*e1*f2*f1*f3+2*e2^2*e1^3*f1^2*f3^2-e2^2*e1^2*f3*f1^2*f2^2
 +e2^2*e1*f3*f1*f2^3+e2^2*e1^3*f2^2*f1*f3+e1*e2^3*f2*f1^3*f3+3*e2^4*e1*f2*f1*f3 -
  2*e2^3*f1^3*f3^2+6*e2*e1*e3*f3*f1^2*f2^2-e2*e3*e1^3*f1*f2^3-135*e2*e1*e3*f2*f1*f3^2 -
  2*e2^4*f2*f1^2*f3-2*e2^3*e1^2*f3*f2^2+e2*e3*e1^2*f1^2*f2^3+18*e2^3*f2*f1*f3^2+6*e2^4*f1*f3^2
 +4*e2^4*f3*f2^2-2*e2^3*f3*f2^3-e2^3*e1^2*f2*f1^2*f3)*X
+ 27*e3*e2^3*f2*f3^2*e1+10*e2^2*e1^2*e3*f1^3*f3^2-27*e2*e3^2*f1^3*f3^2*e1 -
  15*e2*e3*e1^3*f3^2*f2^2+27*e2*e3*e1^3*f1*f3^3-27*e2*e3*e1^2*f1^2*f3^3-27*e2*e3*f2*f1*f3^3*e1 +
  15*e3*e1^2*e2^3*f1*f3^2+27*e2^2*e3*f3^2*f2^2*e1-27*e2^2*e3^2*f1*f3^2*e1-9*e2^2*e3*e1^3*f2*f3^2
 -15*e3*e2^3*f1^2*f3^2*e1-6*e2^2*e3*e1^3*f1^2*f3^2+18*e2*e3*f1^3*f3^3*e1 -
  27*e2*e1^3*e3^2*f1*f3^2-7*e2*e3*e1^3*f2*f1^2*f3^2+54*e2*e3^2*f2*f1*f3^2*e1 +
  5*e2*e3*e1^4*f2*f1*f3^2-81*e3^3*f1^2*f3^2*e1+81*e3^2*f1^2*f3^3*e1-9*e2*e3*f3^2*f1^2*f2^2*e1 -
  27*e2*e3*e1^2*f2*f3^3+3*e2*e3*e1^2*f2*f1^3*f3^2+27*e2*e1^2*e3^2*f2*f3^2+27*e2*e1^2*
  e3^2*f1^2*f3^2+9*e2*e3*f3^2*f2^3*e1+9*e3^2*e1^4*f1^2*f3^2+81*e1^2*e3^3*f1*f3^2 -
  12*e3^2*e1^3*f1^3*f3^2-2*e3*e1^3*f3^2*f2^3-81*e2^2*e3^2*f2*f3^2-27*e2^2*e3*f1^2*f3^3 +
  81*e2^2*e3*f2*f3^3+27*e2^2*e3^2*f1^2*f3^2+18*e2*e3*e1^2*f1*f3^2*f2^2+9*e3*e1^3*f2*f1*f3^3 -
  2*e3*e1^4*f1*f3^2*f2^2-27*e3^2*f1*f3^2*f2^2*e1-27*e3^2*f2*f1^3*f3^2*e1-27*e1^3*e3^2*f2*f1*f3^2
 -6*e2^2*e3*f1^4*f3^2*e1+e1^4*f2*f1*f3^3*e2-e2^3*e1*f2*f1^3*f3^2+3*e2^3*e1^2*f2*f1^2*f3^2 +
  3*e2^3*e1*f1*f3^2*f2^2+5*e1*e2^4*f2*f1*f3^2-2*e2^3*e1^3*f2*f1*f3^2-e2^2*e1^3*f1*f3^2*f2^2 +
  e2^2*e1^2*f3^2*f2^3+e2^2*e1^2*f1^3*f3^3-2*e2^2*e1^3*f1^2*f3^3+15*e2^2*e1^3*f2*f3^3 +
  2*e2^2*e1^4*f1*f3^3+e2^2*e1^4*f3^2*f2^2+8*e3*e2^3*f1^3*f3^2+18*e2^3*f2*f1*f3^3 +
  9*e2^3*e1*f1^2*f3^3-9*e2^3*e1^2*f1*f3^3-6*e2^3*e1^2*f3^2*f2^2-27*e2^3*e1*f2*f3^3 -
  4*e3*e1^3*f1^3*f3^3+2*e3*e1^5*f3^2*f2^2+6*e3*e1^4*f1^2*f3^3-6*e3*e1^5*f1*f3^3 -
  81*e3^2*e1^2*f1*f3^3+9*e3^2*e1^2*f1^4*f3^2-27*e2^2*e3*f1*f3^2*f2^2+9*e2^2*e3*f2*f1^3*f3^2 +
  27*e2^2*e3*e1*f1*f3^3+27*e3^2*f2*f1^2*f3^2*e2-6*e2^5*f2*f3^2+2*e2^5*f1^2*f3^2 -
  4*e2^3*f1^3*f3^3-4*e2^3*f3^2*f2^3+e2^4*f1^4*f3^2+9*e1*e2^4*f3^3+9*e2^4*f3^2*f2^2 +
  2*e3^2*e1^2*f2^5+e3^2*e1^4*f2^4-6*e2*e3^2*f2^5-4*e3^2*e2^3*f2^3+9*e3^2*e2^2*f2^4 -
  9*e3^4*f1^4*f2-4*e1^3*e3^3*f2^3+27*e3^4*f1^2*f2^2-2*e3^3*f1^3*f2^3+27* e3^3*f3^2*f3^3 +
  27*e3^3*f1^3*f3^2+9*e3^3*f1*f2^4-27*e3^2*f1^3*f3^3+e2^3*f3^2*f1^2*f2^2-81*e3^2*f3^2*f2^2*e2
 +e3^2*e1^2*f1^2*f2^4-2*e3^2*e1^3*f1*f2^4-2*e3^2*e1*f1*f2^5-9*e2^2*e1^2*f2*f1*f3^3 -
  27*e3*e2^3*f2*f1*f3^2+9*e2*e3^3*e1*f1^3*f3-9*e2*e1*e3^3*f1^2*f2^2+9*e2*e3^2*e1^3*f3*f2^2 -
  6*e2^4*f2*f1^2*f3^2-2*e1*e2^5*f1*f3^2+e2^4*e1^2*f1^2*f3^2+2*e2^4*e1^2*f2*f3^2 -
  2*e1*e2^4*f1^3*f3^2-2*e1^5*f2*f3^3*e2+e3^2*f2^6-27*e3^4*f2^3+e3^4*f1^6+e2^6*f3^2 -
  27*e2^3*f3^4+e1^6*f3^4-27*e3^3*e1^3*f3^2+27*e3^2*e1^3*f3^3-9*e2*e1^4*f3^4 +
  27*e2^2*e1^2*f3^4+27*e3*e2^3*f3^3-2*e2^3*e1^3*f3^3-9*e3*e2^4*f3^2*e1-54*e2^2*e3*e1^2*f3^3 +
  27*e2^2*e3^2*e1^2*f3^2+9*e2*e3*e1^4*f3^3+2*e2*e3^2*f1^2*f2^4-6*e2*e3^2*e1^2*f2^4 +
  15*e2*e3^3*f1^3*f2^2+18*e2*e3^3*e1^2*f3*f2^2+9*e3^3*f3*f2^2-27*e2*e3^3*f1*f2^3 +
  2*e3^2*e2^2*f1^5*f3-2*e3^2*e2^3*f1^3*f3+e3^2*e2^2*e1^2*f2^3-6*e3^2*e2^2*f1^2*f2^3 -
  2*e2*e3^3*f2*f1^5+e3^2*e2^2*f1^4*f2^2+e2^3*e3^2*f1^2*f2^2-4*e1^3*e3^3*f1^3*f3 +
  e1^3*e3^3*f1^2*f2^2+27*e3^2*e1^2*f3^2*f2^2+27*e3^2*f3^2*f1^2*f2^2+6*e1^2*e3^3*f1^4*f3 -
  2*e3^3*e1^2*f1^3*f2^2-27*e3^3*e1^2*f3*f2^2+9*e3^3*e1^2*f1*f2^3+e1^3*f3^2*f1^2*f2^2*e3 +
  e3^2*e2^2*e1^2*f1^3*f3+3*e3^2*e2^2*e1*f1*f2^3+9*e3^2*e2^3*f2*f1*f3-2*e3^2*e1*e2^2*f1^4*f3 -
  e3^2*e2^2*e1*f1^3*f2^2-27*e3^2*e2^2*e1*f3*f2^2-15*e3^2*e2*e2^2*f2*f1^3*f3+27*e3^2*e2^2*f2^2*f1*f3
 -9*e2*e3^2*f3*f1^3*f2^2+27*e2*e3^2*f3*f1*f2^3-27* e2*e3^3*f2*f1^2*f3-2*e2*e1*e3^2*f1^3*f2^3 +
  5*e2*e1*e3^2*f1*f2^4-27*e2*e1*e3^2*f3*f2^3+e2*e3^3*e1*f2*f1^4-27*e3^3*e1^2*f2*f1^2*f3 +
  27*e3^2*e1^2*f2*f1^2*f3^2+27*e1*e3^3*f2^2*f1*f3-54*e3^3*f3*f1^2*f2^2+9*e3^3*f3*f2*f1^4 +
  8*e3^2*e1^3*f3*f2^3-9*e3^2*f3*f1*f2^4+2*e1*e3^3*f1^4*f2^2-6*e1*e3^3*f1^5*f3 -
  9*e1*e3^3*f1^2*f2^3+6*e2^4*f3*f2^2*e3-12*e2^3*f3*f2^3*e3+6*e2^2*f3*f2^4*e3 +
  27*e1*e3^3*f2*f1^3*f3+15*e3^2*e1*f3*f1^2*f2^3+10*e3^2*e1^3*f3*f1^2*f2^2-6*e3^2*e1^4*f2^2*f1*f3
 -15*e3^2*e1^2*f3*f1*f2^3+18*e3^3*e1^3*f2*f1*f3-6*e3^2*e1^2*f3*f1^3*f2^2 -
  9*e3^2*e2^2*e1^2*f2*f1*f3+18*e3^2*e2^2*e1*f2*f1^2*f3+3*e2*e3^2*e1^3*f2*f1^2*f3 -
  27*e2*e3^3*e1*f2*f1*f3-7*e2*e3^2*e1^2*f2*f1^3*f3-6*e2^2*e1^2*f3*f1^2*f2^2*e3 +
  3*e2^2*e1*f3*f1^3*f2^2*e3-7*e2^2*e1*f3*f1*f2^3*e3+3*e2^2*e1^3*f2^2*f1*f3*e3 +
  5*e2*e1*e3^2*f3*f2*f1^4+3*e1*e2^3*f2*f1^3*f3*e3+e2^4*e1*f2*f1*f3*e3-7*e2^3*e1*f2^2*f1*f3*e3 +
```

```
  3*e2*e1^3*f3*f1*f2^3*e3-e2*e3^2*e1^3*f1*f2^3-2*e2^3*f3*f2*f1^4*e3+10*e2^3*f3*f1^2*f2^2*e3 -
  2*e2^4*f2*f1^2*f3*e3-2*e2^3*e1^2*f3*f2^2*e3+3*e2*e3^2*e1^2*f1^2*f2^3-2*e2^2*f3*f1^2*f2^3*e3 +
  10*e2^2*e1^2*f3*f2^3*e3-e2*e1^2*f3*f1^2*f2^3*e3-2*e2*e1^4*f3*f2^3*e3-2*e2*e1^2*f3*f2^4*e3 +
  e1*e2*f3*f1*f2^4*e3-e2^3*e1^2*f2*f1^2*f3*e3
}

gReQ(a,b,c,d)=
{ my(e1 = -b/a, e2 = c/a, e3 = -d/a);
  my(f1 = conj(e1), f2 = conj(e2), f3 = conj(e3));

X^6+(-2*f2*e1-2*f1*e2)*X^5+(f1^2*e2^2+2*f2*e2^2-6*f3*f1*e2+2*f2^2*e2+3*f1*f2*e2*e1
+3*f2*f1*e3-27*f3*e3+2*f1^2*e3*e1-6*f2*e3*e1+f2^2*e1^2+3*f3*e2*e1+2*f3*f1*e1^2)*X^4
+(-f1^2*f2*e2^2*e1+9*f3^2*e2*e1-2*f1^3*e1*e2*e3+9*f2*f1*e3^2+5*f2*f1*e3*e2*e1
+9*f3*e3*e2*e1-2*f2^3*e1*e2-5*f1^2*f2*e3*e2-2*f3^2*e1^3-2*f1*f2*e2^3-f2^2*f1*e1^2*e2
-5*f3*f2*e1^2*e2-5*f3*f1*e2^2*e1+27*f3*f1*e3*e2-2*f3*f1^2*e1^2*e2+5*f2*f1*f3*e2*e1
-2*f2^2*f1*e2^2+4*f2^2*e3*e1^2+27*f3*f2*e3*e1-5*f2^2*f1*e3*e1+6*f3*f1^2*e3*e1+6*f2^2*e3*e2
+9*f3*f2*f1*e3-2*f3*e2^3-27*f3*e3^2-2*f1^3*e3^2-2*f2^3*e3-27*f3^2*e3+6*f3*f1*e3*e1^2
-2*f1^2*f2*e3*e1^2-2*f2*f1*f3*e1^3+6*f3*f2*e2^2-2*f2^2*e2^2*e1+4*f3*f1^2*e2^2)*X^3
+(27*f3*f1*e3^2*e2+f1^4*e3^2*e1^2-6*f2^2*f1*f3*e2^2+2*f3*f1^2*e1*e2^3-27*f3*f2*e2^2*e3
-3*f2^2*f1*e2^2*e3-6*f1^2*f2*e3^2*e1^2+2*e3^2*f1^4*e2+3*f1^2*f2*e2^2*e1*e3
-9*e3^2*f2*f1^2*e2-6*f2^2*e3*e2^2*e1-18*f3*f2*f1^2*e3*e2+2*f2^4*e3*e1+f3^2*f1^2*e1^4
-18*f3*f2*e3*e2*e1^2+2*f2^3*f1*e3*e1^2-9*f3^2*f2*e2*e1^2-6*f3^2*f1^2*e2*e1^2
-27*f3^2*f1*e3*e1^2+108*f3^2*f1*e3*e2+81*f3*f2*f1*e3^2-9*f3*f1*e3*e2^2*e1-27*f2^3*e3^2
+9*e3^2*f2^2*e1^2+f2^2*f1^2*e1^3*e3+2*f3*f1*e2^4+81*f3^2*e3*e2*e1-2*f2^3*e2^3
-27*f3^2*e2^3+5*f2^3*f1*e3*e2+5*f3^2*f1*e1^3*e2+2*f2^2*f3*e1^3*e2+5*f3*f2*e1*e2^3
-3*f3*f1^2*e3*e1^2*e2-27*f2^2*f3*e3*e2+9*f2^2*f1^2*e3^2+f2^2*f1*e1*e2^3+f2^3*f1*e2^2*e1
-18*f3^2*f1*e2^2*e1-3*f2^2*f3*e2^2*e1-27*f3*f1^2*e3^2*e1-9*f2^2*f1*f3*e3*e1
+f1^3*f2*e1^2*e2*e3+108*f3*f2*e3^2*e1+27*f3^2*f2*e3*e1-18*f2^2*f1*e3^2*e1
+3*f2^2*f1*f3*e1^2*e2+f2*f1^2*f3*e1^3*e2-27*f1^3*f3*e3^2+2*f1^3*f2*e2^2*e3+f2^2*e2^4
+6*f3*f2*f1*e3*e1^3+3*f2*f1*f3*e2^2*e1^2+9*f3^2*e2^2*e1^2-2*f2^3*e3*e1^3-2*f3*f1^3*e3*e1^3
+f1^3*f3*e2^2*e1^2+6*f2*f1*f3*e2^3+6*f2^3*e3*e2*e1-72*f3*f2*f1*e3*e2*e1
+6*f3*f1^3*e3*e2*e1+3*f2^2*f1^2*e3*e2*e1+f2^2*f1^2*e2^3+f2^3*e2^2*e1^2-2*f1^3*f3*e2^3
+f2^4*e2^2-3*f3*f2*f1^2*e3*e1^2+5*f1^3*f2*e3^2*e1+9*f3^2*f1^2*e2^2-27*f3^2*e3*e1^3
+2*f3^2*f2*e1^4)*X^2
+(-54*f2^3*e3^3-54*f3^3*e2^3-3*f1^4*f2*e3^3-27*f3^2*e3*e2^3+3*f1*f2^3*e3^2*e1^2
-8*f1^3*f3*e2^3*e3+18*f1*f2^3*e3^2*e2-2*f1^3*f2^2*e3^2*e1^2-27*f3^3*f1*e2^2*e1
-3*f2*f1*f3*e2^4*e1-2*f2^4*e3*e2*e1^2+18*f3^2*f2*f1*e2^3+27*f2^2*f1^2*f3*e3^2
+18*f2^3*e3^2*e2*e1-2*f2^3*f1^2*e3*e2^2-54*f3^2*f1^3*e3^2+27*f3^2*f1^2*e3*e2^2
-3*f2^4*f1*e3^2+27*f2^2*f1^2*e3^3-2*f1^3*f3^2*e2^3+4*f3*f2^2*e2^4-2*f3*f2^3*e2^3
-27*f2^3*f3*e3^2+33*f1^3*f3*e3^2*e2*e1-135*f3^2*f2*f1*e3*e2*e1+18*f1^3*f2*f3*e3^2*e1
-2*f2^3*e3^2*e1^3+6*f3*f2*f1*e3*e2^2*e1^2+33*f3^2*f2*f1*e1^3*e3-2*f2^5*e3*e2
+15*f1^3*f2*e3^3*e1-2*e3^2*f1^3*f2*e2^2+6*f3^2*f1*e2^4-2*f3^3*f1*e1^5-3*f3^3*e1^4*e2
-3*f3^2*e2^4*e1-27*f3*f1^2*e3^3*e1-f3*f2*f1^3*e2^3*e1+3*f2^2*f1*e3^2*e2*e1^2
-f1^3*f2*e3^2*e2*e1^2+9*e3^2*f2^2*f1*e2^2+9*f3*f1^2*e3^2*e2*e1^2-135*f3*f2*f1*e3^2*e1
+18*f3^2*f1*e3*e1^3*e2-3*f3^2*f2*f1*e1^4*e2+15*f3*f2*f1^2*e1*e3*e2^2+33*f3*f2*f1*e2^3*e3
-27*f3*f2*e3^2*e2*e1^2-27*f3^2*f1^2*f2*e3*e2-2*f3*f1^2*e2^3*e1*e3-f1*f2^2*e2^3*e1*e3
-27*f2^2*f1*e3^3*e1+4*f2^4*e3*e2^2-2*f2^3*e2^3*e3-27*f3^3*e1^3*e3+27*f3^3*e1^2*e2^2
-54*f3^2*e3^2*e1^3-f1^3*f2^2*e3*e2^2*e1+3*f3*f2^2*e2*e3*e1^3+3*f3*f2*f1^3*e3*e2^2
-27*f3*f2*e3^2*e2^2+81*f3*f2*e3^3*e1-108*f3*f2^2*e3^2*e2-3*f2^4*f1*e3*e2*e1
+15*f3*f2*e3*e2^3*e1-2*f3*f1^4*e3*e2^2*e1+15*f2^3*f1*f3*e3*e2-f3^2*f1^2*f2*e1^3*e2
-f2^2*f1*f3*e2^2*e1^3+9*f3^2*f1^2*f2*e3*e1^2-2*f2*f3*e2^5-108*f3^2*f1^2*e3^2*e1
+81*f3^2*f2*e3^2*e1+27*f3^2*e3*e2^2*e1^2+81*f3^2*e3^2*e2*e1+6*f2^2*f1^2*e3^2*e2*e1
-f2^3*f1*e3*e2*e1^3-5*f3^2*f2*e1^3*e2^2-f2^3*f1^2*e3*e2*e1^2+18*f3^2*f1^3*e3*e2*e1
+33*f2^3*f3*e3*e2*e1-f2*f1^2*f3*e2^3*e1^2-2*f2^3*f1*f3*e3*e1^2-3*f1^4*f2*e3^2*e2*e1
-f2^3*f1*f3*e2^2*e1+6*f3^2*f2*f1*e1^2*e2^2-f2^2*f1^2*f3*e2^2*e1^2+81*f3^3*e3*e2*e1
+3*f3^2*f1^2*f2*e2^2*e1+18*f3*f2*f1*e3^2*e1^3-2*f2^2*f1*f3*e3*e1^4-2*f1^5*e3^3*e1
-108*f3^2*f1*e3^2*e1^2-27*f3^3*f1*e3*e1^2+4*f3^2*f1^2*e3*e1^4-2*f3^2*f2^2*e2*e1^3
+3*f3^2*f1^2*e2^3*e1-f2^2*f1^2*e2^2*e1^2*e3-27*f3*f1^3*e3^3-2*f3*f2*f1^2*e2^4
-5*f1^3*f2^2*e3^2*e2+27*f3*f2^2*e3^2*e1^2-8*f2^3*f3*e3*e1^3-2*f2^2*f3*e2^3*e1^2
-108*f3^2*f2*e3*e2^2-5*f2^3*f1^2*e3^2*e1+4*f3*f1^4*e3^2*e1^2+81*f3^2*f1*e3^2*e2
+81*f3^3*f1*e3*e2+6*f3*f1^4*e3^2*e2-27*f3^2*f2^2*e3*e2-2*f1^3*f3*e3^2*e1^3
-5*f3^2*f1*e2^3*e1^2-2*f3^2*f1^2*e1^3*e2^2-2*f3^2*f1^3*e1^3*e3+6*f3^2*f2*e3*e1^4
+15*f3^3*f1*e1^3*e2+18*f3^2*f2*e2^3*e1+9*f3^2*f2^2*e2^2*e1+81*f2*f1*f3*e3^3
+81*f3^2*f2*f1*e3^2+6*f2^4*e3^2*e1+6*f2^2*f1^2*f3*e3*e1*e2+15*f2^2*f1*f3*e3*e1^2*e2)*X
+9*f1^3*f3*e3^3*e2*e1-15*f3^3*f2*e2^2*e1^3-27*f3^4*e2^3-9*e3^2*f3*f2*f1*e2^2*e1^2
+f3^2*f2^3*e2^2*e1^2-9*f2^2*f1^2*e3^3*e2*e1+e3^2*f2^3*e2^2*e1^2-2*e3^2*f1^3*f3*e2^3
-27*f3*f2*f1*e3^3*e2*e1+f2^2*f1^2*e3^3*e1^3+e3^2*f1^3*f3*e2^2*e1^4+2*f3^2*f2*e2^4*e1^2
-6*f3^2*f2^2*e2^3*e1^2-4*f2^3*e3^3*e1^3+e3^2*f1^3*f3*e2^2*e1^2+18*f2^3*e3^3*e2*e1
+2*f2^5*e1^2*e3^2+f3^4*e1^6+2*f2^3*f1^3*e3^3+f3^2*f2^2*e2^2*e1^4+2*f3^2*f2*e2^4*e1^2
+18*f3*f2*f1*e3^3*e1^3-27*f3^3*e3^2*e1^3-4*f3^2*f2^3*e2^3-27*f3^2*f1^3*e3^3
+2*f3^3*f1*e2^2*e1^4-9*f3^3*e2^4*e1+27*f2^2*f1^2*e3^4-9*f1^4*f2*e3^4+9*f3^2*f2^2*e2^4
-27*f3^3*e3*e2^3+f1^2*f3^2*f2^2*e2^3-9*f2^4*f1*e3^3-81*f3^2*f2*e3^2*e2^2
+2*f3^3*e2^3*e1^3+27*f3^3*f2*e3*e2*e1^2-15*f3^2*f1*e3*e2^3*e1^2+27*f3^2*f2*e3^2*e2*e1^2
+2*f3^2*f2^2*f1*e3*e1^4+27*f3^3*f1*e3*e2*e1^3-10*f3^2*f1^3*e3*e2^2*e1^2
```

```
+27*f3^2*f2*f1*e3^2*e1^3+27*f3^3*f1^2*e3*e2*e1^2+27*f3^2*f1^2*e3^2*e2^2+f3^2*f1^4*e2^4
-3*f3^2*f1^3*f2*e3*e2*e1^2-7*f3^2*f2*f1^2*e1^3*e2*e3-15*f3^2*f2^2*e3*e2*e1^3
+2*f3^2*f2^2*e3*e1^5-6*f3^3*f1^2*e3*e1^4-2*f3^2*f2^3*e3*e1^3-9*f3^4*e2*e1^4
-9*f3^2*f2^2*f1^2*e3*e2*e1-9*f3^3*f1*e2^3*e1^2+18*f3^3*f2*f1*e2^3-81*f3^3*f2*e3*e2^2
+2*f3^2*f1*e2^5*e1+27*f3^2*e3^2*e2^2*e1^2-9*f3^2*e3*e2^4*e1+f3^2*f1^2*e2^4*e1^2
-9*f3^3*f1^2*e2^3*e1-3*f3*f1^2*f2*e2*e3^2*e1^3-8*f3^2*f1^3*e3*e2^3+9*e3^2*f3*f2*f1*e2^3
+f3^2*e2^6+e3^2*f2^2*f1^2*e2^3-4*f1^3*f3*e3^3*e1^3-27*f2^3*f3*e3^3-6*f2^5*e3^2*e2
-6*f3^2*f1^2*f2*e2^4+27*f3^4*e2^2*e1^2-27*f3^2*e3^3*e1^3-4*f3^3*f1^3*e2^3+f2*f1*f3*e2^4*e1*e3
+27*f2^2*f1*f3*e3^3*e1-18*f3*f2*f1^2*e1*e3^2*e2^2-54*f3^2*f2*f1*e3^2*e2*e1
-81*f3^2*f2^2*e3^2*e2-7*f2^2*f1*f3*e2^3*e1*e3-9*f3^2*f2*e3*e2^2*e1^3+9*e3^2*f3^2*f1^2*e1^4
-4*f3^3*f1^3*e3*e1^3-81*f3^3*f1*e3^2*e1^2+54*f3^3*e3*e2^2*e1^2-6*f3^3*f1*e3*e1^5
+12*f3^2*f1^3*e3^2*e1^3+9*f3^2*f1^4*e3^2*e1^2-81*f3^2*f1*e3^3*e1^2-81*f3^3*f1^2*e3^2*e1
-81*f3^2*f1^2*e3^3*e1+3*f3^2*f1^2*f2*e2^3*e1^2+27*f3^3*f1*e3*e2^2*e1+f3^2*f1^3*f2*e1*e2^3
-5*f3^2*f2*f1*e2^4*e1+f3^2*f1*f2^2*e1^3*e2^2+27*f3^2*f2^2*f1*e3*e2^2-9*f3^2*f1^3*f2*e2^2*e3
-5*f3^2*f2*f1*e3*e2*e1^4+2*f3^3*f2*e1^5*e2-6*f3^2*f1^2*e3*e2^2*e1^3+27*f3^2*f1^2*e3^2*e2*e1^2
+9*f3^3*f2*f1*e3*e1^3-18*f3^2*f2^2*f1*e3*e2*e1^2+27*f3^2*f1*e3^2*e2*e1^3-27*f3^3*f2*f1*e3*e2*e1
+f2^6*e3^2+f3^3*f2*f1*e1^4*e2+27*f3^2*f1^2*f2*e3^2*e2-9*f3^3*f2*f1*e2^2*e1^2-3*f3^2*f2^2*f1*e2^3*e1
+2*f3^2*f2*f1*e2^3*e1^3+27*f3^2*f2*f1*e3*e2^3+f2*f1^2*f3*e2^3*e1^2*e3+27*f3^2*f1*e3^2*e2^2*e1
+27*f3^2*f2^2*f1*e3^2*e1+18*f3^3*f1^3*e3*e2*e1-15*f3^2*f1^2*e3*e2^3*e1+27*f3^2*f2*e3*e2^3*e1
+9*f3^2*f2^3*e3*e2*e1+27*f3^2*f1^3*f2*e3^2*e1+3*f3*f2*f1^3*e2^3*e1*e3+f2^4*f1*f3*e1*e2*e3
-7*f1^3*f2*f3*e2*e3^2*e1^2+27*f3^2*f2^2*e3*e2^2*e1-6*f3^2*f1^4*e3*e2^2*e1+27*f3^2*f1^3*e3^2*e2*e1
-9*f3^3*e3*e1^4*e2-7*f2^3*f1*f3*e2^2*e1*e3+6*f2^2*f1^2*f3*e2^2*e1^2*e3+3*f3*f2^2*f1^3*e2^2*e1*e3
-27*f3^3*f1^3*e3^2-4*e3^2*f2^3*e2^3-27*f2^3*e3^4+2*f2^4*f1^2*e3^2*e2+27*f3^2*f2^2*e3^2*e1^2
+2*f2^5*f1*e1*e3^2-6*f2^3*f1^2*e3^2*e2^2+f2^4*e1^4*e3^2-9*f1^4*f2*f3*e3^3+54*f2^2*f1^2*f3*e3^3
-6*f2^4*e3^2*e2*e1^2+2*f1^3*f2^2*e3^3*e1^2+27*f1*f2^3*e3^3*e2-9*f1*f2^3*e3^3*e1^2
+2*f2^3*f1^3*e3^2*e2*e1-10*f2^2*f1^2*f3*e3^2*e1^3+27*f3*f1^2*f2*e3^3*e1^2+27*f1^3*f2*f3*e3^3*e1
+27*f2^2*f1*f3*e3^2*e2^2-6*f2^4*f3*e2^2*e3+12*f3*f2^3*e2^3*e3-6*f3*f2^2*e2^4*e3
-10*f2^2*f1^2*f3*e2^3*e3+2*f2^4*f3*e1^2*e2*e3+f3^2*f2^2*f1^2*e1^3*e3+2*f3*f2^3*e1^4*e2*e3
-6*f2^2*f1^3*f3*e3^2*e1^2+27*f2^3*f1*f3*e3^2*e2+2*f3*f1^4*e3^2*e2^2*e1-5*f2^4*f1*e3^2*e2*e1
-81*f3*f2^2*e3^3*e2-15*f3*f2*f1^3*e3^2*e2^2-9*f3*f2^2*e2*e3^2*e1^3+f1^3*f2^2*e3^2*e2^2*e1
+27*f3*f1^2*f2*e3^3*e2-3*f1*f2^3*e3^2*e2^2*e1-6*f2^2*f1*f3*e3^2*e1^4+27*f3*f2^2*e2^2*e3^2*e1
-15*f2^3*f1*f3*e3^2*e1^2+27*f2^3*f3*e3^2*e2*e1-15*f2^3*f1^2*f3*e3^2*e1+3*f2^3*f1^2*e3^2*e2*e1^2
+f2^3*f1*e3^2*e2*e1^3-9*f3*f2^2*f1^3*e3^2*e2+2*f2^2*f3*e2^3*e1^2*e3+2*f1^4*f2*f3*e2^3*e3
+2*f3*f2*f1^2*e2^4*e3+27*f3^3*f1^2*e3*e2^2+2*f3*f1^5*e2^2*e3^2-6*f3*f1^4*e3^3*e1^2
+2*f3^3*f1^2*e1^3*e2^2+f2^2*f1^4*e2^2*e3^2-6*f3*f1^5*e3^3*e1-9*f2^3*f1^2*e3^3*e1
+f2^4*f1^2*e1^2*e3^2-9*f2^4*f1*f3*e3^2+2*f1^5*f2*e3^3*e2+2*f2^2*f1^4*e3^3*e1+2*f2^4*f1*e1^3*e3^2
-8*f2^3*f3*e3^2*e1^3+27*f3*f2^2*e3^3*e1^2-15*f1^3*f2^2*e3^3*e2+27*f3^2*f2^2*f1^2*e3^2
+2*f3^2*f1^3*e2^4*e1+2*f2^3*f1^2*f3*e2^2*e3-10*f2^3*f3*e2^2*e1^2*e3+3*f2^3*f1*f3*e1^3*e2*e3
+f2^3*f1^2*f3*e1^2*e2*e3+f3^3*f1^3*e2^2*e1^2+27*f3^3*f2*e2^3*e1-5*f1^4*f2*f3*e2*e3^2*e1
+27*f3^2*f1^2*f2*e3^2*e1^2-6*f3^2*f2*e2^5+9*f2^4*e3^2*e2^2+2*f3^2*f1^2*e2^5+3*f2^2*f1*f3*e2^2*e1^3*e3;
}
```

# Bibliography


[1] K. Belabas, *Variations sur un thème de Davenport et Heilbronn*, PhD Thesis, Université Bordeaux 1, 1996.

[2] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no.219, 1213–1237.

[3] K. Belabas, *Paramétrisation de structures algébriques et densité de discriminants [d'après Bhargava]*, Astérisque, Vol. **299** (2005), Exp. No. 935, pp. 267–299, Séminaire Bourbaki. Vol. 2003/2004.

[4] K. Belabas, *L'algorithmique de la théorie algébrique des nombres*, dans *Théorie algorithmique des nombres et équations diophantiennes* (N. Berline, A. Plagne, C. Sabbah eds.) Ed. de l'École Polytechnique, 85–153 (2005).

[5] M. Bhargava,*Higher composition laws*, PhD Thesis, Princeton University, 2001.

[6] M. Bhargava,*Higher composition laws I: A new view of Gauss composition*, Ann. of Math. **159** (2004), 217–250.

[7] M Bhargava,*Higher composition laws II: On cubic analogues of Gauss composition*, Ann. of Math. **159** (2004), 865–886.

[8] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. **162** (2005), 1031–1063.

[9] M. Bhargava, *The density of of discriminants of quintic rings and fields*, Ann. of Math., to appear.

[10] L. Bianchi, *Sui gruppi di sostituzioni lineari con coefficienti appartenenti a corpi quadratici immaginari*, Math. Ann. **40** (1892), 332–412 [Opere Matematiche, Vol. 1, pt. 1, p. 270–373].

[11] H. Cohen, *A Course in Computational Algebraic Number Theory (fourth corrected printing)*, Graduate Texts in Math. **138**, Springer-Verlag, 2000.

[12] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Math. **193**, Springer-Verlag, 2000.

[13] H. Cohen, *Comptage exact de discriminants d'extensions abéliennes*, J. Th. Nombres de Bordeaux **12** (2000) 379–397.

[14] H. Cohen, *Counting $A_4$ and $S_4$ number fields with given resolvent cubic*, Fields Institute Communications **41** (2004) 159–168.

[15] H. Cohen, *Number Theory II, Analytic and Modern Tools*, Graduate Texts in Math. **240**, Springer-Verlag, 2007.

[16] H. Cohen, *Constructing and counting number fields*, Proceedings of the ICM, Beijing 2002, Vol. 2, 129–138.

[17] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Cyclotomic extensions of number fields*, Indag. Math. **14** (2003) 183–196.

[18] H. Cohen, F. Diaz y Diaz, and M. Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. reine angew. Math. **550** (2002) 169–209.

[19] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Counting discriminant of number fields*, J. Th. Nombres Bordeaux **18** (2006) 573–593.

[20] H. Cohen and A. Morra, *Counting cubic extensions with given quadratic resolvent*, preprint.

[21] H. Cohn, *The density of abelian cubic fields*, Proc. Amer. Math. Soc. **5** (1954) 476–477.

[22] J. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Mathematica, **51**, n. 3 (1984) 275–324.

[23] J. Cremona, *Reduction of binary cubic and quartic forms*, London Mathematical Society ISSN 1461–1570, 1999.

[24] J. Cremona, *Reduction of binary forms over imaginary quadratic fields*, slides of the talk given in Bordeaux (2007), can be found at http://www.warwick.ac.uk/staff/J.E.Cremona/papers/jec_bordeaux.pdf.

[25] J. Cremona and M. Stoll, *On the reduction theory of binary forms*, J. reine angew. Math. **565** (2003) 79–99.

[26] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields (ii)*, Proc. Roy. Soc. Lond. A **322** (1971), pp. 405–420.

[27] B. Datskovsky and D. J. Wright, *Density of discriminants of cubic extensions*, J. reine angew. Math. **386** (1988) 116–138.

[28] B. N. Delone and D.K. Faddeev, *The theory of irrationalities of the third degree*, volume 10 of Translations of Mathematical Monographs, American Mathematical Society, Providence (1964).

[29] J. A. Dieudonné and J. B; Carrell, *Invariant theory, old and new*, Academic Press, New York-London (1971).

[30] J. S. Ellenberg and A. Venkatesh, *Counting extensions of function fields with bounded discriminant and specified Galois group*, in "Geometric methods in algebra and number theory", Prog. Math., **235**, Birkhäuser Boston (2005), 151–168.

[31] J. Elstrodt, F. Grunewald and J. Mennicke, *Groups Acting on Hyperbolic Space,*Harmonic analysis and number theory. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1998.

[32] J. Elstrodt, F. Grunewald and J. Mennicke, *Zeta-functions of binary Hermitian forms and special values of Eisenstein series on three-dimensional hyperbolic space*, Math. Ann. **277** (1987), 655–708.

[33] J. Elstrodt, F. Grunewald and J. Mennicke, *Eisenstein series on three-dimensional hyperbolic space and imaginary quadratic number fields*, J. Reine Angew.Math. **360** (1985), 160–213.

[34] W. T. Gan, B. Gross and G. Savin, *Fourier coefficients of modular forms on $G_2$*, Duke Math. J. (2002), 105–169.

[35] C. F. Gauss, *Arithmetische Untersuchungen (Disquisitiones Arithmeticae*, Chelsea, 1889.

[36] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin, 1952.

[37] D. Hilbert, *Theory of algebraic invariants*, Cambridge University Press, Cambridge (1993).

[38] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society, Colloquium Publications, **53** (2004), Providence, RI.

[39] G. Julia, *Etude sur les formes binaires non quadratiques à indéterminées réelles ou complexes*, Mémoires de l'Académie des Sciences de l'Institut de France **55** (1917) 1–296. Also in Julia's Oeuvres, vol. 5.

[40] J. Klüners, *A counterexample to Malle's conjecture on the asymptotics of discriminants*, C. R. Math. Acad. Sci. Paris **340** (2005), 411–414.

[41] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math J. **11**, Issue 3, (1964), 257–262.

[42] S. Mäki, *On the density of abelian number fields*, Thesis, Helsinki, 1985.

[43] G. Malle, *On the distribution of Galois groups*, J. Number Theory **92** (2002), 315–329.

[44] G. Malle, *The totally real primitive number fields of discriminant at most $10^9$*, Lecture Notes in Comput. Sci., **4076**, Springer, Berlin (2006), 114–123.

[45] A. Morra, *An algorithm to compute relative cubic fields*, preprint.

[46] D. Mumford, *Geometric invariant theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Band **34**, Springer-Verlag, Berlin-New York (1965).

[47] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischen Körper zueinander*, J. reine angew. Math. **166** (1932) 201–203.

[48] J.-P. Serre, *Corps Locaux (2nd ed.)*, Hermann, Paris, 1968. English translation: Graduate Texts in Math. **67**, Springer-Verlag, 1979.

[49] R. G. Swan, *Generators and Relations for certain Special Linear Groups*, Advances in Mathematics **6**, (1971) 1-77.

[50] T. Taniguchi, *Distribution of discriminants of cubic algebras*, preprint 2006, arXiv:math.NT/0606109v1.

[51] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Institut Elie Cartan **13** (1990), Nancy.

[52] S. Türkelli, *Connected components of Hurwitz Schemes and Malle's conjecture*, submitted.

[53] E. Whitley, *Modular symbols and elliptic curves over imaginary quadratic number fields*, PhD Thesis, Exeter (1990).

[54] T. Womack, *Explicit descent on elliptic curves*, PhD Thesis, Nottingham (2003).

[55] D. J. Wright, *Distribution of discriminants of Abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), 17–50.