UNIVERSITÀ DEGLI STUDI DI MILANO

FACOLTÀ DI SCIENZE E TECNOLOGIE

CORSO DI DOTTORATO IN SCIENZE MATEMATICHE
DIPARTIMENTO DI MATEMATICA FEDERIGO ENRIQUES
XXXII CICLO

APPLICATIONS OF PRIME DENSITIES IN NUMBER THEORY AND CLASSIFICATION OF NUMBER FIELDS WITH BOUNDED INVARIANTS

MAT 02,05

Tesi di dottorato di
Francesco Battistoni

Supervisore:
Prof. Giuseppe Molteni

Coordinatore:
Prof. Vieri Mastropietro

Anno Accademico 2018/2019

"In mezzo c'è tutto il resto
E tutto il resto è giorno dopo giorno
E giorno dopo giorno è
Silenziosamente
Costruire"
(Niccolò Fabi, *Costruire*)

Contents

Introduction

This Ph.D. thesis collects the author's works and interests in several parts of Number Theory, from algebraic problems related to relations between number fields which are based on the factorization of prime numbers in the rings of integers, up to the application of tools concerning the density of primes with given splitting type in number fields to the computation of the average rank of specific families of elliptic curves, concluding finally with the classification and estimate of the main invariants of a number field, like the discriminant and the regulator, pursued by means of analytic formulas and algorithmic methods developed on the previous tools and implemented on suitable computer algebra systems, like PARI/GP [75].
The *fil rouge* linking the aforementioned subjects is the role of Dedekind Zeta functions, which were the author's Master Thesis subject. Given a number field K, the Dedekind Zeta function of K is defined, in one of its equivalent formulations, as the infinite product

$$\zeta_K(s) := \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right)^{-1}$$

where $\mathfrak{p}$ ranges over the non-zero prime ideals of the ring of integers $\mathcal{O}_K$ and $\mathrm{N}(\mathfrak{p})$ is the norm of $\mathfrak{p}$, i.e. the size of the finite ring $\mathcal{O}_K/\mathfrak{p}$, while s is a complex variable with $\mathrm{Re}\, s > 1$. This object assumes central importance in a plenty of problems, and many are the insights which can give assuming different point of views for its study: we focus mainly on three approaches which are the dominant frameworks in this thesis, and they are the analytic, the algebraic and the algorithmic one.
As one immediately recognizes, the function $\zeta_K(s)$ can be seen as a generalization of the classic Riemann Zeta function, and so it is natural to begin a study of its analytic properties as a function of complex variable. Doing so, one gets that any Dedekind Zeta function can be meromorphically extended over the complex plane $\mathbb{C}$, and this can be done in such a way that $\zeta_K(s)$ admits a functional equation and an infinite collection of zeros, called non-trivial zeros of $\zeta_K(s)$, for which one conjectures that their real part is equal to $1/2$, so that we have a specific Riemann Hypothesis for every Dedekind Zeta function. This analytic framework is good for proving results concerning the distribution of prime ideals in number fields via techniques which mimic the ones used for proving the classic Prime Number Theorem.
From the analytic setting one can already detect the algebraic role of the Dedekind Zeta functions: in fact, the computation of the residue of $\zeta_K(s)$ at its unique pole, localized at

$s = 1$, gives as result a product involving all the main invariants of the number field K, like the class number h_K, the discriminant d_K, the regulator R_K, the number of roots of unity w_K and the numbers r_1 and r_2 of embeddings of the field K in $\mathbb{C}$, either as a proper subfield of $\mathbb{R}$ or as a subfield of $\mathbb{C}$ which is not contained in $\mathbb{R}$. Thus, $\zeta_K(s)$ encodes many arithmetic informations of the number field K, and actually this could be already seen by its very definition, which involves the norms of the prime ideals and consequently the factorization behaviour of the prime numbers in K. One could even wonder if the datum of the function $\zeta_K(s)$ is enough in order to completely characterize the isomorphism class of the number field K: this is the problem of arithmetic equivalence, which was studied too in the author's Master Thesis, and weaker form of this equivalence are studied in this work.

Another algebraic question solved by means of Dedekind Zeta functions consists in the study of the number of primes with given factorization behaviour in a number field K, and more in detail in the value of their density in the set of all primes. An answers to this problem is given by Chebotarev's Theorem, which relies heavily on the analytic properties of $\zeta_K(s)$ for its proof, and this result allows to obtain a framework in which it is possible to study both the weaker form of arithmetic equivalence and other problems which need density approaches.

Finally, let us go back to the analysis: just like for the Riemann Zeta function, one could set explicit formulae for every Dedekind Zeta function, i.e. relations arising from analytic tools applied to $\zeta_K(s)$ and which provide an explicit link between the algebraic invariants of the number field and other objects: as an example, Weil's explicit formula describes an explicit relation between the discriminant d_K, the prime ideals of $\mathcal{O}_K$ and the non-trivial zeros of $\zeta_K(s)$. Up to some assumption on the considered field and on the weight function, the relation can be reduced to an inequality which provides an estimate from below of the discriminant, so that an analytic method is able to give quantitative information on the values of an algebraic invariant.

If one was interested in a classification of number fields with bounded discriminant, this analytic setting derived from explicit formulae is then thought as one of the theoretical basis for a classification algorithm: combined with other tools from other branches of Mathematics and Number Theory, like the so called Geometry of Numbers, one can set up an algorithmic procedure which returns a complete list of number fields with bounded discriminants, and for this study it becomes mandatory to consider also concepts like the effectiveness and the speed of the employed procedure. A similar algorithmic study, starting from other kind of explicit formulae, can be set also for the study of the regulator R_K of a number field K and for the classification of number fields with bounded regulator. In conclusion, the role of Dedekind Zeta function consists also in providing theoretical tools on which one can set algoorithmic procedures for the estimate of algebraic invariants of number fields.

These are some of the various roles played by the Dedekind Zeta functions, and all the works and results contained in this thesis, although seeming quite heterogeneous, rely in fact on these several aspects.

In the next lines we give a summary of the collected work, presenting the parts in which is divided and underlying every time where is the author's specific contribution to the approached problems.

Part I consists in a collection of preliminary facts and theorems, with no degree of novelty in them, which are presented in order to provide the mathematical framework in which the remaining parts of the thesis are developed. The presented topics are quadratic forms and their role in the study of lattices in euclidean spaces; Algebraic Number Theory, including basic theory of the prime decomposition, Galois theory and an overview of the main invariants of number fields; Complex Analysis, with a focus on Perron Integral Formula, Phragmen-Lindelöf Theorem and the properties of entire function, plus an overview on Dedekind Zeta functions; elliptic curves, starting from few basic facts of Algebraic Geometry up to Weierstrass equations, Mordell-Weil theorems and the definition of elliptic surface.

Part II is called "Prime densities and applications" and contains Chapters 1, 2 and 3.

Chapter 1, "Chebotarev's Theorem: computation of prime densities", is intended as an additional preliminary chapter in which we present the specific tools needed for this part of the thesis, waiting for the new contributions by the author in the later chapters. We give a short review of the concept of prime density, introducing the two mostly used densities, which are the natural density and Dirichlet density, and we recall Chebotarev's Theorem. The chapter ends by presenting a classical lemma which permits to compute prime densities of primes with fixed splitting types also in number field extensions which are not Galois, together with a section which gives the values of prime densities for every splitting type in every number field extension of degree less or equal than 5, with distinctions given only by the Galois group of the Galois closure of these extensions.

Chapter 2 deals with Local GCD Equivalence, which is an equivalence relation occurring between number fields: given two number field extension K/F and L/F, the extensions are said to be F-locally GCD equivalent if, for every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ which is unramified in both the extensions, then the splitting type of $\mathfrak{p}$ in K coincides with the splitting type of $\mathfrak{p}$ in L. This relation was originally studied by Manfred Lochter [43] as a weaker form of stronger and more studied equivalences, like arithmetic equivalence and Kronecker equivalence; among the results he got, Lochter proved that any two extensions K/F and L/F which are F-locally GCD equivalent and with $[K : F], [L : F] \leq 5$ are in fact F-isomorphic.

The goal of this chapter is to present a new proof of this result, different from Lochter's one: while the older proof was based on the theory of group representations, our new procedure relies on the use of prime densities, and more specifically we show how locally GCD equivalent fields can be isomorphic by looking at the density of the primes with fixed splitting type the fields share, and how to use these densities information to force the isomorphism. This different setting for the proof yields the following rigidity corollary: number fields extension of degree 2, 3 or 5 which share the same inert primes are isomorphic, so that we can state that this kind of extensions are uniquely characterized by

their inert primes. While for quadratic extensions this is a well known fact, for cubic and quintic extensions is not stated elsewhere with this clarity, although it is a straightforward consequence of Lochter's work.

Chapter 3 presents an application of prime densities and related tools to the study of average ranks of specific family of elliptic curves. Given a collection of rational elliptic curves, parametrized by rational numbers t, we consider it as an elliptic curve over the function field $\mathbb{Q}(t)$, and we look for the value of its rank over $\mathbb{Q}(t)$. Following Bettin, David and Delaunay [8], we show how to compute this rank for specific families of elliptic curves: the needed tool is provided by Nagao's conjecture, which for these families of curves returns the value of the above rank as an average over the prime numbers p involving the finite number of points mod p of the elliptic curves in the collection. Our contribution is given by the computation of the average rank of a very specific family of elliptic curves, which falls into the wider collection of Bettin, David and Delaunay, but for which the rank was not already computed because of the need of a computation involving prime densities, which was not used by the previous authors. We used prime densities and Chebotarev's Theorem in order to complete this computation, and found that these average ranks are equal to 0, unless in very few specific cases which are presented in Theorem 15.

Part III is called "Analytic and algorithmic methods" and contains Chapters 4, 5 and 6.

Chapter 4, which like Chapter 1 is a sort of additional preliminary section but way too specific to be contained in the first part of the thesis, deals with explicit formulae of Dedekind Zeta functions, and there we present the two kind of formula upon which the results of the later chapters are based on: these are Weil's explicit formula, which is the main analytic tool used in Chapter 5, and Friedman's explicit formula, which is extensively used in Chapter 6.

The subject of Chapter 5 is the classification of number fields with bounded discriminant and the search of the minimum discriminant for number fields with fixed signature: we begin this chapter by giving an overview of the problem, starting from Minkowski's lower bound for the discriminant of number fields up to Poitou, Odlyzko and Serre's method [58] to provide such lower bounds thanks to Weil's explicit formula. These attempts have proved to be very useful in providing lower bounds for families of number fields with fixed signature: together with this, we also recall the role of the local corrections, which are the lower bounds for the discriminants given by assuming the existence of prime ideals with small norm in the fixed family of fields, and we show Selmane's table of local corrections for fields of degree 8 and 9 in any signature.
Later, we give an overview of some tools of Geometry of Numbers which are helpful in the classification of number fields with low discriminant: in particular, we focus on Hunter-Pohst-Martinet's Theorem, which states that every number field with fixed signature and bounded discriminant contains an algebraic integer such that its Newton sums are bounded by functions depending only on the discriminant and the degree. This result has proven to be crucial for this kind of works, because it allows to associate every

number field with low discriminant to a finite range of values for the Newton sums of algebraic integers and therefore provides only a finite choice for the coefficients of the defining polynomials of the desired fields.
Combining these ideas from Geometry of Numbers with Weil's explicit formula and the local corrections, we present an algorithm for the classification of number fields with given signature and bounded discriminant. Although the theoretical steps of the procedure are very similar to the ones used in the algorithms which allowed several authors to get minimum discriminants and fields with low discriminants for degrees up to 7 and for some signature in degree 8, the actual implementation of this process is the novelty which allowed the author to get the desired discriminants in the remaining signatures for degree 8. In fact, the main novelty consists in the fact that the author was able to write a program in the computer algebra system PARI/GP and, with the aid of Karim Belabas and Bill Allombert from University of Bordeaux, to get minimum discriminants and complete tables of fields with bounded discriminants for the signatures $(2,3),(4,2),(6,1)$ (completing thus the degree 8 case) and also for signatures $(1,4)$ and $(3,3)$ in degree 9. These facts are well summarized in Theorem 25, which is the author's main contribution for this chapter.

Chapter 6 deals with a similar problem, which is the classification of number fields with fixed signature and bounded regulator. Starting from Friedman's explicit formula, we show how Astudillo, Diaz y Diaz and Friedman used the formula, combined with inequalities by Remak and Friedman which bound the discriminant of a number field in function of its regulator, in order to give a method which classifies the number fields with given signature and bounded regulator.
The presented method allowed them [3] to give a complete classification for number fields of degree up to 7 and for fields with signature (8,0), (0,4) and (9,0): the need of a complete list of fields with low discriminants for the procedure to work was the reason which stopped them from giving a classification for every signature in degree 8. We have provided these lists in Chapter 5, thus we have tried to investigate the problem of minimum regulators.
The main fact described in Chapter 6 is that, even with lists of Theorem 25, it is not possible to give a classification of number fields with bounded regulator in the signatures $(2,3),(4,2)$ and $(6,1)$ by using Astudillo, Diaz y Diaz and Friedman's method alone: in order to overcome this difficulty, we looked for an improvement of Remak-Friedman's inequaliy, which is the main theoretical tool needed for the classification method together with Friedman's explcit formula. In particular, the desired improvement should take into account the signature of the fields in a crucial fashion. This idea originates from the fact that, for totally real fields of degree less or equal than 11, Pohst [54] was able to prove that Remak-Friedman's inequality can in fact be improved consistently; moreover, whenever one deals with totally complex fields, Lemma 8 shows that the classic upper bound is sharp for this family of fields.
Starting from these considerations, the author and his supervisor conjectured new values for the upper bounds of Remak-Friedman's inequality which depend heavily on the signature of the involved fields. Although we were not able to mathematically prove it, we

used several computational tools to state that these conjectured values are very likely to be correct: moreover, we show in the final part of the chapter how these better upper bounds would yield a classification of number fields with bounded regulator for fields with signature $(6, 1)$ and how it would allow to give a more exhaustive classification than the already known one for fields with smaller degree, more specifically for signature $(3, 1)$ and $(5, 1)$ (but still no clue for signatures (2,3) and (4,2) comes from here).

The final part of the thesis consists in an appendix in which we present the tables containing the computational data of the algorithmic processes which led to the complete tables of number fields up to isomorphism presented in Theorem 25 of Chapter 5. The PARI/GP programs and the files collecting the detected polynomials can be found at the website **www.mat.unimi.it/users/battistoni/index.html**, together with the GP version of the complete tables.

Part I

Preliminaries

0.1 Quadratic forms and lattices

0.1.1 Positive definite quadratic forms

References for this section are contained in Siegel's lectures [67].

A **real quadratic form** is a function

$$q(x) := x^T A x = \sum_{i,j=1}^{n} a_{i,j} x_i x_j$$

where $A := (a_{i,j})_{i,j=1}^n$ is a symmetric square matrix of dimension n with real coefficients and $x := (x_1, \dots, x_n)$ is a vector in $\mathbb{R}^n$.
Equivalently, a quadratic form is a homogeneous polynomial $q(x) := \sum_{i,j=1}^n a_{i,j} x_i x_j$ of degree 2 with real coefficients and such that $a_{i,j} = a_{j,i}$ for every $i, j = 1, \dots, n$. With this definition, a quadratic form q induces a symmetric matrix A_q defined as

$$(A_q)_{i,j} := \begin{cases} a_{i,j} & i = j \\ a_{i,j}/2 & i \neq j. \end{cases}$$

Given a real vector space V of dimension n, let $A = (a_{i,j})_{i,j=1}^n$ be a real $n \times n$ symmetric matrix. Once a basis for V is fixed, the real quadratic form associated to A is defined on $v \in V$ as

$$q(v) := q(x) \tag{1}$$

where $x := (x_1, \dots, x_n)$ is the coordinate vector of v with respect to the fixed basis. If one chooses a different basis with coordinates y such that $x = Uy$ with $U \in \mathrm{GL}(n, \mathbb{R})$, then the symmetric matrix associated to q in the new basis is equal to UAU^{-1}, so that

$$q(v) = q(x) = x^T A x = (Uy)^T A U y = y^T (U^T A U) y.$$

Being $U^T A U$ a real symmetric matrix itself, one gets that the definition (1) of q over V is independent of the chosen basis.

A quadratic form over a real vector space V is said to be **positive definite** if $q(v) > 0$ for every $v \in V \setminus \{0\}$: this is equivalent to require that, for any fixed a basis of V, the matrix A_q associated to q with respect to the given basis defines a scalar product $\langle \cdot, \cdot \rangle_q$ on $\mathbb{R}^n$, which in turn yields a scalar product on V. The couple (V, q) is called a **real euclidean space**.

Let us suppose that the basis of V is fixed, so that any vector of V can be identified with a vector of $\mathbb{R}^n$. Let $\Lambda \subset V$ be the set of vectors with integer coefficients.
If q is a positive definite quadratic form, then any eigenvalue of A_q is positive. Let m and M be the minimum and maximum eigenvalue of A_q: then $m x^T x \leq q(x) \leq M x^T x$.
If $c > 0$ and $q(x) < c$, then $m x^T x < c$: thus, the coordinates of x are bounded, and so there exists only a finite number of vectors x with integer coefficients such that $q(x) < c$. In particular, there exists an element $\lambda \in \Lambda \setminus \{0\}$ such that $\min\{q(v) \colon v \in \Lambda \setminus \{0\}\} =: q(\lambda)$.

0.1.2 Lattices and their relation with quadratic forms

Let V be a real vector space of dimension n. A **lattice** $\Lambda \subset V$ is a free additive subgroup which is discrete with respect to the euclidean topology on V and such that its generators are $\mathbb{R}$-independent. A **full rank lattice** is a lattice such that its generators span V.
If $\Lambda := \langle \alpha_1, \dots, \alpha_n \rangle$ is a full rank lattice, its **fundamental parallelotope** is the set

$$\Pi_\Lambda := \left\{ \sum_{i=1}^{n} c_i \alpha_i \colon c_i \in [0,1] \ \forall i \right\}.$$

If $\Lambda := \langle \alpha_1, \dots, \alpha_n \rangle$, the **discriminant of the lattice** Λ is the number:

$$d(\Lambda) := \left(\det \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,n} \\ \cdots & \cdots & \cdots \\ \alpha_{n,1} & \cdots & \alpha_{n,n} \end{pmatrix} \right)^2$$

where $(\alpha_{j,1}, \dots, \alpha_{j,n})$ is the coordinate vector of α_j with respect to a fixed basis of V. By its definition, the value of $d(\Lambda)$ is invariant for every change of basis by a matrix $B \in \mathrm{GL}(n, \mathbb{Z})$ (these matrices represent indeed the linear transformations of V which fix lattices). Moreover, $\sqrt{d(\Lambda)}$ is exactly equal to the volume of the fundamental parallelotope.

Given an euclidean space (V, q) and a full rank lattice $\Lambda \subset V$, a natural question consists in estimating the minimum value the positive definite form q assumes over the non-zero elements of Λ. The following theorem is a classical answer to this problem.

Theorem 1 (Hermite)**.** *For every $n \in \mathbb{N}$ there exists a number $\gamma_n \in \mathbb{R}$ such that, for every euclidean space (V, q) of dimension n and for every full rank lattice $\Lambda \subset V$, the minimum value μ_1 which q assumes over $\Lambda \setminus \{0\}$ satisfies the inequality*

$$\mu_1 \leq \gamma_n (\det A_q \cdot d(\Lambda))^{1/n}. \tag{2}$$

Proof. See [10], Chapter II, Section 3.2, Theorem 1. □

The number γ_n is called the **Hermite constant of dimension** n. Here we collect the values of γ_n^n for $n \leq 8$. These numbers are known to be optimal (see [57], Chapter 3, Section 3 for more details):

n	1	2	3	4	5	6	7	8
γ_n^n	1	4/3	2	4	8	64/3	64	2^8

Given a full rank lattice $\Lambda \subset V$ and a positive definite quadratic form q, define the numbers

$$\mu_i := \inf\{\lambda \in \mathbb{R} \colon q(v) < \lambda\} \text{ contains } i \ \mathbb{R}\text{-independent points of } \Lambda\}, \quad i = 1, \dots, n.$$

It is clear that $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$. In particular it is $\mu_1 = \min\{q(v)\colon v \in \Lambda \setminus \{0\}\}$, and by their very definition, the vectors of Λ on which q assumes the values μ_i are $\mathbb{R}$-independent. The numbers $\mu_1, \ldots, \mu_n$ are called the **successive minima of** q **over** Λ; the following classical theorem provides an estimate for their product.

Theorem 2 (Minkowski)**.** *Let $\lambda_q =: \mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$ be the successive minima of a positive definite quadratic form q over a lattice in $\Lambda \subset V$. Then $\prod_{i=1}^{n} \mu_i \leq \gamma_n^n \cdot \det A_q \cdot d(\Lambda)$.*

Proof. See [10], pages 120, 205 and 332. □

Remark 1. Hermite's Theorem can be easily seen as a Corollary of Minkowski's Theorem: in fact,

$$\mu_1^n \leq \prod_{i=1}^{n} \mu_i \leq \gamma_n^n \cdot \det A_q \cdot d(\Lambda)$$

and it is enough to take the n-th root of the left and right hand side to recover (2).

0.2 Number fields and their invariants

0.2.1 Basic facts and prime decomposition

References for this section are contained in the Algebraic Number Theory books [38], [11], [32] and [33].

A number field K is a field containing the rational numbers $\mathbb{Q}$ and such that K is a finite dimensional $\mathbb{Q}$-vector space with respect to the multiplication of K. **The degree of** K **over** $\mathbb{Q}$ is the dimension of K as $\mathbb{Q}$-vector space, and it is denoted with $[K : \mathbb{Q}]$. Given a number field K, a **finite extension of number fields** L/K is a field L containing K which has finite dimension as K-vector space: this dimension is called **degree of** L **over** K and denoted with $[L : K]$. If $K \subseteq L \subseteq N$ is an inclusion of number fields, then $[N : K] = [N : L][L : K]$.

The ring of integers of K is the ring

$$\mathcal{O}_K := \{\alpha \in K\colon \exists p(x) \in \mathbb{Z}[x] \text{ which is monic and such that } p(\alpha) = 0\}.$$

This definition implies that $\mathbb{Z}$ is the ring of integers of the trivial number field $\mathbb{Q}$.
If K is a number field of degree n, then $\mathcal{O}_K$ is a free abelian group of rank n with respect to the usual addition. If $\mathcal{O}_K^*$ is the group of multiplicative units of $\mathcal{O}_K$, then $\mathcal{O}_K^*$ is isomorphic as abelian group to $\mathbb{Z}^r \times \mu_K$, where $r := r_1 + r_2 - 1$ and μ_K is the finite group of roots of unity contained in K.

Denote with $\mathcal{P}_K$ the set of non-zero prime ideals of K; then every $\mathfrak{p} \in \mathcal{P}_K$ is a maximal ideal, and $\mathcal{O}_K/\mathfrak{p}$ is a finite field. The size of the finite field $\mathcal{O}_K/\mathfrak{p}$ is called **the**

(absolute) norm of $\mathfrak{p}$ and is denoted with $\mathrm{N}(\mathfrak{p})$.
Any non-trivial ideal $\mathfrak{I} \subset \mathcal{O}_K$ admits a unique, finite factorization as product of prime ideals of $\mathcal{P}_K$: if $\mathfrak{I} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ as product of prime ideals, then the quotient ring $\mathcal{O}_K/\mathfrak{I}$ is finite and its size is equal to $\prod_{i=1}^{r} \mathrm{N}(\mathfrak{p}_i)$. The size of the quotient ring $\mathcal{O}_K/\mathfrak{I}$ is called **the (absolute) norm of $\mathfrak{I}$**, and is denoted with $\mathrm{N}(\mathfrak{I})$. This definition well fits with the definition of norm of a prime ideal, and it immediately yields that the norm is a multiplicative function on the set of non-trivial ideals of $\mathcal{O}_K$.

Given L/K a finite extension of number fields and $\mathfrak{p} \in \mathcal{P}_K$, consider the factorization of $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_{n_\mathfrak{p}}^{e_{n_\mathfrak{p}}}$$

where the primes q_j are distinct. Each exponent e_i is called **ramification degree** of the corresponding prime $\mathfrak{q}_i$, and the prime $\mathfrak{p}$ is said to be **ramified** if some e_i is strictly larger than one.
Given $\mathfrak{q} \in \mathcal{P}_L$, if $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_K$, the degree of the finite fields extension $(\mathcal{O}_L/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p})$ is called **the inertia degree of $\mathfrak{q}$ over $\mathfrak{p}$**.
Assume $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_{n_\mathfrak{p}}^{e_{n_\mathfrak{p}}}$ and let $f_1, \ldots, f_{n_\mathfrak{p}}$ be the inertia degrees of the primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_{n_\mathfrak{p}}$ respectively. Assume $f_1 \leq f_2 \leq \cdots \leq f_r$; the **splitting type of $\mathfrak{p}$ in** L is defined as the $n_\mathfrak{p}$-ple

$$f_L(\mathfrak{p}) := (f_1, \ldots, f_{n_\mathfrak{p}}).$$

If $f_L(\mathfrak{p}) = (1, 1, \ldots, 1)$, the prime $\mathfrak{p}$ **splits completely** in the field L; $\mathfrak{p}$ is also said to be a totally split prime.
There is a formula connecting the degree of the extension with the ramification and inertia indexes: fixed $\mathfrak{p} \in \mathcal{P}_K$, one has

$$\sum_{i=1}^{n_\mathfrak{p}} e_i \cdot f_i = [L : K].$$

0.2.2 Embeddings, traces and norms

Given a number field K, the Primitive Element Theorem ([48], Chapter 5, Theorem 5.1) assures the existence of an algebraic number $\alpha \in \mathbb{C}$ such that $K = \mathbb{Q}[\alpha]$, so that actually every number field can be thought as a subfield of $\mathbb{C}$. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial with $\deg f = [K : \mathbb{Q}]$ and such that $f(\alpha) = 0$: then there is a field isomorphism $\mathbb{Q}[x]/(f(x)) \to K$ which sends the equivalence class of x to α. Thanks to the existence of the ring of integers $\mathcal{O}_K$, $f(x)$ can always be assumed monic, irreducible and with integer coefficients; in this case $f(x)$ is said to be a **defining polynomial of** K.

Let $\alpha =: \alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(x)$ in $\mathbb{C}$: for every $i = 1, \ldots, n$ there are n field isomorphisms $\mathbb{Q}[x]/(f(x)) \to \mathbb{Q}[\alpha_i]$, and the composite isomorphisms $\sigma_i : K \to \mathbb{Q}[\alpha_i]$ are called **embeddings of K in $\mathbb{C}$**. The embeddings fix the elements of $\mathbb{Q}$ and send α to α_i, so that they provide isomorphic (and possibly different) realizations of K as subfield

of $\mathbb{C}$.
An embedding σ of K is called **real** if $\sigma : K \hookrightarrow \mathbb{R}$, otherwise is said to be **complex**. If τ is a complex embedding of K, then also $\bar{\tau} := {}^{-} \circ \tau$ is a complex embedding of K, where ${}^{-}$ is the usual complex conjugation on $\mathbb{C}$.
Let r_1 be the number of real embeddings of K, and let r_2 be the number of complex embeddings of K up to complex conjugation. If K has degree n, then

$$n = r_1 + 2r_2.$$

The couple (r_1, r_2) is said to be **the signature of** K. K is **totally real** if $r_1 = n$, and **totally complex** if $r_2 = n/2$.
If K has $p(x) \in \mathbb{Q}[x]$ as defining polynomial, then r_1 is the number of real roots of $p(x)$ and r_2 is the number of couples of complex conjugated roots of $p(x)$.

Let $\{\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \dots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}\}$ be the embeddings of K. Given $\alpha \in K$, **the trace of** α is defined as

$$\mathrm{Tr}(\alpha) := \sum_{i=1}^{r_1} \sigma_i(\alpha) + 2\,\mathrm{Re} \sum_{i=1}^{r_2} \sigma_{r_1+i}(\alpha),$$

while **the norm of** α is defined as

$$\mathrm{Nm}(\alpha) := \prod_{i=1}^{r_1} \sigma_i(\alpha) \prod_{i=1}^{r_2} |\sigma_{r_1+i}(\alpha)|^2.$$

Both $\mathrm{Tr}(\alpha)$ and $\mathrm{Nm}(\alpha)$ are in $\mathbb{Q}$: moreover, if $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}(\alpha)$ and $\mathrm{Nm}(\alpha)$ are in $\mathbb{Z}$. Finally, we have

$$|\mathrm{Nm}(\alpha)| = \mathrm{N}(\alpha \mathcal{O}_K).$$

Given L/K a finite extension of number fields, the restriction of any embedding τ of L to K gives an embedding σ of K. We write $\tau|\sigma$ to describe this. For every embedding σ of K, there are exactly $[L : K]$ embeddings τ of L such that $\tau|\sigma$.
Given $\beta \in L$, one defines the **relative trace of** L **over** σ and **relative norm of** L **over** σ as

$$\mathrm{Tr}_\sigma(\beta) := \sum_{\tau|\sigma} \tau(\beta), \qquad \mathrm{Nm}_\sigma(\beta) := \prod_{\tau|\sigma} \tau(\beta).$$

Both $\mathrm{Tr}_\sigma(\beta)$ and $\mathrm{Nm}_\sigma(\beta)$ are in K, and if $\beta \in \mathcal{O}_L$, then both of them are in $\mathcal{O}_K$.

0.2.3 Galois number fields

A number field F is said to be **Galois** if $\sigma_i(F) = F$ for every embedding σ_i of F. In this case the set $\{\sigma_1, \dots, \sigma_n\}$ forms a finite group G with respect to the composition: G is called the **Galois group of** F, which is denoted $\mathrm{Gal}(F/\mathbb{Q})$.
Any number field of degree 2 is Galois, with Galois group isomorphic to the cyclic group

of order 2.
A Galois number field can be either totally real or totally complex: it does not admit an intermediate signature.

Given L/F a finite extension of number fields, consider the group $\mathrm{Aut}(L/F)$ of field automorphisms $\tau : L \to L$ such that $\tau(F) = F$. The extension is said to be **Galois** if $\#\mathrm{Aut}(L/F) = [L : F]$, and in this case $\mathrm{Gal}(L/F) := \mathrm{Aut}(L/F)$ is said to be the **Galois group of the extension**.
If $F = \mathbb{Q}$, this definition coincides with the previous one.

Let L/F be a Galois number field extension, with Galois group $G := \mathrm{Gal}(L/F)$. Given an intermediate field $F \subseteq K \subseteq L$, the extension L/K is Galois too and its Galois group $\mathrm{Gal}(L/K)$ is a subgroup of G: this association provides a bijective correspondence between subextensions of L/F and subgroups of G. Moreover, the intermediate extension K/F is Galois if and only if the corresponding subgroup $\mathrm{Gal}(L/K)$ is normal in $\mathrm{Gal}(L/F)$: if this is the case, the Galois group $\mathrm{Gal}(K/F)$ is isomorphic to $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K)$.

Given a finite extension K/F of fields, the **Galois closure of** K/F is the smallest Galois extension $\widehat{K}/F$ such that $K \subseteq \widehat{K}$. If $f(x)$ is the defining polynomial of K/F, then $\widehat{K}$ is constructed by adding all the roots of $f(x)$ to K: thus, if $[K : F] = n$, then $\mathrm{Gal}(\widehat{K}/F)$ is a subgroup of the symmetric group S_n and $[\widehat{K} : F] \leq n!$. $\widehat{K}$ can be characterized also as the compositum field of all the fields $\sigma(K)$ where $\sigma \in \mathrm{Gal}(\widehat{K}/F)$.
Given a number field extension K/F, its **Galois core** is the biggest Galois extension L/F such that $L \subseteq K$.

Remark 2. The concept of Galois extension is in fact more general and can be defined in any class of fields, up to requiring a wider definition involving properties which are naturally satisfied in number fields.
As an example, any extension K/F of finite fields is Galois in this wider sense, with a cyclic group as Galois group.

0.2.4 Invariants

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n, and let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be the complex roots of $f(x)$. **The discriminant of** $f(x)$ is defined as

$$\mathrm{disc} f := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 .$$

One has $\mathrm{disc} f \in \mathbb{Z}$; moreover, $\mathrm{disc} f = 0$ if and only if $f(x)$ has a multiple root in $\mathbb{C}$.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis for a number field K of degree n, and let

$$\{\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}\}$$

be the embeddings of K.
The discriminant of the n-ple $(\alpha_1, \dots, \alpha_n)$ is defined as $D(\alpha_1, \dots, \alpha_n) := (\det M_\alpha)^2$ where

$$M_\alpha := \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_{r_1+1}(\alpha_1) & \sigma_{r_1+1}(\alpha_2) & \cdots & \sigma_{r_1+1}(\alpha_n) \\ \bar{\sigma}_{r_1+1}(\alpha_1) & \bar{\sigma}_{r_1+1}(\alpha_2) & \cdots & \bar{\sigma}_{r_1+1}(\alpha_n) \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_{r_1+r_2}(\alpha_1) & \sigma_{r_1+r_2}(\alpha_2) & \cdots & \sigma_{r_1+r_2}(\alpha_n) \\ \bar{\sigma}_{r_1+r_2}(\alpha_1) & \bar{\sigma}_{r_1+r_2}(\alpha_2) & \cdots & \bar{\sigma}_{r_1+r_2}(\alpha_n) \end{pmatrix}.$$

The discriminant can be also computed using traces, since $D(\alpha_1, \dots, \alpha_n) = \det N_\alpha$, where $N_\alpha := (\mathrm{Tr}(\alpha_i \alpha_j))_{i,j=1}^n$. This shows that $D(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$ in general, and that $D(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$ if $\alpha_i \in \mathcal{O}_K$ for every $i = 1, \dots, n$.

Assume now that $\{\alpha_1, \dots, \alpha_n\}$ denotes a $\mathbb{Z}$-basis for $\mathcal{O}_K$; then $D(\alpha_1, \dots, \alpha_n)$ is called **the discriminant of** $\mathcal{O}_K$ and is denoted with d_K. The value of d_K does not depend on the chosen $\mathbb{Z}$-basis for $\mathcal{O}_K$.
If $f(x) \in \mathbb{Z}[x]$ is a monic defining polynomial for K, then d_K divides $\mathrm{disc} f$, and moreover their ratio is a square integer.
The sign of the discriminant is uniquely defined by the signature of K: in fact, $d_K = (-1)^{r_2}|d_K|$.
The discriminant of a number field satisfies the following important arithmetical property: a prime number p ramifies in K if and only if p divides the integer d_K.

Remark 3. Consider the real vector space $\mathbb{R}^n$ and assume that it has coordinates $(x_1, \dots, x_{r_1}, x_{r_1+1}, y_{r_1+1}, \dots, x_{r_1+r_2}, y_{r_1+r_2})$, with $r_1 + 2r_2 = n$. Given a number field K of degree n, define the function

$$\begin{aligned} &\sigma : K \to \mathbb{R}^n \\ &\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \mathrm{Re}\, \sigma_{r_1+1}(\alpha), \mathrm{Im}\, \sigma_{r_1+1}(\alpha), \dots, \mathrm{Re}\, \sigma_{r_1+r_2}(\alpha), \mathrm{Im}\, \sigma_{r_1+r_2}(\alpha)) \end{aligned}$$

where the σ_i's are the embeddings of K. Then σ is an homomorphism of additive abelian groups.
Furthermore, being $\mathcal{O}_K$ a free abelian group of rank n, the function σ transforms the ring of integers $\mathcal{O}_K$ into a full rank lattice in $\mathbb{R}^n$. The discriminant $d(\sigma(\mathcal{O}_K))$ of this lattice is equal to $4^{-r_2}|d_K|$, so that the volume of the fundamental parallelotope of $\sigma(\mathcal{O}_K)$ is equal to $2^{-r_2}\sqrt{|d_K|}$.
If one considers the quadratic form $q(x) := \sum_{i=1}^{r_1} x_i^2 + \sum_{j=r_1+1}^{r_1+r_2}(x_j^2 - y_j^2)$, then q restricted to the lattice $\sigma(\mathcal{O}_K)$ is equal to the function $\mathrm{Tr}(x^2)$.

One can define another invariant for a number field: consider the function

$$\begin{aligned} l :&\mathcal{O}_K \to \mathbb{R}^{r_1+r_2} \\ &\alpha \mapsto (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_{r_1}(\alpha)|, 2\log|\sigma_{r_1+1}(\alpha)|, \dots, 2\log|\sigma_{r_1+r_2}(\alpha)|). \end{aligned} \tag{3}$$

Then the subgroup of units $\mathcal{O}_K^*$, which has a free part of rank $r_1 + r_2 - 1$ and a finite torsion part formed by the roots of unity contained in K, is sent by l into a lattice of rank $r := r_1 + r_2 - 1$, which is contained in the hyperplane $\sum_{i=1}^{r_1+r_2} x_i = 0$. If we write

$$l_i(\alpha) := \begin{cases} \log|\sigma_i(\alpha)| & i = 1, \dots, r_1 \\ 2\log|\sigma_i(\alpha)| & i = r_1+1, \dots, r_1+r_2, \end{cases}$$

and if $\varepsilon_1, \dots, \varepsilon_{r_1+r_2-1}$ are the units generating the free part of $\mathcal{O}_K^*$, then one defines the **regulator of** K as

$$R_K := |\det(l_i(\varepsilon_j))_{i,j=1}^{r_1+r_2-1}|.$$

The definition of R_K is based on the choice of the functions l_i, which it has been made by using every embedding of K except σ_{r+1}; since $\sum_{i=1}^{r_1+r_2} l_i(\varepsilon) = 0$ for every $\varepsilon \in \mathcal{O}_K^*$, it follows that any choice of r embeddings among the $r + 1$ which are available provides functions l_i which give the same value of R_K.
The regulator is the volume of the fundamental parallelotope of the lattice $l(\mathcal{O}_K^*)$, but only considering the lattice in a real vector space of dimension $r_1 + r_2 - 1$; if instead we look at $l(\mathcal{O}_K^*)$ as lattice in the hyperplane $x_1 + \cdots + x_{r_1+r_2} = 0$ in the real vector space $\mathbb{R}^{r_1+r_2}$, the $(r_1 + r_2 - 1)$-dimensional Hausdorff measure of the volume of its fundamental parallelotope is equal to $\sqrt{r+1}R_K$ by a projection argument.
The regulator R_K usually is not an algebraic number, although it is equal to 1 whenever K is an imaginary quadratic field.

One can define one more invariant: let K be a number field, and let I_K be the set of fractional ideals of K, i.e. the set of $\mathcal{O}_K$-modules contained in K which are isomorphic to integer ideals of $\mathcal{O}_K$. Consider the subgroup $\mathcal{P}_K$ of principal ideals. The quotient group $\mathrm{Cl}_K := I_K/\mathcal{P}_K$ is called the **class group of** K: it is a finite abelian group, and its size is denoted with h_K, so that the ring of integers $\mathcal{O}_K$ is a Principal Ideal Domain, i.e. all its ideals are principal, if and only if $h_K = 1$.
Moreover, thanks to Class Field Theory it follows that the class group classifies the Galois extensions L/K with abelian Galois group and which are **unramified**, i.e. such that no prime ideals of K ramify in L: in fact, to any subgroup H of Cl_K corresponds a unique unramified Galois extension L_H/K, and $\mathrm{Gal}(L_H/K) = H$.

Finally, let us define the last invariant we need. Consider the set $\hat{\mathcal{O}_K} := \{\alpha \in K \colon \mathrm{Tr}(\alpha \cdot \mathcal{O}_K) \subset \mathbb{Z}\}$; the set $\mathfrak{D}_K := \{\beta \in K \colon \beta \cdot \hat{\mathcal{O}_K} \subset \mathcal{O}_K\}$ is called the **Different ideal of** K.
It is an ideal of $\mathcal{O}_K$ which measures the ramification of the extension $K/\mathbb{Q}$: more in detail, a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is a prime factor of $p\mathcal{O}_K$ for a ramified prime integer p if and only if $\mathfrak{p}$ is a prime factor of $\mathfrak{D}_K$, and $\mathrm{N}(\mathfrak{D}_K) = |d_K|$ (see [50]). Moreover, Hecke ([29], page 234) showed that the class $[\mathfrak{D}_K]$ in Cl_K is always a square.

0.3 Complex analysis and Dedekind Zeta functions

0.3.1 Recalls from Complex Analysis

In this section we give a brief review of some tools and ideas of Complex Analysis which will be used mainly in Chapter 4 .

We begin by recalling a basic instance of the Perron Integral Formula, which is a key tool of computation for the explicit formulae of L-functions.

Theorem 3 (Perron)**.** *Let $\sigma > 0$. We have the formula*

$$\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{x^s}{s} ds = \begin{cases} 1 & x > 1, \\ 0 & 0 < x < 1. \end{cases} \tag{4}$$

Proof. Let us suppose first that $x > 1$. Fix positive numbers B and T, and consider the rectangle R in the complex plane with vertexes $\sigma - iT, \sigma + iT, -B + iT$ and $-B - iT$. Take the integral of the meromorphic function x^s/s over the boundary of R counterclockwise considered: by the Residue Theorem, it is equal to the residue of x^s/s in 0, which is 1. Formula (4) follows if one is able to show that the integrals over the left vertical lines and the horizontal lines go to zero for suitable choices of T and B going to infinity.
In fact, the integral over the upper horizontal line is estimated by

$$\left| \int_{\sigma}^{-B} \frac{x^{u+iT}}{u+iT} \mathrm{d}u \right| = \left| \int_{0}^{B+\sigma} \frac{x^{\sigma-u+iT}}{\sigma-u+iT} \mathrm{d}u \right| \leq x^{\sigma} \int_{0}^{+\infty} \frac{x^{-u}}{T} \mathrm{d}u = \frac{x^{\sigma}}{T(\log x)}$$

and the last term goes to zero for $T \to +\infty$.
The integral over the left vertical line is instead estimated by

$$\left| \int_{T}^{-T} \frac{i x^{-B+it}}{-B+it} \mathrm{d}t \right| \leq \int_{-T}^{T} \frac{x^{-B}}{B} \mathrm{d}t = 2T \frac{x^{-B}}{B}$$

and the last term goes to zero for $T \to +\infty$ and $B \to +\infty$, up to choosing B of the correct order of magnitude: as an example, take $B = T$.
In this way we get Perron formula for $x > 1$: the proof for $0 < x < 1$ is completely similar, the only difference being that the assumption on x allows to choose the vertexes $B \pm iT$ instead of $-B \pm iT$, so that the integral over the boundary of R is equal to 0. □

An **entire function** is a function $f : \mathbb{C} \to \mathbb{C}$ which is holomorphic over the whole complex plane $\mathbb{C}$. If f has infinitely many zeros, then they form a discrete set which accumulates to infinity. The following theorem, due to Hadamard, gives a canonical decomposition of entire functions as infinite products depending on their zeros.

Theorem 4 (Hadamard)**.** *Let $f(z)$ be an entire function, and let $\{a_n\}$ be its set of zeros which are not equal to 0. There exist integers $m \in \mathbb{Z}_{\geq 0}$, $m_n \in \mathbb{Z}_{\geq 0}$ for every $n \in \mathbb{N}$ and entire function $g(z)$ such that*

$$f(z) = z^m e^{g(z)} \prod_{n=1}^{\infty} \left(1 - \frac{z}{a_n}\right) e^{\frac{z}{a_n} + \frac{1}{2}\left(\frac{z}{a_n}\right)^2 + \cdots + \frac{1}{m_n}\left(\frac{z}{a_n}\right)^{m_n}}$$

Proof. See [1], Chapter 5, Section 2.3, Theorem 7. □

Let f be a continuous function on a vertical strip $\operatorname{Re} s \in [\sigma_1, \sigma_2]$ which is holomorphic on the interior. The f is said to be a function of **finite order** if there exists $\lambda > 0$ such that $|f(s)| \ll \exp(|s|^\lambda)$ for $|s| \to \infty$ in the strip. The following theorem, due to Phragmen and Lindelöf, provides estimates for functions of finite order in complex vertical stripes.

Theorem 5 (Phragmen-Lindelöf)**.** *Let f be a function of finite order in a strip $\operatorname{Re} s \in [\sigma_1, \sigma_2]$. Suppose that there exists $M \in \mathbb{N}$ such that $f(\sigma_1 + it) \ll |t|^M$ and $f(\sigma_2 + it) \ll |t|^M$ for $|t| \to +\infty$. Then $f(s) \ll |s|^M$ for $|s| \to +\infty$ and s in the strip.*

Proof. See [39], Chapter XII, Section 6. □

We conclude this section by briefly recalling the definition and some properties of the **Gamma function** $\Gamma(s)$. It is the unique meromorphic function defined by

$$\frac{1}{\Gamma(s)} := s e^{\gamma s} \prod_{n=1}^{\infty} \left(1 + \frac{z}{n}\right) e^{\frac{z}{n}}$$

where $\gamma := \lim_{n \to +\infty} \left(\log n - \sum_{k=1}^{n} \frac{1}{k}\right)$i is the Euler-Mascheroni constant.
The function $\Gamma(s)$ has thus simple poles in the non-positive integers.
When s is a positive real number, the Gamma function can be expressed as

$$\Gamma(s) = \int_0^{+\infty} e^{-x} x^s \frac{\mathrm{d}x}{x}.$$

The logarithmic derivative Γ'/Γ is called **Digamma function**; it is denoted with $\Psi(s)$ and it has the expression

$$\Psi(s) = -\gamma - \frac{1}{s} - \sum_{n=1}^{+\infty} \left(\frac{1}{n+s} - \frac{1}{n}\right). \tag{5}$$

Finally, we give the statement of a version of Stirling's Formula, which is the key tool for estimating the Gamma function over values with large imaginary part.

Proposition 1 (Stirling)**.** *Let $s = a + ib$ with $a_1 \leq a \leq a_2$ and $|b| > 1$. Then*

$$|\Gamma(a+ib)| = \sqrt{2\pi} |b|^{a-\frac{1}{2}} e^{-\pi \frac{|b|}{2}} \left[1 + O_{a_1,a_2}\left(\frac{1}{|b|}\right)\right]. \tag{6}$$

Proof. See [2], Section 1.4. □

0.3.2 Dedekind Zeta functions

References for this section can be found in [38], Chapter XIII.
Let K be a number field. The **Dedekind Zeta function of** K is defined as the series:

$$\zeta_K(s) := \sum_{\mathfrak{I} \subset \mathcal{O}_K} \frac{1}{\mathrm{N}(\mathfrak{I})^s},$$

where $\mathfrak{I}$ runs among the non-zero ideals of the ring of integers $\mathcal{O}_K$, $\mathrm{N}(\mathfrak{I})$ is the absolute norm of $\mathfrak{I}$ and s is any complex number with $\mathrm{Re}\, s > 1$.
If $K = \mathbb{Q}$, then the Dedekind Zeta function ζ_K is the classical Riemann Zeta function.
Dedekind Zeta functions satisfy the following properties:

- For every $s = \sigma + it \in \mathbb{C}$ with $\mathrm{Re}\, s = \sigma > 1$, the series defining $\zeta_K(s)$ converges absolutely. Thus, $\zeta_K(s)$ is an holomorphic function on the half-plane $\mathrm{Re}\, s > 1$.

- On the same half-plane, the Dedekind Zeta function can be rearranged as an infinite product. In fact

$$\zeta_K(s) = \prod_{\mathfrak{p} \in \mathcal{P}_K} \frac{1}{(1 - \mathrm{N}(\mathfrak{p})^{-s})}, \tag{7}$$

  where $\mathfrak{p}$ ranges over the non-zero prime ideals of $\mathcal{O}_K$. This expression is called the **Euler product of** $\zeta_K(s)$.

- Let (r_1, r_2) denote the signature of K, and define the function

$$\Lambda_K(s) := |d_K|^{s/2} \left(\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\right)^{r_1} ((2\pi)^{-s}\Gamma(s))^{r_2}\zeta_K(s). \tag{8}$$

  Then $\Lambda_K(s)$ has an analytic continuation as a meromorphic function on $\mathbb{C}$, with poles uniquely at 0 and 1, which are simple. From this fact it follows that $\zeta_K(s)$ admits a meromorphic continuation over $\mathbb{C}$ with a unique pole, which is simple, localized at $s = 1$.

- The function $\Lambda_K(s)$ satisfies a functional equation

$$\Lambda_K(1 - s) = \Lambda_K(s).$$

- The residue of $\zeta_K(s)$ in $s = 1$ is equal to

$$\frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\omega_K |d_K|^{1/2}}, \tag{9}$$

  where (r_1, r_2) is the signature of K; h_K, R_K and d_K are respectively the order of the class group of K, the regulator of K and the discriminant of K; ω_K is the number of roots of unity contained in K.

- The Euler product (7) shows that $\zeta_K(s)$ has no zeros for $\operatorname{Re} s > 1$. One can prove that there are no zeros also with real part equal to 1. The functional equation of $\Lambda_K(s)$ implies that if a zero of $\zeta_K(s)$ has $\operatorname{Re} s \leq 0$, then it must be located in the non-positive integers (which are necessarily even for totally real fields).
  The zeros of this form are called **trivial zeros of** ζ_K.

- There exist infinitely many zeros ρ of $\zeta_K(s)$ such that $0 < \operatorname{Re} \rho < 1$: they are called **non trivial zeros of** ζ_K. If ρ is a non trivial zero, then $\bar{\rho}, 1-\rho$ and $1-\bar{\rho}$ are non trivial zeros too.
  The **Generalized Riemann Hypothesis** (GRH) conjectures that any non trivial zero of any Dedekind Zeta function $\zeta_K(s)$ has real part equal to $1/2$.

0.4 Elliptic curves

0.4.1 Recalls from Algebraic Geometry

References for this section can be found in Hartshorne's classic book [28]: we refer to it for the concepts of algebraic varieties and projective algebraic varieties over fixed fields, which we are not going to recall. We also assume the knowledge of Zariski topology and we assume that any algebraic variety is endowed with the Zariski topology.

Let K be a field and X an algebraic variety defined over K. A function $f : X \to K$ is called **regular at** $P \in X$ if there exist an open neighborhood U containing P and two polynomials $g, h \in K[x_1, \ldots, x_n]$ such that h is nowhere 0 on U and $f = g/h$ over U. A function is **regular on** X if it is regular at every $P \in X$.
Given two algebraic varieties X and Y over K, a **morphism** $f : X \to Y$ is a continuous map such that, for any open set $V \subset Y$ and for any regular function $g : V \to K$, the function $g \circ f : f^{-1}(V) \to K$ is regular.
A **rational map** $\phi : X \to Y$ is a map between algebraic varieties such that there exists a non empty open set $U \subset X$ such that $\phi_{|U} : U \to Y$ is a morphism. The rational map is said to be **dominant** if the image of U is Zariski dense in Y.
A dominant rational map $\phi : X \to Y$ is said to be **birational** if there exists a dominant rational map $\Psi : Y \to X$ such that $\Psi \circ \phi = id_X$ and $\phi \circ \Psi = id_Y$. In this case X are Y are said to be **birationally equivalent over** K.

0.4.2 Elliptic curves, Weierstrass Equations

References for this section can be found in Silverman's book [68].

Let K be a field and let $\bar{K}$ be its algebraic closure. An **elliptic curve** E **over** K is the non-singular algebraic variety described by the solutions $(x, y) \in \bar{K}^2$ of the equation

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_j \in K \text{ for every } j \in \{1, 2, 3, 4, 6\}. \tag{10}$$

The equation (10) is called **Weierstrass Equation of the elliptic curve** E/K: its coefficients must be chosen so that the two variable polynomial $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ has partial derivatives with no common zeros, in order to guarantee that the curve E/K is non-singular.
Assume now that $\operatorname{char} K \neq 2$: then, up to a change of variables, an elliptic curve E/K can be described as the set of solutions of a simplified Weierstrass equation:

$$E/K : y^2 = x^3 + a_2x^2 + a_4x + a_6, \qquad a_j \in K \text{ for every } j \in \{2, 4, 6\} \tag{11}$$

where the cubic polynomial in x has no multiple roots in order to guarantee that the curve is non-singular.
Moreover, if $\operatorname{char} K$ is also different from 3, then there is a simpler formulation for the Weierstrass Equation given by

$$E/K : y^2 = x^3 + px + q \tag{12}$$

where $p, q \in K$ and the trinomial $x^3 + px + q$ does not have multiple roots in $\bar{K}$.

Although the equation is presented in an affine form, the best way to work with elliptic curves is to study them in the projective plane $\mathbb{P}^2_K$: in this context, E is a non-singular compact curve. Define $E(K)$ as the set of K**-rational points of** E, i.e. the set of solutions of the homogenized version of Equation (12) with all coordinates in K.
For any elliptic curve E/K, there is a specified point $O \in E(K)$ and a group operation on $E(K)$ such that O is the identity element for this operation.

Let K now be a field of characteristic zero, and assume it is the fraction field of a subdomain R. Let E/K be an elliptic curve described by a Weierstrass Equation (11) with coefficients in K. Then, up to a proper change of variables, it is possible to describe E/K as the set of solutions of a Weierstrass equation $y^2 = x^3 + ax + b$ where the coefficients a and b belong to the subdomain R.
As an example, any elliptic curve over $\mathbb{Q}$ can be described by a Weierstrass equation with coefficients in $\mathbb{Z}$, and any elliptic curve over the function field $\mathbb{Q}(t)$ admits a Weierstrass equation with coefficients in the polynomial ring $\mathbb{Z}[t]$.

0.4.3 Discriminant, elliptic curves over finite fields

Let K be a field with $\operatorname{char} K \neq 2, 3$ and let E/K be an elliptic curve with Weierstras equation $y^2 = x^3 + px + q$, with $p, q \in K$.
The **discriminant of** E is the number

$$\Delta_E := -16(4p^3 + 27q^2).$$

The discriminant of an elliptic curve is always different from 0, because of the hypothesis of non singularity of the curve: in fact, up to the factor 16 which is useful for other reasons, Δ_E is nothing but the polynomial discriminant of the trinomial $x^3 + px + q$. The

discriminant of an elliptic curve E over K is independent of the choice of the Weierstrass equation defining E, provided the curve given by this new Weierstrass equation is K-isomorphic to E/K.

Let F be a finite field of characteristic ≥ 5. By means of a non-singular Weierstrass equations, one can define an elliptic curve over E/F and the set $E(F)$ of F-rational points is a finite group.
Consider now an elliptic curve $E/\mathbb{Q}$, and take a prime number p: if one reduces the coefficients of the Weierstrass equation mod p, a Weierstrass equation with coefficients in $\mathbb{F}_p$ is obtained. The curve $E_p/\mathbb{F}_p$ is an elliptic curve over $\mathbb{F}_p$ if and only if the rational discriminant Δ_E of $E/\mathbb{Q}$ is not 0 mod p: thus, for almost any prime p, the reduced curve E_p is again an elliptic curve.
Define finally the numbers:

$$a_E(p) := \begin{cases} 0 & \text{if } p|\Delta_E \\ p + 1 - \#E_p(\mathbb{F}_p) & \text{otherwise.} \end{cases} \tag{13}$$

There is a geometric interpretation of these numbers, as the trace of the Frobenius morphism of E_p (see [68], Chapter 5).

Remark 4. The discriminant of an elliptic curve E/K can be defined also if the characteristic of K is equal to 2 or 3: the definition requires the general form (10) of the Weierstrass equation of an elliptic curve, and is more complicated than the one given above. However, it gives the same value for the discriminants whenever char K is neither 2 and 3.

0.4.4 Mordell-Weil theorems, rank of elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve. Consider the group $E(\mathbb{Q})$ of rational points. The following theorem, which is exhaustively proved in [68], Chapter VIII, provides a very important result about the structure of this group.

Theorem 6 (Mordell-Weil)**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q})$ is a finitely generated abelian group.*

Being finitely generated, $E(\mathbb{Q})$ is the direct sum of a finite torsion group and a free group with finite rank r. The **rank of the elliptic curve** E is the rank of the free part of $E(\mathbb{Q})$.

There is a useful and broad generalization of Mordell-Weil's Theorem which permits to obtain a similar result (and a similar concept of rank) for every elliptic curve over a wide family of fields.

Theorem 7 (Neròn-Lang)**.** *Let F be either $\mathbb{Q}$ or $\mathbb{F}_p$, with p a prime number. Let K/F be a finitely generated extension of fields. Let E be an elliptic curve over the field K. Then the group of K-rational points $E(K)$ is a finitely generated abelian group, and the rank of its free part is called rank of E over K.*

Proof:
See the paper [40].
□

Among the fields to which Neròn-Lang's Theorem applies there are finite fields and function fields over number fields (remember that a finitely generated extension may not be a finite extension, e.g. $\mathbb{Q}(t)/\mathbb{Q}$).

0.4.5 Elliptic surfaces

In the following chapters we will be interested in working not with single elliptic curves, but with collections of elliptic curves: in this last lines we recall the needed concepts in order to characterize these collections in the most proper geometrical point of view.

Let K be a field, and let C be a non singular, projective curve over K. An **elliptic surface** is given by:

- A surface $\mathcal{E}$, i.e. a projective variety of dimension 2.
- A surjective morphism $\pi : \mathcal{E} \to C$ such that for all but finitely many $t \in C(\bar{K})$ the fiber $\pi^{-1}(t)$ is a non-singular curve of genus 1.
- A section $\sigma_0 : C \to \mathcal{E}$.

An intuitive realization of an elliptic surface is given by a Weierstrass equation (10) where the coefficients a_j belong to a function field $K(t)$, and the equation is suh that substituting t with an element $\alpha \in K$, one obtains almost every time an elliptic curve over K.
Finally, we give a last definition, concerning a specific kind of elliptic surface: an elliptic surface $\mathcal{E}$ is said to be a **rational elliptic surface** if there exists a birational map $\phi : \mathcal{E} \to \mathcal{P}^2_K$.

Part II

Prime densities and applications

Chapter 1

Chebotarev's Theorem: computation of prime densities

1.1 Prime densities

1.1.1 Introduction to prime densities

Let us begin with some preliminary examples. Fix a big enough integer M and consider the set of numbers $\{1, 2, \ldots, M\}$. Let $q \in \mathbb{N}$. If a is a given residue class modulo q, what is the chance of picking a number of the form $a + kq$ in $\{1, 2, \ldots, M\}$? Dividing this set in consecutive sequences of q integers, one immediately sees that the desired probability is very near to $1/q$, and is exactly $1/q$ whenever q divides M.
If one is interested in extending this question to the whole set $\mathbb{N}$ of natural numbers, a simple way to do this would be to consider a limit of the form

$$\lim_{x \to +\infty} \frac{\#\{n \leq x \colon n = a \bmod q\}}{x}. \tag{1.1}$$

The value of this limit, which is called **density of the residue class a mod q in $\mathbb{N}$**, is exactly $1/q$. The result of the limit is independent of the chosen residue class modulo q, and so one can affirm that these classes have the same density in $\mathbb{N}$.

Consider now a very similar question, but related to the prime numbers: what is the number of prime numbers in $\{1, \ldots, M\}$ of the form $4k + 1$ and $4k + 3$ respectively? With the only exception of 2, every prime number is odd and thus admits only 1 and 3 as residue classes modulo 4; but the existence of only two residue classes is not a strong enough reason to conclude that the number of primes $p \equiv 1 \bmod 4$ is almost the same of the number of primes $p \equiv 3 \bmod 4$, or that these two kind of primes have the same density, using the previous terminology.
Nonetheless, a heuristic computation shows that the two quantities are very close as more primes are taken into account, and the proportions of the two classes are both very near

to the "expected value" 1/2 (see Table 1.1 below).

Table 1.1

M	$A :=$ $\#\{p = 4k+1 \leq M\}$	$B :=$ $\#\{p = 4k+3 \leq M\}$	$C :=$ $\#\{p \leq M \text{ odd}\}$	A/C	B/C
10^4	609	619	1228	0.49592833..	0.50407166..
10^5	4783	4808	9591	0.49906365..	0.50093634..
10^6	39175	39322	78497	0.49906365	0.50093634
10^7	332180	332398	664578	0.49983598..	0.50016401..
10^8	2880504	2880950	5761454	0.49996129..	0.50003870..
10^9	25423491	25424042	50847533	0.49999458..	0.50000541..

The more primes are considered, the more the distribution of the two residue classes approaches to 1/2; thus, one would like to introduce a sort of density for prime numbers, similar to the one introduced for natural numbers, which would allow to say that the primes of the form $4k + 1$ and $4k + 3$ have same density in the set of prime numbers.

There is an arithmetical reason for being interested in a concept of density for prime numbers: in fact, it is well known that the factorization of an odd prime number p in the Euclidean ring $\mathbb{Z}[i]$ depends only on its residue class modulo 4, and that the principal ideal $p\mathbb{Z}[i]$ splits as a product of two distinct prime ideals if and only if $p = 4k + 1$, it remains a prime ideal if and only if $p = 4k + 3$, while $2\mathbb{Z}[i]$ ramifies as a square of a prime ideal. Similar yet more complicated behaviours can be noticed in the ring of integers $\mathcal{O}_K$ of a generic number field K, and thus the idea of a density for prime numbers would be relevant in order to detect the proportion of prime numbers with given factorization behaviour in $\mathcal{O}_K$.
Moreover, a completely similar concept could be defined not only for prime numbers but also for prime ideals, whenever one considers a number field extension L/K and wants to detect the proportion of prime ideals with given factorization type as product of prime ideals in the ring $\mathcal{O}_L$. The result could be gained by counting the ideals with respect to their absolute norm, which coincides with the size of the prime in the case of rational prime numbers.

1.1.2 Natural density and Dirichlet density

In this section we recall precise concepts of density which allow to formalize the ideas previously introduced.

Given a number field K, let $\mathcal{P}_K$ be the set of non-zero prime ideals of $\mathcal{O}_K$. Given a

subset $A \subset \mathcal{P}_K$, **the natural density of A in $\mathcal{P}_K$** is the limit (if it exists)

$$\delta_K(A) := \lim_{x \to +\infty} \frac{\#\{\mathfrak{p} \in A \colon \mathrm{N}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in \mathcal{P}_K \colon \mathrm{N}(\mathfrak{p}) \leq x\}}.$$

This definition resembles the computation of densities of residue classes presented in (1.1), and it is called "natural" as it is indeed the naivest way to define a density as the ratio between the number of elements of the subset and the number of elements of the total set.
It is clear from the definition that the whole set $\mathcal{P}_K$ has a natural density which is equal to 1. Moreover, assume that $S \subset A$ is such that $\delta_K(S) = 0$: then $\delta_K(A) = \delta_K(A \setminus S)$, provided $\delta_K(A)$ exists.
The formulation of the natural density can be simplified thanks to the Prime Ideal Theorem (see [11], Chapter IX, Section 2, Theorem 1), which states that the number of prime ideals with norm less than a positive upper bound x is asymptotic to $x/\log x$ as x goes to infinity: the natural density of $A \subset \mathcal{P}_K$ is then equal to

$$\delta_K(A) = \lim_{x \to +\infty} \frac{\#\{\mathfrak{p} \in A \colon \mathrm{N}(\mathfrak{p}) \leq x\}}{x/\log x}.$$

By this new formulation one can see that any finite set $S \subset \mathcal{P}_K$ has natural density equal to 0, and so the natural density of a set of prime ideals does not change by removing a finite number of elements; this fact will be largely exploited in the next sections.

Although being a very natural definition, this instance of density is not always the most practical to deal with: Analytic Number Theory shows that already for natural numbers there are different definitions of densities which cover and include wider cases. One of these new densities arises from the study of the Dedekind Zeta function of a number field K.

Given $A \subset \mathcal{P}_K$, **the Dirichlet density of A in K** is defined as the limit (if it exists)

$$\partial_K(A) := \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in A} \mathrm{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}_K} \mathrm{N}(\mathfrak{p})^{-s}}.$$

The limit is made over real numbers s greater than 1, and the denominator comes from the logarithmic expression of the Dedekind Zeta function of K: in fact, the Euler product formula (7) for $\zeta_K(s)$, combined with the fact that $s = 1$ is a simple pole for $\zeta_K(s)$, provides the following chain of asymptotics when $s \to 1^+$, s real.

$$\log\left(\frac{1}{s-1}\right) \sim \log \zeta_K(s) \sim \sum_{\mathfrak{p} \in \mathcal{P}_K} \sum_{m=1}^{+\infty} \mathrm{N}(\mathfrak{p})^{-ms} \sim \sum_{\mathfrak{p} \in \mathcal{P}_K} \mathrm{N}(\mathfrak{p})^{-s}.$$

Thus, the Dirichlet density can be computed as

$$\partial_K(A) := \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in A} \mathrm{N}(\mathfrak{p})^{-s}}{\log\left(1/(s-1)\right)}.$$

Just like for the natural density, a finite set S has $\partial_K(S) = 0$ and the Dirichlet density of a set of prime ideals A does not change whenever a set with Dirichlet density equal to 0 is removed from A.
Furthermore, there is a very important set of prime ideals in $\mathcal{P}_K$ having Dirichlet density equal to 1 without being the whole set $\mathcal{P}_K$.

Proposition 2. *Let $A \subset \mathcal{P}_K$ be the set of non-zero prime ideals of $\mathcal{O}_K$ which have inertia degree over rational primes equal to 1. Then $\partial_K(A) = 1$.*

Proof. One has

$$\sum_{\mathfrak{p}\in\mathcal{P}_K} \mathrm{N}(\mathfrak{p})^{-s} = \sum_{\substack{\mathfrak{p}\in\mathcal{P}_K \\ \mathrm{N}(\mathfrak{p}) \text{ prime}}} \mathrm{N}(\mathfrak{p})^{-s} + \sum_{\substack{\mathfrak{p}\in\mathcal{P}_K \\ \mathrm{N}(\mathfrak{p}) \text{ power} \geq 2 \text{ of a prime}}} \mathrm{N}(\mathfrak{p})^{-s}. \tag{1.2}$$

The second sum in the right hand side is uniformly bounded by the convergent series $[K : \mathbb{Q}] \sum 1/p^2$ for every $s \geq 1$, where the sum is made over the prime numbers. Thus the Dirichlet density of A is equal to

$$\lim_{s\to 1^+} \frac{\sum_{\substack{\mathfrak{p}\in\mathcal{P}_K \\ \mathrm{N}(\mathfrak{p}) \text{ prime}}} \mathrm{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in\mathcal{P}_K} \mathrm{N}(\mathfrak{p})^{-s}} = \lim_{s\to 1^+} \frac{\sum_{\substack{\mathfrak{p}\in\mathcal{P}_K \\ \mathrm{N}(\mathfrak{p}) \text{ prime}}} \mathrm{N}(\mathfrak{p})^{-s}}{\sum_{\substack{\mathfrak{p}\in\mathcal{P}_K \\ \mathrm{N}(\mathfrak{p}) \text{ prime}}} \mathrm{N}(\mathfrak{p})^{-s} + \sum_{\substack{\mathfrak{p}\in\mathcal{P}_K \\ \mathrm{N}(\mathfrak{p}) \text{ power} \geq 2 \text{ of a prime}}} \mathrm{N}(\mathfrak{p})^{-s}} = 1.$$

□

Remark 5. Although apparently more complicated, Dirichlet densities have proven to be easier to study than natural densities, the reason relying on the analytic behaviour of Dedekind Zeta functions and other similar L-functions (like Hecke L-functions). In fact, the Dirichlet density only requires the study of the behaviour of these functions over the half-line $s > 1$ by looking at their limit for $s \to 1^+$. Natural densities are instead related to the study of sums like $\sum_{\mathrm{N}(\mathfrak{p})\leq x} \mathrm{N}(\mathfrak{p})$, which in the case of Dedekind Zeta functions is needed to establish the Prime Ideal Theorem; it is known that a necessary condition to prove it comes by showing that $\zeta_K(s)$ has no zeros over the line $\mathrm{Re}\, s = 1$, and this result requires an analytic study of $\zeta_K(s)$ over the half-plane $\mathrm{Re}\, s \geq 1$, being thus more complicated than the one needed for Dirichlet density.

As an additional example, consider Dirichlet's theorem on the infinitude of primes in arithmetic progressions $a + kq$; this result is in fact much easier to obtain if one deals with Dirichlet densities, because the formulation of the density reduces the problem to the proof that every L-function associated to a non-trivial character mod q does not vanish at $s = 1$ (see [31], Chapter 2 for more details). From these considerations, one obtains that the Dirichlet density of primes of the form $a + kq$ is equal to $1/\varphi(q)$, where φ is Euler's totient function.
It is indeed harder to get the value of the natural density for primes in arithmetic progression, but in the end this value is again equal to $1/\varphi(q)$ (a proof of this result can be found in Serre's book [66]), Chapter VI.

As the previous remark suggests, it may not be easy to establish a link between the two densities we have introduced. It is actually possible to produce sets of prime numbers which have Dirichlet density but do not admit a natural density: such families do not arise from usual arithmetical problems and are instead trickier collection of primes. An example is given by the set of prime numbers with first decimal digit equal to 1: see [25] for more details.
The following lemma yields a result in the opposite direction, providing a connection between natural density and Dirichlet density.

Lemma 1. *If $A \subset \mathcal{P}_K$ admits a natural density $\delta_K(A)$, then it also admits a Dirichlet density $\partial_K(A)$ and $\partial_K(A) = \delta_K(A)$.*

Proof. See [73], Section III.1.2, Theorem 2. □

As we have just seen, the worlds described by natural and Dirichlet density may not overlap. Nonetheless, we will see in the next sections that for every family of prime ideals arising naturally from arithmetical factorization in number fields, the two concepts not only exist at the same time but they also coincide, simplifying thus the description of the densities.

1.2 Chebotarev's Theorem

1.2.1 Splitting types and Artin symbols

Let us begin by recalling a Lemma of Algebraic Number Theory which links the splitting type of a prime ideal $\mathfrak{p}$ in an extension of number fields to the factorization modulo $\mathfrak{p}$ of the defining polynomial of the extension.

Lemma 2. *Let K/F be a finite number field extension, with $K = F(\alpha)$ where α is an algebraic integer and $g(x) \in F[x]$ is the minimum polynomial of α. Assume that $\mathfrak{p} \in \mathcal{P}_F$ is unramified in K and that the characteristic of the finite field $\mathcal{O}_F/\mathfrak{p}$ does not divide the index $[\mathcal{O}_K : \mathcal{O}_F[\alpha]]$.*
Then $f_K(\mathfrak{p}) = (f_1, \dots, f_r)$ if and only if $g(x) \equiv g_1(x) \cdots g_r(x) \mod \mathfrak{p}$, where $g_1(x), \dots, g_r(x)$ are irreducible polynomials modulo $\mathfrak{p}$ of degree $f_1, \dots, f_r$ respectively.

Proof. See [33], Chapter 5, Proposition 5.42. □

Remark 6. The set of primes $\mathfrak{p}$ not satisfying the hypothesis of Theorem 2 is finite: thus, whenever one is interested in problems regarding natural and Dirichlet densities, it can be assumed that any prime has the splitting type given by the reduction of the defining polynomial of the field.

Assume now that K/F is a finite Galois number field extension, with Galois group G. Let $\mathfrak{p} \in \mathcal{P}_F$ unramified which satisfies the hypothesis of Lemma 2. Let $\mathfrak{p}\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ be its factorization as a product of prime ideals in $\mathcal{O}_K$; then the Galois Group G acts

transitively on the set $\{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$.
The stabilizer group $D(\mathfrak{q}_i) := \{\sigma \in G \colon \sigma(\mathfrak{q}_i) = \mathfrak{q}_i\}$ is called **the decomposition group of $\mathfrak{q}_i$ over $\mathfrak{p}$**. The transitivity of the action implies that the decomposition groups over $\mathfrak{p}$ are G-conjugated.
Consider the finite fields $\mathcal{O}_K/\mathfrak{q}_i$ and $\mathcal{O}_F/\mathfrak{p}$: the extension $(\mathcal{O}_K/\mathfrak{q}_i)/(\mathcal{O}_F/\mathfrak{p})$ is finite and Galois, with cyclic Galois group generated by the Frobenius automorphism $\phi : x \to x^p$, where p is the characteristic of these fields.
For every $i = 1, \dots, r$ there is then a group isomorphism

$$\Psi_i : D(\mathfrak{q}_i) \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{q}_i)/(\mathcal{O}_F/\mathfrak{p}))$$

which is induced by the natural projection morphism $G \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{q}_i)/(\mathcal{O}_F/\mathfrak{p}))$ (for a proof of this isomorphism, see [32], Chapter III, Section 1).
Finally, the sets $\Psi_i^{-1}(\phi)$ form a conjugation class in G: the **Artin symbol of $\mathfrak{p}$ in K/F** is defined then as

$$\left[\frac{K/F}{\mathfrak{p}}\right] := \{\Psi_i^{-1}(\phi) \colon i = 1, \dots, r\}.$$

Remark 7. If K/F is Galois, the transitivity of the action of G forces the splitting type $f_K(\mathfrak{p})$ to be of the form $(f, \dots, f)$, where f divides $[K : F]$. Thus, if K/F has $g(x)$ as defining polynomial, the Artin symbol of an unramified prime $\mathfrak{p}$ is formed by elements of order f only if $g(x)$ factorizes modulo $\mathfrak{p}$ as a product of irreducible polynomials of degree f.

Remark 8. In an abelian Galois group, any Artin symbol is formed by a single element.

1.2.2 Statement of Chebotarev's Theorem

The definition and properties of Artin symbols naturally lead to the following question: given a finite Galois number field extension K/F with Galois group G, does any conjugation class of G occur as an Artin symbol for some unramified prime $\mathfrak{p} \in \mathcal{P}_F$?
The answer to this question is not only affirmative but it also carries precise knowledge about the densities of the primes with prescribed Artin symbol.

Theorem 8 (Chebotarev)**.** *Let K/F be a finite Galois extension with group G, and let $\mathcal{C} \subset G$ be a conjugation class. Then there exist infinitely many unramified prime ideals $\mathfrak{p} \in \mathcal{P}_F$ such that $\mathcal{C} = \left[\frac{K/F}{\mathfrak{p}}\right]$: moreover, these primes form a set $A_{\mathcal{C}}$ which admits both natural and Dirichlet density in $\mathcal{P}_F$, and*

$$\delta_K(A_{\mathcal{C}}) = \partial_K(A_{\mathcal{C}}) = \frac{\#\mathcal{C}}{\#G}.$$

Proof. The original proof is in Chebotarev's original paper [76], and it relies on the properties of Dedekind Zeta functions and other kinds of L-functions, like the Dirichlet L-functions associated to cyclotomic fields. A modern exposition of the proof can be found in [71], and a proof with a different procedure can be found in Neukirch's book [51], Chapter VII, Section 13, Theorem 13.4. □

Remark 9. Dealing with the primes associated to Artin symbols, we will use the term "density" referred to either the natural density or Dirichlet density, which now we know to coincide for these sets of primes.

The link between splitting types and Artin symbols gives a strong practical criterion for the computation of densities: if for a finite Galois extension one is interested in computing the density of the primes with splitting type $(f, \dots, f)$, then Chebotarev's Theorem guarantees that this density exists and is easily determined once one has found the correct conjugation class formed by elements of order f in the Galois Group.
A straightforward Corollary, which actually was proved earlier by Kronecker, provides the density of primes which split completely in a finite Galois extension.

Corollary 1 (Kronecker)**.** *Let L/F be a finite Galois extension of number fields. Then, the set of primes which split completely in L has prime density equal to $1/[L : F]$.*

As an application of Chebotarev's Theorem, let us go back to the introductory problem of the primes of the form $4k + 1$ and $4k + 3$. Consider the quadratic extension $\mathbb{Q}[i]/\mathbb{Q}$, which has Galois group C_2 (the base field $\mathbb{Q}$ is associated to the identity subgroup). Given an odd prime number p, we have that p is equal to 1 modulo 4 if and only if the defining polynomial $x^2 + 1$ splits modulo p, and by Lemma 2 this happens if and only if p splits completely in $\mathbb{Z}[i]$. By Chebotarev, this is equivalent to say that the primes $p \equiv 1 \mod 4$ have the identity element of C_2 as Artin symbol, while the primes $q \equiv 3 \mod 4$ have the non trivial element of C_2 as Artin symbol: hence the two classes of primes have same density equal to $1/2$ in $\mathcal{P}_{\mathbb{Q}}$.
Similarly, the equi-distribution of primes in arithmetic progressions modulo $\mathfrak{q}$ can be recovered by applying Chebotarev's Theorem to the cyclotomic field $\mathbb{Q}(\zeta_q)$, which is a Galois extension of $\mathbb{Q}$ with cyclic Galois group of size $\varphi(q)$: in fact, the primes with residue class a mod q, with a coprime to q, admit a itself as Artin symbol in the group.

Remark 10. Chebotarev's theorem and the density results related hold also whenever one discards a set of primes with natural and Dirichlet density equal to 0, like finite sets.

1.2.3 Densities for generic number field extensions

Let us consider now a finite number field extension K/F and its Galois closure $\widehat{K}/F$ with Galois group G. Chebotarev's Theorem would apply only to the bigger extension, which is Galois; is there a way to use it in order to get the densities of the primes with a given splitting type in the intermediate field K?
The following Proposition gives an answer to this question.

Proposition 3. *Let K/F be a finite number field extension, with Galois closure $\widehat{K}/F$ having Galois Group G. Let $H := \mathrm{Gal}(\widehat{K}/K) \subset G$ be the subgroup associated to K, and let $\{H, \sigma_1 H, \dots, \sigma_l H\}$ be the left cosets of H in G.*
Let $\mathfrak{p} \in \mathcal{P}_F$ be an unramified prime in $\widehat{K}$ (and so also in K), and let $\sigma \in G$ be an element

of $\left[\frac{\widehat{K}/F}{\mathfrak{p}}\right]$. *Consider the action of the cyclic group* $\langle\sigma\rangle$ *on the set* $\{H, \sigma_1 H, \dots, \sigma_l H\}$ *given by left multiplication.*
Then there is a bijection

$$\{\mathfrak{q} \in \mathcal{P}_K \colon \mathfrak{q} \cap \mathcal{O}_F = \mathfrak{p}\} \leftrightarrow \{\textit{orbits of the above action}\}$$

and if $f_K(\mathfrak{p}) = (f_1, \dots, f_r)$, *then the orbits have size* $f_1, \dots, f_r$ *respectively.*

Proof. See [32], Chapter III, Prop.2.8. □

Proposition 3 yields a method to compute densities for generic number field extensions:

- First of all, one looks at the Galois group G of the closure $\widehat{K}/F$ and finds the subgroup H corresponding to K. Then, one writes the left cosets of H.
- For every conjugation class $\mathcal{C} \subset G$, one chooses an element $\sigma \in \mathcal{C}$ and studies the action of $\langle\sigma\rangle$ on the left cosets of H.
- Let $(f_1, \dots, f_r)$ be an orbit for the previous action, and assume it is given by the action of elements in the conjugacy classes $\mathcal{C}_1, \dots, \mathcal{C}_s$. Then Chebotarev's Theorem and Proposition 3 imply that there exist infinitely many primes $\mathfrak{p} \in \mathcal{P}_F$ with splitting type $f_K(\mathfrak{p}) = (f_1, \dots, f_r)$, and they form a set with density equal to $\sum_{i=1}^{s} (\#\mathcal{C}_i/\#G)$ in $\mathcal{P}_F$.

We conclude this part by recalling some well known lemmas from Algebraic Number Theory which will be etensively used in later sections.

Lemma 3. *Let* K/F *and* L/F *be number fields extensions, and let* KL/F *be their composite extension, which is the smallest extension containing both* K *and* L. *Then* $\mathfrak{p} \in \mathcal{P}_F$ *splits completely in* KL *if and only if it splits completely in both* K *and* L.

Proof. See [51], Chapter I, Section 8.3. □

Corollary 2. *Given* K/F *and its Galois closure* $\widehat{K}/F$, *a prime ideal* $\mathfrak{p} \in \mathcal{P}_F$ *splits completely in* K *if and only if it splits completely in* $\widehat{K}$.

Proof. We know that $\widehat{K}$ is the compositum field of all the fields $\sigma(K)$ where $\sigma \in \mathrm{Gal}(L\widehat{K}/F)$; but if a prime splits completely in K, it must be totally slit in $\sigma(K)$ as well. The claim follows then from Lemma 3. □

Corollary 3. *Let* K/F *and* L/F *be two Galois extensions, and assume that a prime* $\mathfrak{p} \in \mathcal{P}_F$ *splits completely in* K *if and only if it splits completely in* L. *Then* $K = L$.

Proof. Let KL/F be the composite extension, which is Galois. By Lemma 3 it follows, up to exceptions of null prime density,

$$\{\mathfrak{p} \in \mathcal{P}_F \colon f_{KL}(\mathfrak{p}) = (1, \dots, 1)\} = \{\mathfrak{p} \in \mathcal{P}_F \colon f_K(\mathfrak{p}) = (1, \dots, 1) \text{ and } f_L(\mathfrak{p}) = (1, \dots, 1)\}.$$

Applying Chebotarev's Theorem, the identity above gives the equality

$$\frac{1}{[K:F]} = \frac{1}{[KL:F]} = \frac{1}{[L:F]}$$

which immediately implies $K = KL = L$. □

We will use these tools in order to list all the possible splitting types in number fields extensions of degree less or equal than 5.

1.3 Densities for low degree extensions

We now gather all the possible splitting types for all number fields extensions K/F with $[K:F] \leq 5$ and Galois closure $\widehat{K}/F$. The Galois group of $\widehat{K}/F$ will be denoted with G, while the subgroup corresponding to K will be called H.
Computations are not presented but they all rely on Proposition 3: every possible choice for the Galois group G is presented in the online datebase [37] and arises from the study of the transitive subgroups of S_n for $n \leq 5$. The properties of each group are reported in the correspondent pages of the wiki Groupprops [77].

1.3.1 Quadratic fields

If $[K:F] = 2$, then the extension is Galois with cyclic group C_2. The following table presents the possible splitting types and the densities of the primes with specified slitting type.

splitting type	(1,1)	(2)
density	1/2	1/2

1.3.2 Cubic fields

If $[K:F] = 3$, we have 2 possible choices for G:

- $G = C_3$, the cyclic group of order 3. Then K/F is Galois, and

splitting type	(1,1,1)	(3)
density	1/3	2/3

- $G = S_3$, the symmetric permutation group over 3 elements. Then H can be chosen among any subgroup of order 2, being them all conjugated, and so:

splitting types	(1,1,1)	(1,2)	(3)
densities	1/6	1/2	1/3

1.3.3 Quartic fields

If $[K : F] = 4$, there are 5 possible choices for G:

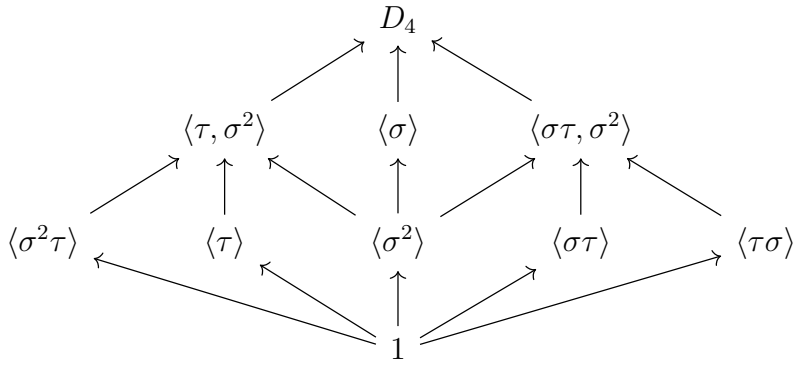
- $G = C_4$, the cyclic group of order 4. Then K/F is Galois, and we have the following splitting types and densities:

splitting types	(1,1,1,1)	(2,2)	(4)
densities	1/4	1/4	1/2

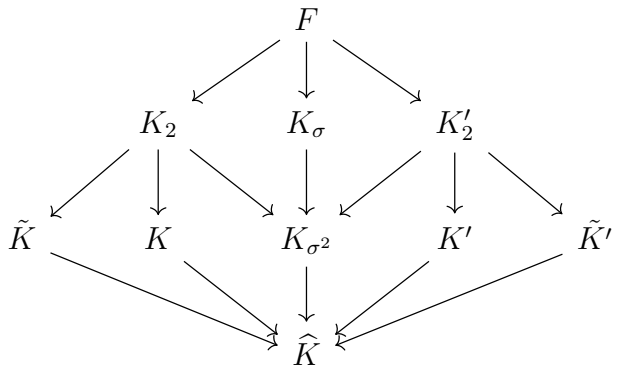
- $G = C_2 \times C_2$: then K/F is Galois, and we have:

splitting types	(1,1,1,1)	(2,2)
densities	1/4	3/4

- $G = D_4 := \langle \sigma, \tau | \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$: then $[\widehat{K} : F] = 8$. Let us recall the lattice of subgroups of D_4, and the corresponding lattice of sub-extensions of $\widehat{K}/F$:



(1.3)



(1.4)

One can assume that $H = \langle \tau \rangle$: then K is F-isomorphic to $\tilde{K}$, which is associated to $\langle \sigma^2\tau \rangle$, but not to K' and $\tilde{K}'$, associated to $\langle \sigma\tau \rangle$ and $\langle \tau\sigma \rangle$ respectively. The quartic extension K_{σ^2}/F is Galois and it is associated to $\langle \sigma^2 \rangle$.
With this choice for H, we get the following splitting types:

splitting types	(1,1,1,1)	(1,1,2)	(2,2)	(4)
densities	1/8	1/4	3/8	1/4

It is important to notice that, with our assumption on H, the primes with splitting type $(1,1,2)$ have Artin symbol equal to $\{\tau, \sigma^2\tau\}$, while the primes with splitting type $(2,2)$ divide into two kinds: the ones with Artin symbol $\{\sigma\tau, \tau\sigma\}$, having density $1/4$, and the ones with Artin symbol equal to $\{\sigma^2\}$, with density $1/8$.

Remark 11. If one assumes $H = \langle\sigma\tau\rangle$, and so considers K' instead of K, the roles of $\{\tau, \sigma^2\tau\}$ and $\{\sigma\tau, \tau\sigma\}$ as Artin symbols simply reverse, and all the remaining splitting types and densities are as before. Thus, one can always assume that $H = \langle\tau\rangle$.

- $G = A_4$, the alternating group over 4 elements: then $[\widehat{K} : F] = 12$ and H can be chosen among any subgroup of order 3, being them all conjugated. Thus we have the following splitting types and densities:

splitting types	(1,1,1,1)	(1,3)	(2,2)
densities	1/12	2/3	1/4

- $G = S_4$, the symmetric group over 4 elements: then $[\widehat{K} : F] = 24$ and H can be chosen among any subgroup of order 6, all of them being conjugated and isomorphic to S_3. Therefore:

splitting types	(1,1,1,1)	(1,1,2)	(1,3)	(2,2)	(4)
densities	1/24	1/4	1/3	1/8	1/4

1.3.4 Quintic fields

If $[K : F] = 5$, we have five possible choices for G.

- $G = C_5$, the cyclic group of order 5: then K/F is Galois, and so

splitting type	(1,1,1,1,1)	(5)
density	1/5	4/5

- $G = D_5 := \langle\sigma, \tau | \sigma^5 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1}\rangle$. Then $[\widehat{K} : F] = 10$, and H can be chosen among any subgroup of order 2, being them all conjugated. The splitting types and densities are:

splitting types	(1,1,1,1,1)	(1,2,2)	(5)
densities	1/10	1/2	2/5

- $G = F_5 := \langle\sigma, \mu | \sigma^4 = \mu^5 = 1, \mu\sigma = \sigma\mu^2\rangle$. Then $[\widehat{K} : F] = 20$, and H can be chosen among any subgroup of order 4, which are conjugated between them. Thus:

splitting types	(1,1,1,1,1)	(1,1,1,2)	(1,4)	(5)
densities	1/20	1/4	1/2	1/5

- $G = A_5$, the alternating group over 5 elements. Then $[\widehat{K} : F] = 60$ and H can be chosen among any subgroup of order 12, which are conjugated between them and isomorphic to A_4. We have:

splitting types	(1,1,1,1,1)	(1,2,2)	(1,1,3)	(5)
densities	1/60	1/4	1/3	2/5

- $G = S_5$, the symmetric permutation group over 5 elements. Then $[\widehat{K} : F] = 120$ and H can be chosen among any subgroup of order 24: these are isomorphic to S_4 and conjugated between them.

splitting types	(1,1,1,1,1)	(1,1,1,2)	(1,2,2)	(1,1,3)	(2,3)	(1,4)	(5)
densities	1/120	1/12	1/8	1/6	1/6	1/4	1/5

Remark 12. Let K/F be a quintic extension with $G = A_5$, and consider any non-trivial subextension E/F: then K and E share the same totally split primes by Corollary 2. In other words, K is uniquely characterized by any of its non-trivial subextensions over F. A similar result holds for quintic extensions with $G = S_5$: these extensions are uniquely characterized by any of their subextensions which are neither F nor the unique quadratic subextension of K.
These facts will be crucial for the final proofs of Chapter 2.

Chapter 2

Local GCD equivalence

2.1 Recalls on arithmetic equivalence

2.1.1 Number fields characterized by the splitting types

Given two isomorphic number fields K and L, it is clear that the equality of splitting types $f_K(p) = f_L(p)$ holds for every prime number p. Because of the importance the arithmetical factorization of prime numbers assumes in rings of integers, one could wonder if knowing the splitting type of any prime number is enough to recover the isomorphism class of a number field; it could be also possible to reduce to work with the unramified primes, being the ramified primes a finite set. Furthermore, a completely similar question could be extended to any number field extension over a fixed base field F: is the list of splitting types of unramified prime ideals $\mathfrak{p} \subset \mathcal{O}_F$ enough to recover an F-isomorphism class of extensions K/F?

We recall the notation introduced before: given two extensions of number fields K/F and L/F, the set $\mathcal{P}_F$ contains the prime ideals in $\mathcal{O}_F$ which are unramified in both L and K.
Two number fields K and L are said to be **arithmetically equivalent** when $f_K(p) = f_L(p)$ for every prime number $p \in \mathcal{P}_{\mathbb{Q}}$. This is an equivalence relation, and it is natural to ask whether this relation reduces to isomorphism or is somehow weaker, and which invariants of the fields remain the same in an arithmetic equivalence class.
The definition for extensions over generic base number fields F is straightforward: given two extensions K/F and L/F, K and L are said to be **F-arithmetically equivalent** if $f_K(\mathfrak{p}) = f_L(\mathfrak{p})$ for every prime ideal $\mathfrak{p} \in \mathcal{P}_F$. The previous notion of arithmetic equivalence is nothing but F-arithmetic equivalence with $F = \mathbb{Q}$: notice that the dependence on F is crucial, and in fact we will see examples of $\mathbb{Q}$-arithmetic equivalent fields which are not equivalent over a bigger field F.

2.1.2 Properties of arithmetically equivalent number fields

In order to study and characterize a relation like arithmetic equivalence, one needs to detect some invariants which have the same values and behaviour in both the fields subjected to the relation. The following lines provide some examples.

Proposition 4. *Let K and L be arithmetically equivalent fields. Then $\zeta_K(s) = \zeta_L(s)$.*

Proof. Assume $s > 1$ so that both $\zeta_K(s)$ and $\zeta_L(s)$ are given as Euler product. The definition of arithmetical equivalence implies that all non ramified primes factorize in the same way, so that

$$\frac{\zeta_K(s)}{\zeta_L(s)} = \frac{\prod_{\substack{\mathfrak{p}|p \\ p|d_L}} (1 - \mathrm{N}(\mathfrak{p})^{-s})}{\prod_{\substack{\mathfrak{q}|p \\ p|d_K}} (1 - \mathrm{N}(\mathfrak{q})^{-s})} \tag{2.1}$$

where the factors in right hand side of Equation (2.1) are in finite number. The properties of Dedekind Zeta functions imply that this quotient can be extended to a meromorphic function over $\mathbb{C}$, but for the same reason we know that the points of the form $2\pi i \log \mathrm{N}(\mathfrak{q})$ and $2\pi i \log \mathrm{N}(\mathfrak{p})$ cannot be zeros or poles of $\zeta_K(s)$ and $\zeta_L(s)$. Thus, for every prime $\mathfrak{p}$ appearing in the numerator, there exists a prime $\mathfrak{q}$ appearing in the denominator such that $\mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{q})$ and viceversa, and this fact yields that the quotient is equal to 1. □

Thus, arithmetically equivalent fields share the same Dedekind Zeta function, and just from its analytic properties one can get the following rigidity results:

- If K and L are arithmetically equivalent, then they have the same number r_2 of complex embeddings: this follows from the equal multeplicity of the odd trivial zeros.

- From the point above, K and L have also the same number r_1 of real embeddings and so they have the same degree.

- K and L have the same discriminant d_K and thus the same set of ramified primes. This can be recovered using a procedure similar to the one of Proposition 4, but there is also another way: if $N_{\zeta_K}(T)$ is the number (counting multiplicity) of non-trivial zeros of $\zeta_K(s)$ in the critical strip $0 < \mathrm{Re}\, s < 1$, then

$$N_{\zeta_K}(T) = [K : \mathbb{Q}]\Big(\frac{T}{\pi} \log \frac{T}{2\pi e}\Big) + \frac{T}{\pi} \log |d_K| + O(\log T) \qquad \text{as } T \to +\infty.$$

  The proof of this formula is just an adaption of the classical argument used for the Riemann Zeta function, which is presented in [14], Chapter 15. Given this result, the arithmetical equivalence and the equality of the signatures immediately imply the equality of discriminants.

There are other properties satisfied by arithmetic equivalence classes of number fields ([53], Theorem 1), namely:

- If K and L are arithmetically equivalent, then they have the same Galois core (for the definition of Galois core see Section 0.2.3);
- If K and L are arithmetically equivalent, then K and L share the same finite group of roots of unity.

However, differently from the previous results, these properties seem not to be reachable using only analytic properties of Dedekind Zeta functions; they require instead some tools arising from Group and Representation Theory.

2.1.3 Group theoretical setting of arithmetic equivalence

The following proposition, proved in Gassmann's classic paper [26], gives a group-theoretic characterization of arithmetic equivalence which in the end is proved to be the most striking tool.

Proposition 5 (Gassmann)**.** *Let K and L be two number fields. Let N be a Galois number field containing both L and K, and denote $G := \mathrm{Gal}(N/\mathbb{Q}), H_K := \mathrm{Gal}(N/K)$ and $H_L := \mathrm{Gal}(N/L)$. Then K and L are arithmetically equivalent if and only if*

$$\#(H_K \cap C) = \#(H_L \cap C) \qquad \forall C \subset G \text{ conjugacy class.}$$

This formulation not only helped in proving all the aforementioned properties of arithmetical equivalence, but it also allowed Gassmann to provide the first instances of arithmetically equivalent number fields which are not isomorphic, given by two fields of degree 180. We will see later that this number is very far from being the minimal degree for which there exist equivalent, non-isomorphic fields.

Remark 13. The group theoretic formulation via Gassmann equivalence permits to study also F-arithmetic equivalence: in fact, the definition is the same, with the only difference that the Galois groups involved are groups of extensions over F.
Moreover, this setting is the right one for proving that F-arithmetically equivalent fields have same degree over F, same discriminant ideal and same Galois core over F.

We have listed some properties satisfied by arithmetically equivalent extensions. Now, in order to introduce the next sections, we think about a different question: for which families of number fields the arithmetical equivalence is enough to recover the isomorphism class of a field and so reduces to the isomorphism?
In one of the most important papers about this subject, Perlis [53] used the group theoretic setting of arithmetical equivalence to provide an answer.

Theorem 9 (Perlis)**.** *Let K/F and L/F be F-arithmetically equivalent extensions. Then the two extensions are F-isomorphic if at least one of the following is satisfied:*

1) One between K/F and L/F is Galois;

2) $[K : F] = [L : F] \leq 6$.

Remark 14. Notice that Perlis' result 1) does not derive immediately from Corollary 3 on the totally split primes of Galois extensions, because Corollary 3 needs both the extensions to be Galois. Moreover, the upper bound 2) is sharp: Perlis' paper already presents instances of equivalent number fields of degree 7 which are not isomorphic. An additional example is given by the octic fields $\mathbb{Q}(\sqrt[8]{3})$ and $\mathbb{Q}(\sqrt[8]{48})$: not only they are equivalent, non-isomorphic fields, but they also share a quartic sub-field $F := \mathbb{Q}(\sqrt[4]{3})$, so that they are also non equivalent fields over F.

2.2 Introducing local GCD equivalence

2.2.1 Weaker relations between number fields

Once arithmetic equivalence has been understood, one can start to investigate relations between number fields which require less hypotheses to be satisfied. In particular, one is interested in proving what invariants of the number fields are not modified under weaker relations, and for which families of number fields the new relations reduce to isomorphism. A first instance is given by the Kronecker Equivalence: two number fields extensions K/F and L/F are said to be F**-Kronecker equivalent** if any prime $\mathfrak{p} \in \mathcal{P}_F$ satisfies the following condition:

$$1 \in f_K(\mathfrak{p}) \Leftrightarrow 1 \in f_L(\mathfrak{p}),$$

i.e. a prime of the base field is divided by a prime with inertia degree 1 in one extension if and only if the same happens in the other extension.
The name *Kronecker equivalence* was chosen by Jehne, who first studied this relation in detail in [34], in honour to *Kronecker's JugendTraum*, i.e. the research project started by Kronecker in order to characterize number fields the more as possible by their splitting types and by the arithmetic decomposition of the primes of a base field. Any arithmetically equivalent couple of number field extensions is also Kronecker equivalent, but the latter is in fact a weaker relation: as proved by Jehne in [34], there exist infinitely many Kronecker equivalent fields with different degrees, and thus the degree is an invariant which is no longer shared.
Just like arithmetic equivalence, Kronecker equivalence can be stated in a different form by the representation theory of groups, which considers the Galois groups associated to the extensions instead of the fields: this approach is precisely the one followed by Jehne in [34].

Relations which are even weaker can be introduced in this landscape: an instance, which is the one we will focus on for the rest of the chapter, is given by the *Local GCD Equivalence*. Two extensions K/F and L/F are said to be F**-locally GCD equivalent** if for every prime $\mathfrak{p} \in \mathfrak{p}_F$ which is unramified in both K and L then

$$\gcd(f_{1,K}(\mathfrak{p}), \dots, f_{t,K}(\mathfrak{p})) = \gcd(f_{1,L}(\mathfrak{p}), \dots, f_{t',L}(\mathfrak{p})). \tag{2.2}$$

Thus, instead of requiring precise equalities for the splitting types for some subset of prime ideals, one studies number fields which share primes with a much weaker arithmetical similarity.
The name *Local GCD Equivalence* was used by Linowitz, McReynolds and Miller [42], where their main goal was the study of a stronger relation involving isomorphisms of Brauer groups, yielding the Local GCD Equivalence as a corollary relation from which one can gain some information on the fields. However, this relation was already known under a different name: in fact Lochter [43] introduced this equivalence under the name *Weak Kronecker Equivalence*, and studied in detail its properties in his paper. The choice of the name was motivated by the fact that he previously worked on Kronecker's Equivalence and in [44] he found a condition equivalent to Jehne's formulation which, generalized, led naturally to the definition of Weak Kronecker Equivalence; in fact, it follows from the definitions that two F-Kronecker equivalent extensions are also F-weak Kronecker equivalent. Moreover, up to degree 4 these equivalences are the same relation.
Despite its original credits, we will not follow Lochter's notation and instead we will always refer to this relation as Local GCD Equivalence, in order to emphasize the role played by the greatest common divisors of the inertia degrees. Notice that by Definition 2.2 and Corollary 3 one immediately gets the following rigidity result on locally GCD equivalent Galois extensions.

Proposition 6. *Let K/F and L/F be two Galois extensions which are F-locally GCD equivalent. Then $L = K$.*

Proof. In a Galois extension the splitting types are formed by equal elements: thus, the primes $\mathfrak{p} \in \mathcal{P}_F$ with greatest common divisor of the inertia degrees equal to 1 are exactly the totally split primes. Corollary 3 on totally split primes in Galois extensions yields the thesis. □

Just as for stronger equivalences, the setting in which Local GCD Equivalence was studied by Lochter was the Group and Representation theory: in fact, he translated the conditions of Definition 2.2 into statements regarding the Galois groups associated to the number field extensions. This allowed Lochter to recover many results, among which there is the following theorem, which describes a class of fields for which this weak equivalence actually reduces to an isomorphism.

Theorem 10. *Let K/F and L/F be locally GCD equivalent over F and such that $[K : F], [L : F] \leq 5$. Then K and L are F-isomorphic.*

In the next lines we give a precise motivation for our interest in this particular result.

2.2.2 An elementary formulation for fields of low degree

As already known, a quadratic extension K/F of number fields is Galois and thus completely characterized by its totally split primes. Being $(1, 1)$ and (2) the only possible

splitting types for unramified primes in this extension, the previous statement is equivalent to say that a quadratic extension is uniquely determined by its inert primes.
What about the role of inert primes in cubic extensions? In the Galois case it is completely equivalent to the one of totally split primes: being $(1,1,1)$ and (3) the only possible splitting types, a Galois cubic extension has a prescribed set of totally split primes if and only if it has a prescribed set of inert primes. But what can be said for cubic extensions which are not Galois? This time there is a third possible splitting type, equal to $(1,2)$, which seems to complicate the problem.
Assume however that K/F and L/F are non-Galois cubic extension with same inert primes, i.e. $f_K(\mathfrak{p}) = 3$ if and only if $f_L(\mathfrak{p}) = 3$. The remaining splitting types having greatest common divisors of the inertia degrees equal to 1, we have also $\gcd(f_{1,K}(\mathfrak{p}), \dots, f_{t,K}(\mathfrak{p})) = 1$ if and only if $\gcd(f_{1,L}(\mathfrak{p}), \dots, f_{t',L}(\mathfrak{p})) = 1$: this means that K and L are F-locally GCD equivalent and thus isomorphic by Theorem 10.
A completely identical phenomenon happens for quintic fields: being (5) the only splitting type with greatest common divisors of the inertia degrees different from 1, two quintic extensions which share the same inert primes are necessarily F-locally GCD equivalent, and thus isomorphic by Theorem 10. We have thus obtained a statement which really expresses the rigidity of this equivalence in low degrees.

Corollary 4. *A number field extension K/F of degree 2,3 and 5 is uniquely determined by its inert primes.*

The formulation of Corollary 4 is much more elementary, and even quite surprising: in fact, while one knows and expects inert primes to completely characterize quadratic extension, it seems not obvious at all that this kind of primes is strong enough to characterize up to isomorphism also cubic and quintic extensions, even if they are not Galois. Moreover, this formulation suggests that there could be a proof of this fact which relies on concepts different from Lochter's ones: instead of using a purely group-theoretic formulation, this new setting could be recovered by means of some density results about the primes, thanks to applications of Chebotarev's Theorem.

The next sections will prove the validity of this different assumption: in fact, it will be presented a different proof of Theorem 10 (and thus of Corollary 4) which starts from considerations on the densities of the primes subjected to the Local GCD Equivalence and from these we recover the desired isomorphisms, thanks to the elementary characterizations of the Galois groups for number fields extensions K/F with $[K : F] \leq 5$ described in Chapter 1.
The proofs will have no main differences between them, and to underline the few different approaches we used the following symbols:

- $*$: this symbol denotes the first approach, which consists in reducing the study of two equivalent extensions K/F and L/F at looking for an equivalence of some **Galois companions** of K and L, i.e. some Galois extensions over F which are naturally related to the original fields and have small degree (e.g: if K/F has degree 3 and

is not Galois, its Galois closure contains a unique quadratic extension K_2/F, which we take as companion of K).

** : this symbol denotes a different approach, which we call **big Galois closure**: instead of looking for some Galois extension of low degree, one considers a big Galois extension containing both the equivalent extensions K/F and L/F, and one proves that the isomorphism works in this larger setting. We use this technique to deal with the cases where one of the extensions involved is primitive, i.e. has only F and itself as F-sub-extensions.

Remark 15. Notice that Corollary 4 does not involve quartic fields: in fact, its claim does not apply to them and in the end of the chapter we will provide an example of two quartic extensions having the same inert primes which are not isomorphic.

2.3 Local GCD equivalence in low degrees

2.3.1 Equivalence in degree 2

We already know that locally GCD equivalent quadratic fields are isomorphic. Nonetheless, in this section we still examine them, in order to get some few results which will be useful for higher degree cases.
Remember that the only splitting types available for a quadratic field are $(1,1)$ and (2).

Proposition 7. *Let K and L be two quadratic fields over F.*

1) If $\{\mathfrak{p} \in \mathcal{P}_F \colon f_K(\mathfrak{p}) = f_L(\mathfrak{p}) = (1,1)\}$ has prime density strictly greater than $1/4$, then $K = L$.

2) The set $\{\mathfrak{p} \in \mathcal{P}_F \colon f_K(\mathfrak{p}) = f_L(\mathfrak{p})\}$ has prime density $\geq 1/2$. K and L are equal if and only if the strict inequality holds.

Proof.

1) Assume that $K \neq L$: then their composite field KL is a Galois field of degree 4 over F, and so

$$\{\mathfrak{p} \in \mathcal{P}_F \colon f_{KL}(\mathfrak{p}) = (1,1,1,1)\} = \{\mathfrak{p} \in \mathcal{P}_F \colon f_K(\mathfrak{p}) = f_L(\mathfrak{p}) = (1,1)\}.$$

But this gives a contradiction, since the first set has prime density equal to $1/4$, while the second one has a greater density by the assumption.

2) Let $K = F[x]/(x^2 - \alpha)$ and $L = F[x]/(x^2 - \beta)$, such that $K \neq L$: the set $\{\mathfrak{p} \in \mathcal{P}_F \colon f_K(\mathfrak{p}) = f_L(\mathfrak{p})\}$ is identified with the set of totally split primes in $F[x]/(x^2 - \alpha\beta)$. The claim follows immediately.

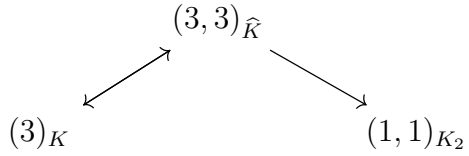
□

2.3.2 Equivalence in degree 3

The equivalence problem in this degree can be solved by means of the sole Galoic companions technique.
Let K and L be two cubic fields over F which are locally GCD equivalent.

* Assume that one of the extensions is Galois, for example K. Then, as reported in Section 1.3, its inert primes have density equal to $2/3$: being L F-locally GCD equivalent to K, it must have the same value for the density of its inert primes, so that L/F is Galois too. But if K/F and L/F are Galois cubic extensions and are locally GCD equivalent, they have the same totally split primes, and thus $K = L$ by Proposition 6.

* Let us assume that both K and L are not Galois. Consider their Galois closures $\widehat{K}$ and $\widehat{L}$, and the quadratic Galois companions K_2 and L_2.
  Using Proposition 3, it is easy to show the following correspondence among the splitting types of the fields involved:



  One gets the following identity:

$$\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p}) = (1,1), f_K(\mathfrak{p}) = (3)\} = \{\mathfrak{p}\colon f_{L_2}(\mathfrak{p}) = (1,1), f_L(\mathfrak{p}) = (3)\}. \tag{2.3}$$

  The computations in Section 1.3 implies that $\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p}) = (1,1) = f_{L_2}(\mathfrak{p})\}$ has prime density at least $1/3 > 1/4$, and by Proposition 7 one has $K_2 = L_2$.
  The remaining totally split primes in K_2, which have prime density equal to $1/2 - 1/3 = 1/6$, are exactly the ones that split completely in $\widehat{K}$. But this fact, together with $K_2 = L_2$ and Equality (2.3), force $\widehat{K}$ and $\widehat{L}$ to have the same totally split primes, i.e. $\widehat{K} = \widehat{L}$, which in turn implies $K \simeq L$ (because the cubic extensions in $\widehat{K}/F$ are F-conjugated between them).

2.3.3 Equivalence in degree 4

Just like for the previous degree, searching for Galois companions will be enough to study the equivalence between extensions of degree 4.
The tables of densities presented in Section 1.3 show that the Galois closures of locally GCD equivalent quartic number field extensions must have the same Galois group. This immediately implies that whenever one of the extensions is Galois, then the equivalence is actually an isomorphism.

* $G = D_4$: Let us take K/F and L/F locally GCD equivalent quartic extensions with Galois closures $\widehat{K}$ and $\widehat{L}$ and Galois group D_4. We follow the notations of diagram (1.3) for the sub-extensions of $\widehat{K}$ and $\widehat{L}$.

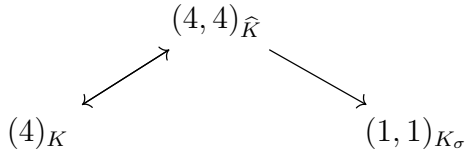
Consider the subfield $K_2 \subseteq K$: it is immediate to see from Proposition 3 that, if $f_K(\mathfrak{p}) = (4)$, then $f_{K_2}(\mathfrak{p}) = (2)$; in the same way, a prime ideal $\mathfrak{p}$ such that $f_K(\mathfrak{p}) \in \{(1,1,1,1),(1,1,2)\}$ has splitting type $f_{K_2}(\mathfrak{p}) = (1,1)$. These facts, together with the local GCD equivalence between K and L, yield the equalities:

$$\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p}) = (2), f_K(\mathfrak{p}) = (4)\} = \{\mathfrak{p}\colon f_{L_2}(\mathfrak{p}) = (2), f_L(\mathfrak{p}) = (4)\}, \tag{2.4}$$

$$\begin{aligned} &\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p}) = (1,1), f_K(\mathfrak{p}) \in \{(1,1,1,1),(1,1,2)\}\} \\ =&\{\mathfrak{p}\colon f_{L_2}(\mathfrak{p}) = (1,1), f_L(\mathfrak{p}) \in \{(1,1,1,1),(1,1,2)\}\}. \end{aligned} \tag{2.5}$$

From Section 1.3, the sets in Equality (2.4) have prime density equal to $1/4$, while the ones in Equality (2.5) have prime density equal to $3/8$. This fact implies that K_2 and L_2 have the same splitting type on at least $5/8$ of the primes, and so $K_2 = L_2$ by Proposition 7.

Let us consider now the field K_σ. Using Proposition 3, it is possible to show the following behaviour:



Thus one obtains the equality

$$\{\mathfrak{p}\colon f_{K_\sigma}(\mathfrak{p}) = (1,1), f_K(\mathfrak{p}) = (4)\} = \{\mathfrak{p}\colon f_{L_\sigma}(\mathfrak{p}) = (1,1), f_L(\mathfrak{p}) = (4)\} \tag{2.6}$$

and the sets above have prime density equal to $1/4$ from Section 1.3.
Furthermore, the set of primes $\{\mathfrak{p}\colon f_K(\mathfrak{p}) = f_L(\mathfrak{p}) = (1,1,1,1)\}$ has positive density $\varepsilon > 0$ (because it corresponds to the set of totally split primes in the composite extension KL) and, thanks to the fact that these primes split completely also in $\widehat{K}$ and $\widehat{L}$, it is clear that for each of these primes, the equalities $f_{K_\sigma}(\mathfrak{p}) = f_{L_\sigma}(\mathfrak{p}) = (1,1)$ hold. Thus, thanks to Equality (2.6), K_σ and L_σ share a set of primes with density $1/4 + \varepsilon$, and so $K_\sigma = L_\sigma$; being $K_2 = L_2$ one gets the equality $K_{\sigma^2} = L_{\sigma^2}$ between the composite fields.
Now, we show that $\widehat{K} = \widehat{L}$: one has the equalities

$$\{\mathfrak{p}\colon f_K(\mathfrak{p}) = (2,2)\} = \{\mathfrak{p}\colon f_L(\mathfrak{p}) = (2,2)\},$$

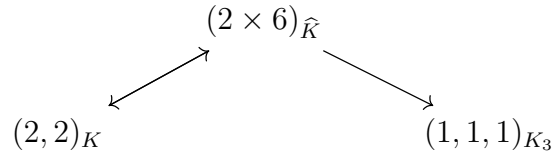
$$\{\mathfrak{p}\colon f_{K_{\sigma^2}}(\mathfrak{p}) = (1,1,1,1)\} = f_{L_{\sigma^2}}(\mathfrak{p}) = (1,1,1,1)\}$$

and the intersection of these sets gives

$$\{\mathfrak{p}\colon f_{K_{\sigma^2}}(\mathfrak{p}) = (1,1,1,1), f_K(\mathfrak{p}) = (2,2)\} = \{\mathfrak{p}\colon f_{L_{\sigma^2}}(\mathfrak{p}) = (1,1,1,1), f_L(\mathfrak{p}) = (2,2)\}.$$

The computations in Section 1.3 imply that the sets above have prime density exactly equal to $1/8$, because they are the primes with Artin symbol equal to $\{\sigma^2\}$. This means that the remaining totally split primes in K_{σ^2}, which have prime density equal to $1/4 - 1/8 = 1/8$, identify $\widehat{K}$; but being $K_{\sigma^2} = L_{\sigma^2}$, this means that $\widehat{K}$ and $\widehat{L}$ have the same totally split primes, i.e. $\widehat{K} = \widehat{L}$.
Finally, we show that $K \simeq L$: if they were not, it would be $L \simeq K'$, where K'/F is the quartic extension shown in Diagram (1.3); but then K and L could not be locally GCD equivalent, because a prime with Artin symbol τ would have splitting type $(2,2)$ in one field but $(1,1,2)$ in the other.

* $G = A_4$: Let K_3/F and L_3/F be the unique cubic Galois extensions contained in $\widehat{K}/F$ and $\widehat{L}/F$ respectively: we consider them as the cubic Galois companions of K and L. Proposition 3 yields the following behaviour on the splitting types:



Thus one gets the identity

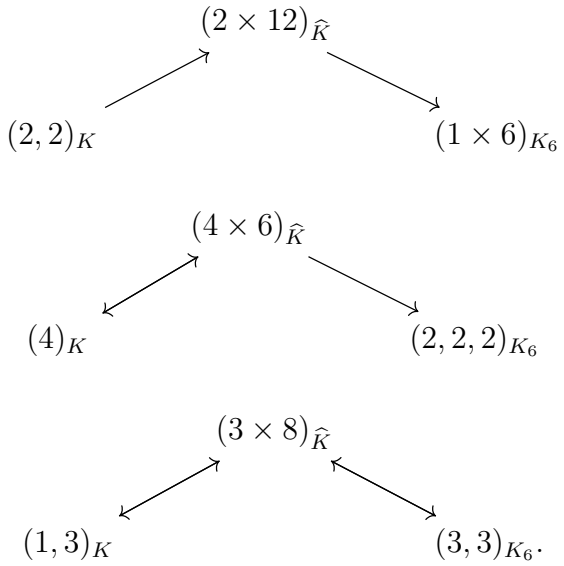
$$\{\mathfrak{p}\colon f_{K_3}(\mathfrak{p}) = (1,1,1), f_K(\mathfrak{p}) = (2,2)\} = \{\mathfrak{p}\colon f_{L_3}(\mathfrak{p}) = (1,1,1), f_L(\mathfrak{p}) = (2,2)\}. \tag{2.7}$$

From Section 1.3, one sees that the sets above have prime density $1/4$, and this forces $K_3 = L_3$; if this was not true, the composite Galois extension KL/F would have degree 9. But being

$$\{\mathfrak{p}\colon f_{K_3L_3}(\mathfrak{p}) = (1\times 9)\} = \{\mathfrak{p}\colon f_{K_3}(\mathfrak{p}) = f_{L_3}(\mathfrak{p}) = (1,1,1)\},$$

the left hand side would have prime density equal to $1/9$, which is in contradiction with Equality (2.7).
The remaining totally split primes in K_3 have density $1/3 - 1/4 = 1/12$ and are precisely the primes which split completely in the Galois closure $\widehat{K}$. Thus, equality (2.7) and $K_3 = L_3$ force $\widehat{K}$ and $\widehat{L}$ to have the same totally split primes, i.e. $\widehat{K} = \widehat{L}$, which implies $K \simeq L$.

* $G = S_4$: Let K_6/F be the Galois companion of degree 6 associated to K. Proposition 3, together with the correspondence between K and any subgroup of order 6 of S_4 and the one between K_6 and the normal subgroup of order 4 of S_4, gives the following relations between the splitting types:



This immediately shows that, if K/F and L/F have Galois closure with group S_4 and are locally GCD equivalent, there is the equality

$$\{\mathfrak{p}\colon f_{K_6}(\mathfrak{p}) = (1 \times 6), f_K(\mathfrak{p}) = (2,2)\} = \{\mathfrak{p}\colon f_{L_6}(\mathfrak{p}) = (1 \times 6), f_L(\mathfrak{p}) = (2,2)\} \quad (2.8)$$

and the prime density of these sets (which is equal to the one of primes with splitting type $(2,2)$ in K) is equal to $1/8$, as reported in Section 1.3.
Assuming $K_6 \neq L_6$, the Galois composite K_6L_6 would have degree $n \geq 12$. But then the equality

$$\{\mathfrak{p}\colon f_{K_6L_6}(\mathfrak{p}) = (1 \times n)\} = \{\mathfrak{p}\colon f_{L_6}(\mathfrak{p}) = (1 \times 6) = f_{L_6}(\mathfrak{p})\}$$

would be a contradiction with respect to the previous computation, because the sets of Equality (2.8) would be contained in a set of prime density $1/n \leq 1/12$.
Being $K_6 = L_6$, let us look now the Galois closures $\widehat{K}$ and $\widehat{L}$. From the locally GCD equivalence between K and L, one already has

$$\{\mathfrak{p}\colon f_{\widehat{K}}(\mathfrak{p}) = (4 \times 6)\} = \{\mathfrak{p}\colon f_{\widehat{L}}(\mathfrak{p}) = (4 \times 6)\},$$

$$\{\mathfrak{p}\colon f_{\widehat{K}}(\mathfrak{p}) = (2 \times 12), f_K(\mathfrak{p}) = (2,2)\} = \{\mathfrak{p}\colon f_{\widehat{L}}(\mathfrak{p}) = (2 \times 12), f_L(\mathfrak{p}) = (2,2)\}.$$

Moreover, the equality $K_6 = L_6$ yields

$$\{\mathfrak{p}\colon f_{\widehat{K}}(\mathfrak{p}) = (3 \times 8)\} = \{\mathfrak{p}\colon f_{\widehat{L}}(\mathfrak{p}) = (3 \times 8)\}$$

and the primes with splitting type $(2,2,2)$ in K_6 which do not come from inert ideals of K have necessarily splitting type (2×12) in $\widehat{K}$: this allows us to conclude that

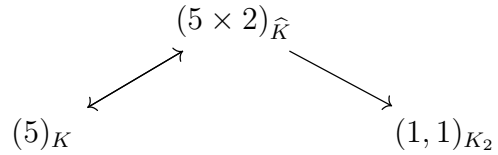
$$\{\mathfrak{p}\colon f_{\widehat{K}}(\mathfrak{p})=(2\times 12)\}=\{\mathfrak{p}\colon f_{\widehat{L}}(\mathfrak{p})=(2\times 12)\},$$

which in turn yields that $\widehat{K}$ and $\widehat{L}$ share the same totally split primes, i.e. $\widehat{K}=\widehat{L}$, and from this it follows $K\simeq L$.

2.3.4 Equivalence in degree 5

Degree 5 extensions represent the first case for which there exist simple non-abelian Galois groups, whose structure forbids the existence of a Galois companion. Whenever one of these extensions occur, we will use the Big Galois Closure approach instead of the Galois companions.
Let K and L be locally GCD equivalent fields of degree 5 over F. It is immediate from the calculations in 1.3.4 and the density of the inert primes that, if one of them is Galois over F, then the two fields are actually isomorphic. Moreover, if $\widehat{K}$ has group $G_K=D_5$, then $\widehat{L}$ has group G_L equal to either D_5 or A_5; if $\widehat{K}$ has $G_K=F_5$, then $\widehat{L}$ has group G_L equal to either F_5 or S_5.

* $G_K=D_5$ and $G_L=D_5$: let K_2/F and L_2/F be the quadratic Galois companions of K and L respectively. Proposition 3 yield the following behaviour on inert primes:

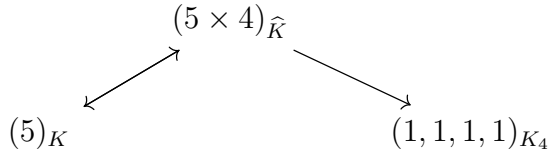


Thus one has the identity

$$\{\mathfrak{p}\colon f_{K_2}(\mathfrak{p})=(1,1), f_K(\mathfrak{p})=(5)\}=\{\mathfrak{p}\colon f_{L_2}(\mathfrak{p})=(1,1), f_L(\mathfrak{p})=(5)\}. \tag{2.9}$$

Thanks to the computations in Section 1.3, the above set has prime density equal to $2/5>1/4$, and this implies $K_2=L_2$ by Proposition 7.
The remaining totally split primes in K_2 (which have density $1/2-2/5=1/10$) are precisely the primes which split completely in $\widehat{K}$. Thus Equality (2.9) and $K_2=L_2$ force $\widehat{K}$ and $\widehat{L}$ to have the same totally split primes, i.e. $\widehat{K}=\widehat{L}$. This yields $K\simeq L$.

* $G_K=F_5$ and $G_L=F_5$: Let K_4 and L_4 be the quartic Galois companions of K and L respectively. There is the following correspondence on splitting types



which yields the identity

$$\{\mathfrak{p}\colon f_{K_4}(\mathfrak{p}) = (1,1,1,1), f_K(\mathfrak{p}) = (5)\} = \{\mathfrak{p}\colon f_{L_4}(\mathfrak{p}) = (1,1,1,1), f_L(\mathfrak{p}) = (5)\}. \tag{2.10}$$

The above sets have prime density equal to $1/5$, thanks to Section 1.3. If K_4 and L_4 were not equal, their Galois composite K_4L_4 would be a field of degree $n \geq 8$ over F; but then one would have the identity

$$\{\mathfrak{p}\colon f_{K_4L_4}(\mathfrak{p}) = (1 \times n)\} = \{\mathfrak{p}\colon f_{K_4}(\mathfrak{p}) = f_{L_4}(\mathfrak{p}) = (1,1,1,1)\},$$

and the left hand side would have prime density $1/n \leq 1/8$, which is in contradiction with our assumption. Thus $K_4 = L_4$.
The remaining totally split primes (which have density $1/4 - 1/5 = 1/20$) are precisely the primes which split completely in $\widehat{K}$: then Equality (2.10) and $K_4 = L_4$ force $\widehat{K}$ and $\widehat{L}$ to have the same totally split primes, i.e. $\widehat{K} = \widehat{L}$.
This immediately implies $K \simeq L$.

** $G_K = A_5$ and $G_L = A_5$: consider the Galois closures $\widehat{K}$ and $\widehat{L}$ and let us study their intersection.
If $\widehat{K} \cap \widehat{L}$ is different from F, then there is a common non-trivial subfield, which identifies the same totally split primes for both the fields, implying $\widehat{K} = \widehat{L}$ and $K \simeq L$ (see the end of Chapter 1 for more details).
So assume the intersection is equal to F: the composite Galois extension $\widehat{K}\widehat{L}$ has degree 3600 and Galois group $A_5 \times A_5$. A prime $\mathfrak{p}$ which is inert in both K and L has Artin symbol formed by elements of order 5 in $A_5 \times A_5$. These elements have the form (g,h) with $g^5 = h^5 = 1_{A_5}$, with the only exception of $g = h = 1_{A_5}$.
But by local GCD equivalence, the set of such primes has prime density $2/5$, while the density of the primes having elements of order 5 in $A_5 \times A_5$ as Artin symbols is $(25 \cdot 25 - 1)/3600 = 624/3600 < 1/4 < 2/5$, which is a contradiction.

** $G_K = D_5$ and $G_L = A_5$: just like in the previous case, consider the intersection between the Galois closures $\widehat{K}$ (with group D_5) and $\widehat{L}$ (with group A_5). The intersection can be either a quintic field or F.
In the first case a field isomorphic to K would be contained in $\widehat{L}$, which would yield $K \simeq L$.
Otherwise, if the intersection is trivial, consider the composite Galois field $\widehat{K}\widehat{L}$. It

has degree $10 \cdot 60 = 600$ and has group $D_5 \times A_5$.
A prime which is inert in both K and L has an element of order 5 in the new group as Artin symbol. But such inert primes form a set of prime density equal to $2/5$, as reported in Section 1.3, while the density of the primes having these symbols is $(5 \cdot 25 - 1)/600 = 124/600 < 2/5$.

** $G_K = F_5$ and $G_L = S_5$: Let us consider the closures $\widehat{K}$ (with group F_5) and $\widehat{L}$ (with group S_5). We recall that the symmetric group S_5 does not have a subgroup with index 4 (see the corresponding page on [77]) and has no normal subgroups of order strictly gratr than 2, while F_5 contains the normal subgroup of order 10 $\langle \sigma^2, \mu \rangle$, which in turn forces $\widehat{K}$ to admit a quadratic sub-extension.
Given this, the degree of the intersection field $\widehat{K} \cap \widehat{L}$ over F can be either $1, 2, 5, 10$ or 20: if it was 20, then it would be $\widehat{K} \subset \widehat{L}$, which is not possible because a Galois field in $\widehat{L}$ has only degree 1 or 2. If $[\widehat{K} \cap \widehat{L} : F] = 10$, then the two Galois fields share a non Galois field of degree 10, and by Corollary 2 $\widehat{K}$ and $\widehat{L}$ would share the same totally split primes, yielding $\widehat{K} = \widehat{L}$, which is absurd. If the intersection has degree 5, then the two Galois fields share a common quintic field, which implies $K \simeq L$.
Thus, we are now left with two possibilities, where the intersection is a Galois field. Assume first that the intersection is equal to F: then the composite Galois extension $\widehat{K}\widehat{L}$ has degree $20 \cdot 120 = 2400$ and Galois group $F_5 \times S_5$. A prime $\mathfrak{p}$ which is inert in both K and L has a conjugacy class of elements of order 5 as Artin symbol in $F_5 \times S_5$. But Section 1.3 implies that these primes form a set with prime density $1/5$, while the density of order 5 Artin symbols in $F_5 \times S_5$ is equal to $(5 \cdot 25 - 1)/2400 = 124/2400 < 1/10$, and this is a contradiction.
In the very same way, if $[\widehat{K} \cap \widehat{L} : F] = 2$, the composite Galois extension $\widehat{K}\widehat{L}$ has degree $(20 \cdot 120)/2 = 1200$ and its Galois group is a subgroup of $F_5 \times S_5$ of index 2, having the same elements of order 5 as $F_5 \times S_5$. Again thanks to Section 1.3, the density of primes which are inert both in K and L is equal to $1/5$, but the Artin symbols of order 5 in the Galois subgroup have density $(5 \cdot 25 - 1)/1200 = 124/1200 < 1/5$, which is a contradiction.

** $G_K = S_5$ and $G_L = S_5$: the Galois closure $\widehat{K}$ is uniquely determined by any subfield which is neither F or the quadratic extension K_2/F.
Let us consider $\widehat{K} \cap \widehat{L}$: whenever this intersection is a field of degree > 2, then the two fields share a common subfield which uniquely determines them, and this yields $\widehat{K} = \widehat{L}$, i.e. $K \simeq L$.
If $\widehat{K} \cap \widehat{L} = F$, the composite extension $\widehat{K}\widehat{L}$ has degree $120 \cdot 120 = 14400$ and Galois group $S_5 \times S_5$. A prime $\mathfrak{p}$ which is inert in both K and L necessarily as an element of order 5 as Artin symbol.
But again, the set of common inert primes of K and L has prime density equal to $1/5$, while the Artin symbols of order 5 have density $(25 \cdot 25 - 1)/14400 = 624/14400 < 1440/14400 = 1/10$.

If instead $\widehat{K} \cap \widehat{L} = K_2$, the composite extension $\widehat{K}\widehat{L}$ has degree 7200 and its Galois group is a subgroup of $S_5 \times S_5$ of index 2, which has the same elements of order 5 of $S_5 \times S_5$.
Thus, following the sketch of the previous case, one obtains a contradiction, because the density of the primes which are inert in both K and L is $1/5$, while the Artin symbols of order 5 in this new Galois group have density $(25 \cdot 25 - 1)/7200 = 624/7200 < 720/7200 = 1/10$.

2.4 Some further remarks

2.4.1 Comparing equivalent fields of different degree

The proofs in the previous section showed that any two number field extensions having same degree $n \leq 5$ which are locally GCD equivalent are in fact isomorphic. In order to complete the proof of Theorem 10, one needs to see what happens when one compares equivalent fields of different degrees.
The densities computations of Chapter 1 show that this possibility cannot exist for locally GCD equivalent fields of degree $n \leq 5$: among the field extensions with these degrees, cubic fields can be equivalent (and thus isomorphic) only to cubic fields, because the inert primes have greatest common divisor of their splitting type equal to 3, a number which is not obtained in any other low degree. For the same reason, quintic fields can be equivalent only to quintic fields.
We are left only with the comparison between quadratic and quartic extensions; but in any quadratic extension the inert primes have density $1/2$, while in quartic fields such a density value is not attained by primes with splitting type $(2, 2)$.

Notice that, whenever considering higher degrees, the chance of having locally GCD equivalent number field extensions with different degrees is possible: this already happens for a stronger relation like Kronecker equivalence, as exlained in Section 2.2.

2.4.2 A counterexample in degree 6

Theorem 10 proves that the local GCD equivalence reduces to isomorphism on equivalent fields of degree $n \leq 5$. It can be proven that there are counterexamples already in degree 6 : in fact, for every Galois cubic extension K/F, it is possible to present two non isomorphic quadratic extensions L/K and M/K such that L/F and M/F are F-locally GCD equivalent extensions of degree 6.
The construction relies on two concepts: first, local GCD equivalence can be proved to be equivalent to the fact that the norm groups of the fractional ideals are the same for the two extensions (see [36], Chapter VI, Section 1.b for the details). Then, using this different formulation, Stern [70] proved the existence of the sextic extensions L/F and M/F as above.

Moreover, being the much stronger relation given by arithmetic equivalence not reducible to the isomorphism for degrees $n \geq 7$, we can finally state that 5 is the maximum degree n for which the claim of Theorem 10 hold for every number field extension of degree n.

2.4.3 Inert primes are not enough in quartic fields

As reported by Corollary 4, Theorem 10 can be expressed, for number fields extensions of prime degree $p \leq 5$, by saying that these extensions are uniquely determined by their inert primes. This formulation, although very elementary, has no direct references in literature: in fact, a proof of this result for cubic fields was the original reason for the author to start studying this subject, and which in the end led him to Lochter's paper [43] and recover Corollary 4 from Lochter's results.

One could wonder if also quartic fields are uniquely determined by their inert primes, in the cases for which they actually exist. This request is much weaker than local GCD equivalence, and, as we show below, it is not enough in order to have an isomorphism.
In fact, there are easy counterexamples: take a quartic field K with Galois closure $\widehat{K}$ having Galois group D_4 and consider the non-conjugated non-Galois field K' contained in $\widehat{K}$ (refer to diagram 1.3 for notations). Then a prime $\mathfrak{p} \in \mathcal{P}_F$ is inert in K if and only if its Artin symbol in D_4 is formed by elements of order 4: but the computations given by Proposition 3 show that the very same property holds also for K', and so we have two non-isomorphic quartic field extensions with same inert primes.
As an explicit example, consider $K := \mathbb{Q}[x]/(x^4 - 3x^2 - 3)$ and $K' := \mathbb{Q}[x]/(x^4 - 3x + 3)$: these quartic fields are not Galois over $\mathbb{Q}$ and share the same Galois closure over $\mathbb{Q}$, which is the octic field $\widehat{K} := \mathbb{Q}[x]/(x^8 + x^6 - 3x^4 + x^2 + 1)$ with Galois group D_4; so they share the inert primes, but in fact K and K' are not isomorphic.

2.4.4 Similar results in higher degree

Although 5 is the maximum degree for which Theorem 10 holds, it is still possible to get a similar rigidity result for large families of field extensions in arbitrary prime degree by a simple adaptation of the Big Galois Closure technique used previously.
Let p be a prime number. Let K/F be a number field extension of degree p, and assume that its Galois closure has group equal to either A_p or S_p. Applying Proposition 3 it is easy to prove that this field has inert primes. If one mimics the procedure used to reduce the equivalence of quintic fields having group A_5 or S_5 to isomorphism, then it is possible to get the following theorem.

Theorem 11. *Let K and L be number fields of prime degree p over F which are F-locally GCD Equivalent and such that their Galois closures share the same Galois group G. Assume G equal either to A_p or S_p Then K and L are F-isomorphic.*

Theorem 11 is actually very strong, because of the fact that a "random" number field extension of prime degree tends to have Galois group of its closure equal to the symmetric

group S_p: from this one can conclude that, for these degrees, the local GCD equivalence reduces very often to isomorphism.
A stronger result, always by Lochter, proves Theorem 11 for every degree n and Galois groups S_n and A_n. At the moment, it seems not reachable without the group-theoretic setting, or by means of the Big Galois Closure technique alone.

Chapter 3

Average rank of a family of elliptic curves

3.1 Rank of elliptic surfaces

3.1.1 Nagao's conjecture

A **family of elliptic curves over** $\mathbb{Q}$ is an elliptic curve over the function field $\mathbb{Q}(t)$ defined by a Weierstrass equation

$$\mathcal{F} : y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t) \tag{3.1}$$

where the coefficients $a_2(t), a_4(t), a_6(t)$ belong to the polynomial ring $\mathbb{Z}[t]$. Being $\mathbb{Q}(t)$ a finitely generated transcendental extension of $\mathbb{Q}$, it follows by Neron-Lang's Theorem that the set of $\mathbb{Q}(t)$-rational points $\mathcal{F}(\mathbb{Q}(t))$ is a finitely generated abelian group: we denote with $r_{\mathcal{F}}$ the rank of the free part of $\mathcal{F}(\mathbb{Q}(t))$.

What happens when one substitutes the formal variable t with a rational number? It can be proved that, for every $s \in \mathbb{Q}$ up to a finite number of exceptions, the curve given by the evaluation of t at s is an elliptic curve over $\mathbb{Q}$: in fact, the finite set of values of t for which this reduction does not apply is the set of solutions of the polynomial equation $\Delta_{\mathcal{F}}(t) = 0$, where $\Delta_{\mathcal{F}}(t)$ is the discriminant of the curve $\mathcal{F}$ over $\mathbb{Q}(t)$. We denote $F(s)$ the curve obtained by the valuation at $s \in \mathbb{Q}$.
With this fact in mind, it is straightforward to see that the family of elliptic curves (3.1) is an elliptic surface in the sense of Section 0.4.5.

Remark 16. The previous consideration permits to consider the elliptic surface (3.1) as a collection of elliptic curves, each one parametrized by a specific rational value of t.

One could wonder about the link between the rank $r_{\mathcal{F}}$ of the elliptic surface over $\mathbb{Q}(t)$ and the ranks $r_{\mathcal{F}(t)}$ of any elliptic curve $\mathcal{F}(t)$ given by the evaluation in a point $t \in \mathbb{Q}$.

Proposition 8. *Let $\mathcal{F}$ be a family of elliptic curves given by the Weierstrass Equation (3.1). Then $r_{\mathcal{F}} \leq r_{\mathcal{F}(t)}$ for all but finitely many $t \in \mathbb{Q}$.*

Proof. This proposition is Silverman's Specialization Theorem ([68], Theorem 20.3 in Appendix C). □

Remark 17. The Parity Conjecture would imply $r_{\mathcal{F}(t)} = r_{\mathcal{F}}$ or $r_{\mathcal{F}(t)} = r_{\mathcal{F}} + 1$, depending on the parity of the root number of $\mathcal{F}(t)$ (see [20] for more details). As a consequence one can think at $r_{\mathcal{F}}$ as an *average* of the ranks of the elliptic curves forming the family.

As mentioned above, one would like to consider the rank of the family $\mathcal{F}$ as an average, under a precise definition, of the ranks of the elliptic curves forming the family. An idea could arise from a suitable average involving the rational points of the elliptic curves modulo prime numbers. Let us state this idea formally in the stricter setting of rational elliptic surfaces.
Given a rational elliptic surface $\mathcal{F}$ and an elliptic curve $\mathcal{F}(t)$ obtained by the specialization of $\mathcal{F}$ at $t \in \mathbb{Q}$, define the number

$$A_{\mathcal{F}}(p) = \frac{1}{p} \sum_{t=0}^{p-1} a_{\mathcal{F}(t)}(p)$$

where the numbers $a_{\mathcal{F}(t)}(p)$ are defined as in Equation (13).
In the paper [49], Nagao established an empirical connection between an average of the numbers $A_{\mathcal{F}}(p)$ and the rank over $\mathbb{Q}(t)$ of a rational elliptic surface $\mathcal{F}$. Supported by many experimental data, he formulated a precise conjecture relating these quantities. The conjecture was proved by Rosen and Silverman [60]: their proof relies on Tate's conjecture, which is proved to be true for rational elliptic surfaces.

Theorem 12 (Nagao's Conjecture)**.** *Let $\mathcal{F}$ be a rational elliptic surface over $\mathbb{Q}$, and let r be its rank over $\mathbb{Q}(t)$. Then:*

$$r = \lim_{x \to +\infty} \frac{1}{x/\log x} \sum_{p \leq x} -A_{\mathcal{F}}(p). \tag{3.2}$$

Remark 18. Nagao's Conjecture is usually presented in the form

$$r = \lim_{x \to +\infty} \frac{1}{x} \sum_{p \leq x} -A_{\mathcal{F}}(p) \log p$$

which is equivalent to the formulation (3.2) thanks to the Prime Number Theorem and summation by parts.

We will use Nagao's conjecture and the formula (3.2) as a practical tool to compute average ranks of families of elliptic curves.

3.1.2 Examples of computations

In this section we illustrate a method for computing the average rank of a family of elliptic curves, used by Bettin, David and Delaunay [8]. The considered family is in fact a rational elliptic surface, to which is possible to apply Nagao's Conjecture, and given by the equation

$$\mathcal{F} : y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t), \quad \deg a_i(t) \leq 2 \text{ for every } i \in \{2, 4, 6\}. \tag{3.3}$$

The constraints on the degrees of the coefficients $a_i(t)$ were needed by Rosen and Silverman to prove that this family of elliptic curves is a rational elliptic surface.

Lemma 4. *The family of elliptic curves given by Equation (3.3) is a rational elliptic surface.*

Proof. See [62], Section 8. □

The equation (3.3) defining the family can be rewritten as

$$\mathcal{F} : y^2 = A(x)t^2 + B(x)t + C(x)$$

where $A(x), B(x), C(x)$ are integer polynomials, $C(x)$ is monic of degree 3 and $\deg A, \deg B \leq 2$.

One needs first to compute the traces $a_{\mathcal{F}(t)}(p)$ of Frobenius morphisms in order to use Nagao's conjecture. By means of the Legendre symbol $\left(\frac{\cdot}{p}\right)$, one gets

$$\begin{aligned} a_{\mathcal{F}(t)}(p) &= p + 1 - \#\mathcal{F}(t)(\mathbb{F}_p) \\ &= p - \sum_{\substack{x \bmod p \\ A(x)t^2+B(x)t+C(x)=\square}} 2\left(\frac{A(x)t^2 + B(x)t + C(x)}{p}\right) - \sum_{\substack{x \bmod p \\ A(x)t^2+B(x)t+C(x)=0}} 1 \end{aligned}$$

$$\begin{aligned} &= \sum_{\substack{x \bmod p \\ A(x)t^2+B(x)t+C(x)\neq 0}} 1 \\ &- \sum_{\substack{x \bmod p \\ A(x)t^2+B(x)t+C(x)\neq 0}} \left(1 + \left(\frac{A(x)t^2 + B(x)t + C(x)}{p}\right)\right)\left(\frac{A(x)t^2 + B(x)t + C(x)}{p}\right) \\ &= - \sum_{\substack{x \bmod p \\ A(x)t^2+B(x)t+C(x)\neq 0}} \left(\frac{A(x)t^2 + B(x)t + C(x)}{p}\right) \\ &= - \sum_{x \bmod p} \left(\frac{A(x)t^2 + B(x)t + C(x)}{p}\right). \end{aligned} \tag{3.4}$$

From (3.4) one gets the equality

$$-\sum_{t=0}^{p-1} a_{\mathcal{F}(t)}(p) = \sum_{x \bmod p} \sum_{t=0}^{p-1} \left(\frac{A(x)t^2 + B(x)t + C(x)}{p} \right). \tag{3.5}$$

The above expression can be simplified.

Proposition 9. *Fix x modulo p. If $A(x) \equiv 0 \mod p$, then*

$$\sum_{t=0}^{p-1} \left(\frac{B(x)t + C(x)}{p} \right) = \begin{cases} p\left(\frac{C(x)}{p}\right) & \text{if } p|B(x) \\ 0 & \text{otherwise,} \end{cases} \tag{3.6}$$

while, whenever $A(x) \neq 0 \mod p$,

$$\sum_{t=0}^{p-1} \left(\frac{A(x)t^2 + B(x)t + C(x)}{p} \right) = -\left(\frac{A(x)}{p}\right) + \begin{cases} p\left(\frac{A(x)}{p}\right) & \text{if } p|B^2(x) - 4A(x)C(x) \\ 0 & \text{otherwise.} \end{cases} \tag{3.7}$$

Proof. The proof of Equation (3.6) is immediate, while for Equation (3.7) we need [41], Theorem 5.48. □

Assuming that p does not divide the discriminant of $\mathcal{F}$, the combination of Equations (3.5), (3.6) and (3.7) yields the formula

$$-A_{\mathcal{F}}(p) = \sum_{\substack{x \bmod p \\ A(x) \neq 0 \bmod p \\ (B^2-4AC)(x) = 0 \bmod p}} \left(\frac{A(x)}{p}\right) - \frac{1}{p} \sum_{\substack{x \bmod p \\ A(x) \neq 0 \bmod p}} \left(\frac{A(x)}{p}\right) + \sum_{\substack{x \bmod p \\ A(x) \equiv B(x) \equiv 0}} \left(\frac{C(x)}{p}\right). \tag{3.8}$$

It is then enough to have more precise informations on the polynomials A, B and C to obtain an explicit result on the numbers $A_{\mathcal{F}}(p)$ and compute their average.

Remark 19. The polynomials $A(x), B(x)$ and $C(x)$ in Equation (3.8) can be assumed to be squarefree, because the sums ranging over their zeros does not take in consideration the multiplicity.

3.2 A specific family of elliptic curves

3.2.1 Definition

Bettin, David and Delaunay [8] mentioned their interest in the enumeration of all the possible average ranks of the family (3.3) depending on all the possible cases for the polynomials $A(x), B(x)$ and $C(x)$. In a work yet to publish, they studied this problem and provided precise values of the ranks for many cases, each one by means of a common

technique. A unique case was not solved, because of its fundamental difference relying in the need of the tools provided by Chebotarev's Theorem and Artin symbols. This additional computation is proved by the author in the next lines.

Consider the family of elliptic curves

$$\mathcal{F} : y^2 = kt^2 + B(x)t + C(x) \tag{3.9}$$

where the parameters are given as follows:

- $k \in \mathbb{Z}$, is non-zero and is not a square;
- $C(x) \in \mathbb{Z}[x]$ is monic with degree 3;
- $B(x) \in \mathbb{Z}[x]$ and $\deg B(x) \leq 2$.

The family (3.9) is a rational elliptic surface and its average rank can be computed via Nagao's Conjecture, obtaining Formula (3.8). Being $k \neq 0$, one has $k \neq 0 \mod p$ for almost every prime number p: thus the third sum in (3.8) vanishes. Moreover, the second sum is equal to

$$-\left(\frac{k}{p}\right)\frac{1}{p}\sum_{x \bmod p} 1 = -\left(\frac{k}{p}\right)$$

and so

$$-A_{\mathcal{F}}(p) = \sum_{\substack{x \bmod p \\ (B^2-4kC)(x)\neq 0 \bmod p}} \left(\frac{k}{p}\right) - \left(\frac{k}{p}\right) = N_{(B^2-4kC)}(p)\left(\frac{k}{p}\right) - \left(\frac{k}{p}\right).$$

where $N_F(p)$ represents the number of distinct zeros modulo p of an integer polynomial F.
The average rank of the family (3.9) is then equal to

$$\begin{aligned} r = \lim_{x\to+\infty} \frac{1}{x/\log x}\sum_{p\leq x} -A_{\mathcal{F}}(p) = &\lim_{x\to+\infty} \frac{1}{x/\log x}\sum_{p\leq x}\left(N_{(B^2-4kC)}(p)\left(\frac{k}{p}\right)\right) \\ &- \lim_{x\to+\infty} \frac{1}{x/\log x}\sum_{p\leq x}\left(\frac{k}{p}\right). \end{aligned} \tag{3.10}$$

The question is the following: how to compute the limit averages in the right hand side of Equation (3.10)? Let us begin by looking at the second sum, which is easier to deal with.
Being k not a square in $\mathbb{Q}$, we know that the value of the Legendre symbol $\left(\frac{k}{p}\right)$ is strictly related to the decomposition of the prime number p in the quadratic field $\mathbb{Q}(\sqrt{k})$: in fact, for every prime number p not dividing $4k$ (i.e. the discriminant of the defining polynomial x^2-k), k is a square modulo p if and only if p splits in the ring of integers of $\mathbb{Q}(\sqrt{k})$. But

we know that the primes totally splitting in $\mathbb{Q}(\sqrt{k})$ have the same density of the inert primes, both of them equal to $1/2$. Thus the second limit in the right-hand side of (3.10) becomes

$$-\lim_{x\to+\infty}\frac{1}{x/\log x}\sum_{\substack{p\leq x\\ k=\square \bmod p}} 1-\lim_{x\to+\infty}\frac{1}{x/\log x}\sum_{\substack{p\leq x\\ k\neq\square \bmod p}}(-1)=-\frac{1}{2}+\frac{1}{2}=0$$

and the rank of the family (3.9) is then equal to

$$r=\lim_{x\to+\infty}\frac{1}{x/\log x}\sum_{p\leq x}N_{(B^2-4kC)}(p)\left(\frac{k}{p}\right). \tag{3.11}$$

Now, how can we detect the result of the above limit? The previous lines tell us that a similar approach with densities could be useful to get the result: the idea, as we will see, is actually correct, but we need to fully understand the relation between k and the polynomial B^2-4kC. More in detail, the rank (3.11) can be easily computed if one understands the intersection between the number field generated by a root of B^2-4kC (which has degree 4 at most) and $\mathbb{Q}(\sqrt{k})$.

3.2.2 A general theorem about a limit average

Let $F(x)\in\mathbb{Z}[x]$ be an integer, squarefree polynomial with degree less or equal than 4. Let $k\in\mathbb{Q}^*$ be not a square. We want to characterize all the possible outcomes of the limit

$$r_F=\lim_{x\to+\infty}\frac{1}{x/\log x}\sum_{p\leq x}N_F(p)\left(\frac{k}{p}\right). \tag{3.12}$$

First of all, it is easy to notice that, if $F=\prod_{i=1}^m G_i$ is the factorization of F as a product of irreducible polynomials in $\mathbb{Q}[x]$, then $N_F(p)=\sum_{i=1}^m N_{G_i}(p)$ for almost every prime number p, and this yields $r_F=\sum_{i=1}^m r_{G_i}$.
Thus, we can always assume that F is irreducible of degree less or equal than 4, and get the general result for squarefree polynomials by adding the results for the irreducible components. We denote with $\mathbb{Q}(F)$ the number field generated by F over $\mathbb{Q}$ and with $\widehat{\mathbb{Q}(F)}$ its Galois closure.

Theorem 13. *Let F and k be as above, and consider r_F as in Equation (3.12).*
Then $r_F=0$, unless one of the following occurs:

- *F has degree 2 and $D_F/k\in(\mathbb{Q}^*)^2$, where D_F is the discriminant of F;*
- *F has degree 4 and there is a number field inclusion $\mathbb{Q}(\sqrt{k})\subseteq\mathbb{Q}(F)$, where $\mathbb{Q}(F):=\mathbb{Q}[x]/(F(x))$.*

For each one of these latter cases we get $r_F=1$ instead.

Remark 20. For all but finitely many primes p, $N_F(p)$ equals the number of prime ideals of $\mathbb{Q}(F)$ over p of inertia degree equal to 1.

The proof of Theorem 13 relies heavily on the computation of densities of prime ideals explained in Chapter 1 by means of Artin symbols. The most important thing to understand, in order to show the computations, is the relation between the field $\mathbb{Q}(F)$ generated by F, its Galois closure $\widehat{\mathbb{Q}(F)}$ and the field $\mathbb{Q}(\sqrt{k})$, so that the computations involving Artin symbols become understandable.
In fact, many of the cases involving irreducible polynomials of degree ≤ 4 are immediately solved by means of the following general theorem.

Theorem 14. *Let $F \in \mathbb{Q}[x]$ be an irreducible polynomial, let $k \in \mathbb{Q}^*$ be not a square, and consider r_F as in Equation (3.12). Let $\mathbb{Q}(F) := \mathbb{Q}[x]/(F(x))$ and let $L(F)/\mathbb{Q}$ be its Galois closure. Assume that $\mathbb{Q}(\sqrt{k}) \cap L(F) = \mathbb{Q}$. Then $r_F = 0$.*

Proof. Assume $[L(F) : \mathbb{Q}] = n$ and $G := \mathrm{Gal}(L(F)/\mathbb{Q})$: then the composite extension $L(F)\mathbb{Q}(\sqrt{k})/\mathbb{Q}$ is Galois of degree $2n$ and with Galois group $C_2 \times G$, because we are assuming that $Q(\sqrt{k}) \cap L(F) = \mathbb{Q}$. Let $C \subset G$ be an Artin symbol for a set of primes in $\mathbb{Q}(F)$ with splitting type $(f_1, \ldots, f_r)$, having density δ: then, thanks to Proposition 3 and to the fact that a conjugation class in a direct product of groups is the direct product of conjugation classes in the factor groups, we get that $A := \{1_{C_2}\} \times C$ and $B := \{-1_{C_2}\} \times C$ form two distinct Artin symbols in $C_2 \times G$ with equal density $\delta/2$. In fact, the first symbol represents the primes with symbol C in G for which k is a square modulo p, while the second one represents the primes with same symbol C in G but for which k is not a square modulo p.
Putting the contribution of these new symbols in Equation (3.12), the weighted average of the primes with symbol A is equal to $\delta/2$ while for the primes with symbol B we get $-\delta/2$, which means that the contributions of the above Artin symbols delete each other. Applying the same procedure to any other Artin symbol in G we obtain $r_F = 0$. □

Let us look now how to prove the remaining cases for polynomials of low degree:

- $[\mathbb{Q}(F) : \mathbb{Q}] = 2$ and $\mathbb{Q}(\sqrt{k}) = \mathbb{Q}(F)$: first of all, notice that $\mathbb{Q}(F) = \mathbb{Q}(\sqrt{k})$ if and only if $D_F/k \in (\mathbb{Q}^*)^2$.
  For every prime p unramified in $\mathbb{Q}(F)$ we have $N_F(p) \in \{0, 2\}$ and $N_F(p) = 2$ if and only if $(k/p) = 1$. These primes form a set of prime density equal to $1/2$ and thus

$$r = \lim_{x \to +\infty} \frac{1}{x/\log x} \sum_{\substack{p \leq x \\ N_F(p)=2}} 2 = 2 \cdot 1/2 = 1.$$

- $[\mathbb{Q}(F) : \mathbb{Q}] = 3, [L(F) : \mathbb{Q}] = 6$ and $\mathbb{Q}(\sqrt{k}) \subseteq L(F)$: being $\mathrm{Gal}(L(F)/\mathbb{Q}) = S_3$, we have $N_F(p) \in \{0, 1, 3\}$. More precisely, $N_F(p) = 1$ if and only if $(k/p) = -1$

and these primes form a set of prime density equal to $1/2$. The primes p such that $N_F(p) = 3$ have prime density equal to $1/6$, and thus

$$r = \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\le x\\ N_F(p)=1}} (-1) + \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\le x\\ N_F(p)=3}} 3 = -1\cdot\frac{1}{2} + 3\cdot\frac{1}{6} = 0.$$

- $[\mathbb{Q}(F):\mathbb{Q}] = 4$, $\mathbb{Q}(F) = L(F)$, $\mathbb{Q}(\sqrt{k}) \subseteq L(F)$ and $G = C_4$; we have $N_F(p) \in \{0, 4\}$, and the primes with $N_F(p) = 4$ have $(k/p) = 1$ and prime density equal to $1/4$. Thus
$$r = \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\le x\\ N_F(p)=4}} 4 = 4\cdot\frac{1}{4} = 1.$$

- $[\mathbb{Q}(F) : \mathbb{Q}] = 4$, $\mathbb{Q}(F) = L(F)$, $\mathbb{Q}(\sqrt{k}) \subseteq L(F)$ and $G = C_2 \times C_2$; we have $N_F(p) \in \{0, 4\}$ and the primes with $N_F(p) = 4$ have $(k/p) = 1$ and prime density equal to $1/4$. Just like above,
$$r = \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\le x\\ N_F(p)=4}} 4 = 4\cdot\frac{1}{4} = 1.$$

- $[\mathbb{Q}(F) : \mathbb{Q}] = 4, [L(F) : \mathbb{Q}] = 24$ and $\mathbb{Q}(\sqrt{k}) \subseteq L(F)$: being $\mathrm{Gal}(L(F)/\mathbb{Q}) = S_4$, we have $N_F(p) \in \{0, 1, 2, 4\}$. More in detail, $N_F(p) = 1$ forces $(k/p) = 1$, while $N_F(p) = 2$ yields $(k/p) = -1$ (this follows from the fact that a prime p with $N_F(p) = 2$ has splitting type $(1, 1, 2)$ in $\mathbb{Q}(F)$, which by Proposition 3 is associated to the Artin symbols formed by transpositions in S_4 and yield $f_{\mathbb{Q}(\sqrt{k})}(p) = (2)$.

  Thus

$$\begin{aligned} r &= \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\le x\\ N_F(p)=1}} 1 + \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\le x\\ N_F(p)=2}} 2\cdot(-1) + \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\le x\\ N_F(p)=4}} 4 \\ &= 1\cdot\frac{1}{3} - 2\cdot\frac{1}{4} + 4\cdot\frac{1}{24} = 0. \end{aligned}$$

We are left with the cases dealing with $[\mathbb{Q}(F) : \mathbb{Q}] = 4$, $[L(F) : \mathbb{Q}] = 8$, $G = D_4 := \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1}\rangle$ and $\mathbb{Q}(\sqrt{k}) \subseteq L(F)$.
We can assume that $\mathrm{Gal}(L(F)/\mathbb{Q}(F)) = \langle\tau\rangle$: this forces the primes with splitting type $(1, 1, 2)$ to have the set $\{\tau, \sigma^2\tau\}$ as Artin symbol. Otherwise, $\mathrm{Gal}(L(F)/\mathbb{Q}(F)) = \langle\sigma\tau\rangle$, and we obtain the same results simply exchanging τ and $\sigma^2\tau$ with $\sigma\tau$ and $\sigma^3\tau$.
Notice that $N_F(p) \in \{0, 2, 4\}$, the primes with $N_F(p) = 4$ having prime density $1/8$ and $(k/p) = 1$.

- $\mathrm{Gal}(L(F)/\mathbb{Q}(\sqrt{k})) = \langle \sigma\tau, \sigma^2 \rangle$: with this assumption it follows, thanks to Proposition 3, that every prime with $N_F(p) = 2$ has $(k/p) = -1$. This set has prime density equal to $1/4$ and thus

$$r = \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\leq x \\ N_F(p)=2}} 2\cdot(-1) + \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\leq x \\ N_F(p)=4}} 4 = -2\cdot\frac{1}{4} + 4\cdot\frac{1}{8} = 0.$$

- $\mathrm{Gal}(L(F)/\mathbb{Q}(\sqrt{k})) = \langle \sigma \rangle$; again, $N_F(p) = 2$ forces $(k/p) = -1$, and as before:

$$r = \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\leq x \\ N_F(p)=2}} 2\cdot(-1) + \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\leq x \\ N_F(p)=4}} 4 = -2\cdot\frac{1}{4} + 4\cdot\frac{1}{8} = 0.$$

- $\mathrm{Gal}(L(F)/\mathbb{Q}(\sqrt{k})) = \langle \tau, \sigma^2 \rangle$, i.e. $\mathbb{Q}(\sqrt{k}) \subseteq \mathbb{Q}(F)$: every prime with $N_F(p) \in \{2, 4\}$ has $(k/p) = 1$, and thus

$$r = \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\leq x \\ N_F(p)=2}} 2 + \lim_{x\to+\infty} \frac{1}{x/\log x} \sum_{\substack{p\leq x \\ N_F(p)=4}} 4 = \cdot\frac{1}{2} + 4\cdot\frac{1}{8} = 1.$$

3.2.3 The rank of the family

Thanks to Theorem 13, we have now proven how to determine precisely the average rank of the family of elliptic curves (3.9).
In order to state the conclusive result, let us recall that, given a polynomial $p(x) \in \mathbb{Z}[x]$, the squarefree part of $p(x)$ is defined as the product of the irreducible factors of $p(x)$ without multiplicity.

Theorem 15. *Let $\mathcal{F}$ be the family of elliptic curves given by (3.9), and let $F = (B^2 - 4kC)^*(x)$ be the squarefree part of the discriminant polynomial $(B^2 - 4kC)(x)$. Then $r_{\mathcal{F}} = 0$, unless:*

- *F is irreducible of degree 4, and $\mathbb{Q}(\sqrt{k}) \subseteq \mathbb{Q}(F)$. In this case $r_{\mathcal{F}} = 1$.*
- *F has an irreducible quadratic factor G such that D_G/k is a square in $\mathbb{Q}$. In this case $r_{\mathcal{F}} = 1$.*
- *F has degree 4 and $F = G_1 \cdot G_2$, with G_1 and G_2 irreducible of degree 2, such that D_{G_1}/k and D_{G_2}/k are squares in $\mathbb{Q}$. In this case $r_{\mathcal{F}} = 2$.*

This result will be contained in [5], written jointly with Sandro Bettin, Chantal David and Christophe Delaunay, as remaining case of a more general computation of average ranks of elliptic curves.

Part III

Analytic and algorithmic methods

Chapter 4

Explicit formulae

4.1 A short introduction on explicit formulae

4.1.1 Where does Riemann Hypothesis come from?

We begin this section by looking at a classical example involving the Riemann Zeta function $\zeta(s) := \sum_{n=1}^{+\infty} n^{-s}$. Remember that the Riemann Zeta function can be thought as the Dedekind Zeta function of the trivial number field $\mathbb{Q}$.
This function has an Euler product

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

and admits a meromorphic continuation over $\mathbb{C}$ via the function

$$\Lambda(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

which in turn is a meromorphic function with simple poles at 0 and 1; furthermore, $\Lambda(s)$ satisfies the functional equation $\Lambda(1-s) = \Lambda(s)$.
Define the function $\xi(s) := s(s-1)\Lambda(s)$: then $\xi(s)$ is an entire function which satisfies the functional equation $\xi(1-s) = \xi(s)$; it can be proved, via the Phragmen-Lindelöf Theorem, that ξ is an entire function of finite order 1, with infinitely many zeros ρ, all of real part between 0 and 1, which are the so called non-trivial zeros of the Riemann Zeta function. Moreover, the function ξ can be expressed as the product over the zeros

$$\xi(s) := e^{bs+a} \prod_\rho \left(1 - \frac{s}{\rho}\right) e^{s/\rho} \quad a, b \in \mathbb{C}. \tag{4.1}$$

Observe that, by the functional equation and by Schwarz' reflection principle, if ρ is a non trivial zero then the numbers $\bar{\rho}, 1-\rho$ and $1-\bar{\rho}$ are non trivial zeros too.
The Riemann Hypothesis asserts that the real part of the non-trivial zeros is equal to $1/2$.

This conjecture arises naturally from the functional equation, being the line $\mathrm{Re}\, s = 1/2$ the symmetric axis for the equation, and it is known that Riemann itself was able to compute the non-trivial zeros with lowest imaginary part, proving that their real part is indeed equal to $1/2$.
Although it derives from the symmetry of $\xi(s)$, this setting alone does not make clear why the Riemann hypothesis is so important in Number Theory: in order to understand this we need to introduce a tool, the explicit formula, with several generalizations which will be explained in the next sections.

4.1.2 The connection between prime numbers and non-trivial zeros

The definition $\xi(s) = s(s-1)\Lambda(s)$ and the Euler product expression of $\zeta(s)$ suggest a possible connection between the non trivial zeros of $\zeta(s)$ and the prime numbers. To explicitly get this link, let us compute the logarithmic derivative of both $s(s-1)\Lambda(s)$ and of the product in Equation (4.1): it is necessary also to exploit the series expression (5) for the Digamma function. This produces the identity:

$$\left(\frac{1}{s} + \frac{1}{s-1}\right) + \left(-\frac{\log \pi}{2}\right) + \left(-\frac{\gamma}{2} - \frac{1}{s} - \sum_{n=1}^{\infty} \frac{s}{2n(2n+s)}\right) + \frac{\zeta'}{\zeta}(s) = b + \sum_{\rho} \frac{s}{\rho(s-\rho)}$$

i.e.

$$\frac{1}{s-1} - \frac{\log \pi}{2} - \frac{\gamma}{2} - \sum_{n=1}^{\infty} \frac{s}{2n(2n+s)} + \frac{\zeta'}{\zeta}(s) = b + \sum_{\rho} \frac{s}{\rho(s-\rho)}. \tag{4.2}$$

Letting s go to 0, one obtains the explicit value

$$b = -1 - \frac{1}{2}\log \pi - \frac{\gamma}{2} + \frac{\zeta'}{\zeta}(0)$$

and thus one can rearrange (4.2) to get the expression

$$\frac{\zeta'}{\zeta}(s) = -\frac{s}{s-1} + \frac{\zeta'}{\zeta}(0) + \sum_{n=1}^{\infty} \frac{s}{2n(2n+s)} + \sum_{\rho} \frac{s}{\rho(s-\rho)}.$$

Now, assume that s has real part greater than 1: than, thanks to the Euler product expression of $\zeta(s)$, the logarithmic derivative of the Riemann Zeta function can be expressed as a sum over the prime numbers of logarithmic terms:

$$\frac{\zeta'}{\zeta}(s) = -\sum_{p} \frac{\log p}{p^s - 1}. \tag{4.3}$$

By exploiting also the power series of (4.3) one gets

$$\sum_p \sum_{m=1}^{\infty} \frac{\log p}{p^{ms}} = \frac{s}{s-1} - \frac{\zeta'}{\zeta}(0) - \sum_{n=1}^{\infty} \frac{s}{2n(2n+s)} - \sum_{\rho} \frac{s}{\rho(s-\rho)}. \tag{4.4}$$

Now fix an upper bound x, which is assumed to not be an integer, to the size of powers of primes p^m and apply the Perron Integral Formula (4) (Theorem 3) to both sides of Equation (4.4), where the formula is used choosing a number $\sigma > 1$ as real part for the vertical line of integration. Up to requiring some careful estimates about the number of zeros of $\zeta(s)$ in horizontal strips, one can finally apply the Residue Theorem in order to get the equality

$$\sum_{\substack{p \\ m \geq 1 \\ p^m \leq x}} \log p = x - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{1}{2} \log\left(1 - \frac{1}{x^2}\right), \quad \text{for every positive } x \in \mathbb{R} \setminus \mathbb{Z}. \tag{4.5}$$

The left hand side of Equation (4.5) is known to be asymptotic to x for $x \to \infty$ by the Prime Number Theorem. Thus, the only interesting contribution on the error term is given by the sum over the non-trivial zeros, and in fact the error term is the sharpest possible, equal to $O(x^{1/2+\varepsilon})$ for every $\varepsilon > 0$, if and only if the real part of the non-trivial zeros is equal to $1/2$, i.e. if and only if Riemann Hypothesis holds.

The explicit formula (4.5), which was conjectured by Riemann and proved only 40 years later by Von Mangoldt, is the first instance of a technique widely used in Analytic Number Theory, which consists in linking arithmetic objects such as prime numbers or prime ideals to analytic objects like the zeros of a suitable Zeta function; this connection allows to gain distribution results and arithmetic knowledge from analytic behaviours.
In the following, we will focus on Dedekind Zeta functions and we will present two instances of explicit formulae related to Dedekind Zeta functions: the first formula is due to Weil, while the second one was formulated by Friedman.

4.2 Weil's explicit formula

4.2.1 The discriminant as conductor

As mentioned in the previous section, the study of arithmetic invariants of a number field K could be pursued also by means of a suitable explicit formula for its Dedekind Zeta function. In particular, whenever the field K is not the trivial number field $\mathbb{Q}$, then the discriminant d_K is bigger than 1 in absolute value: this means that the function $\Lambda_K(s)$ defined in Equation (8) has an additional exponential factor, which must be taken into account whenever one applies logarithmic derivatives and integral operators. An approach of this kind would express the discriminant as a sum of many terms, some of them involving the non-trivial zeros of $\zeta_K(s)$ and others related to the prime ideals of

$\mathcal{O}_K$.
There is also another fact to consider: in a process which tries to imitate the explicit formula for the Riemann Zeta function, there is nothing which forces to use $\Lambda_K(s)$ instead of a product of the form $\Lambda_K(s) \cdot F(s)$, where F is a suitable weight function. There are two reasons which suggest the use of this variant: on one side, it can increase the easiness of the proof of the explicit formula thanks to regularity properties of the weight function F; on the other side, it gives sharper estimates for the exponential factor related to the discriminant whenever one is interested in numerical computations.
Each one of the previous concepts is given in the following explicit formula, which is due to Weil: although here is presented for Dedekind Zeta functions, there exist generalizations which are related to other kinds of Zeta functions.

4.2.2 Statement of the formula

Let $F : \mathbb{R} \to \mathbb{R}$ be a function which satisfies the following properties:

- F is even and $F(0) = 1$.
- There exists $a > 0$ such that the function $G(x) := F(x) \cdot \exp\left(\left(\frac{1}{2} + a\right) x\right)$ belongs to $L^1(\mathbb{R})$ and has bounded variation over $\mathbb{R}$.
- The function $G(x)$ satisfies in every point the *mean condition*
$$G(x) = \frac{1}{2}\left(G(x^+) + G(x^-)\right).$$
- The function $\frac{F(0)-F(x)}{x}$ has bounded variation over $\mathbb{R}$.

Define now the *transform* of F as the function of complex variable
$$\Phi(s) := \int_{-\infty}^{+\infty} F(x) \cdot \exp\left(\left(s - \frac{1}{2}\right) x\right) \mathrm{d}x. \tag{4.6}$$
The conditions on F imply that Φ is a holomorphic function in the strip $-a < \operatorname{Re} s < 1+a$, for a suitable choice of $a > 0$.

Theorem 16. *Let K be a number field of degree n and signature (r_1, r_2). Let F be a function which satisfies the conditions above and let Φ be its transform.*
Then we have the equality
$$\begin{aligned}\log|d_K| = {} & r_1\frac{\pi}{2} + n(\gamma + \log 8\pi) - r_1\int_0^{+\infty}\frac{1-F(x)}{2\cosh(x/2)}\mathrm{d}x \\ & - n\int_0^{+\infty}\frac{1-F(x)}{2\sinh(x/2)}\mathrm{d}x - 4\int_0^{+\infty}F(x)\cosh(x/2)\mathrm{d}x \\ & + 2\sum_{\mathcal{P}\subset\mathcal{O}_K}\sum_{m=1}^{\infty}\frac{\log \mathrm{N}(\mathcal{P})}{\mathrm{N}(\mathcal{P})^{m/2}}F(m\log \mathrm{N}(\mathcal{P})) + \sum_{\rho}\Phi(\rho).\end{aligned} \tag{4.7}$$
where γ is Euler's constant and $\sum_\rho$ ranges over the set of non trivial zeros of ζ_K.

Remark 21. If the complex number s in the transform (4.6) has real part equal to $1/2$, then the transform $\Phi(s)$ reduces to the classic Fourier transform. Thus, if the Generalized Riemann Hypothesis for Dedekind Zeta functions was true, the contribution of the term given by non-trivial zeros in the explicit formula (4.7) would be much more easier to estimate.

4.2.3 Sketch of proof

The details of the proof can be found in Poitou's paper [58]. Here we present the main stages of the proof:

- Fix a positive number $T > 0$ which is not the imaginary part of a non trivial zero of $\zeta_K(s)$. Consider a positive number a such that the transform $\Phi(s)$ of F is holomorphic over the strip $\operatorname{Re} s \in (-\varepsilon, 1+\varepsilon)$ and define the rectangle $R := (-\varepsilon, 1+\varepsilon) \times (-T, T)$.

- The formula (4.7) is obtained computing the integral

$$\frac{1}{2\pi i}\int_{\partial R} \Phi(s)\frac{\Lambda_K'}{\Lambda_K}(s)\mathrm{d}s \tag{4.8}$$

  where the boundary ∂R is counterclockwise oriented. By the Residue Theorem, this is equal to

$$\sum_{|\operatorname{Im}\rho|<T} \Phi(\rho) - \Phi(0) - \Phi(1).$$

  The sum of $\Phi(0)$ and $\Phi(1)$ provides a term very similar $4\int_0^{+\infty} F(x)\cosh(x/2)\mathrm{d}x$, which is distinguished from it just by its dependence on T.

- Using the factorization (8) of $\Lambda_K(s)$, the integral (4.8) splits as the sum

$$\begin{aligned}
&\frac{1}{2\pi i}\int_{\partial R} \Phi(s)\left(\log|d_K| - \frac{r_1}{2}\log\pi - 2r_2\log 2\pi\right)\mathrm{d}s \\
&+ \frac{r_1}{2}\frac{1}{2\pi i}\int_{\partial R}\Phi(s)\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right)\mathrm{d}s + r_2\frac{1}{2\pi i}\int_{\partial R}\Phi(s)\frac{\Gamma'}{\Gamma}(s)\mathrm{d}s \\
&+ \frac{1}{2\pi i}\int_{\partial R}\Phi(s)\frac{\zeta_K'}{\zeta_K}(s)\,\mathrm{d}s.
\end{aligned}$$

  The contribution of the first line is immediate to compute, while the second one requires the knowledge of properties of the Gamma function and its logarithmic derivative, including Stirling's asymptotic formula (6) (see [2], Chapter 1). Taking them together, one obtains terms which are very similar to the numbers and the integrals on the right hand side of Formula (4.7), but with the dependence on T as additional condition.

- The contribution of the term related to the logarithmic derivative of $\zeta_K(s)$ is studied in two steps: first, one shifts the computation of the integral on the line $\operatorname{Re} s = 1+\varepsilon$, where $\zeta_K(s)$ can be expressed as an Euler product; then, one uses this product decomposition (4.1) and the analytic properties of the function F and of its transform Φ to get a series over the prime ideals of $\mathcal{O}_K$ with terms involving F.
- Each of the previous terms has a dependence on T: in order to eliminate it and get Weil's explicit formula, one needs some additional information on the distribution of the imaginary parts of the non trivial zeros. More in detail, one verifies that in the horizontal strip $\operatorname{Im} s \in [T, T+1]$ the number of non trivial zeros is $O(\log T)$, and then use this fact to detect suitable sequence $(T_k)_k$ of real numbers going to infinity which are well spaced from the non-trivial zeros, in the same sense used in Chapter 15 of Davenport's book [14], so that Weil's explicit formula finally comes from this limit process.

4.3 Friedman's explicit formula

4.3.1 Recovering the regulator

Weil's explicit formula permits to get an expression of the discriminant d_K of a number field K which depends only on sums related to terms arising from the completed Dedekind Zeta function $\Lambda_K(s)$, such as the prime ideals and the non-trivial zeros.
One could wonder if a similar thing could be done also for the regulator R_K, which plays an analogous role with respect to the group of units $\mathcal{O}_K^*$: this request seems however more difficult to be accomplished because R_K does not appear in the factorization of Λ_K like the discriminant. The only practical analytic expression containing the regulator seems to be the Class Number Formula (9), where R_K is presented together with many other invariants.
Nonetheless, it is still possible to use an approach similar to the previous one to recover an explicit formulation for R_K with no error terms, the proof of which is due to Friedman.

4.3.2 Statement of the formula

Given a number field K with signature (r_1, r_2), define the real function

$$g_{r_1,r_2}(x) := \frac{1}{2^{r_1} 4\pi i} \int_{2-i\infty}^{2+i\infty} (\pi^n 4^{r_2} \cdot x)^{-s/2} \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} (2s-1) \mathrm{d}s. \tag{4.9}$$

This function is defined on the positive real values of x, which allows the integral to be absolutely convergent.

Theorem 17. *For a number field K with signature (r_1, r_2), the following explicit formula holds:*

$$\frac{R_K}{\omega_K} = \sum_{\mathfrak{a}} g_{r_1,r_2}\left(\frac{\mathrm{N}(\mathfrak{a}^2)}{|d_K|}\right) + \sum_{\mathfrak{b}} g_{r_1,r_2}\left(\frac{\mathrm{N}(\mathfrak{b}^2)}{|d_K|}\right) \tag{4.10}$$

where $\mathfrak{a}$ runs over the principal ideals of $\mathcal{O}_K$, while $\mathfrak{b}$ runs over the ideals which in the class group Cl_K belong to the same class of the different ideal $\mathfrak{D}_K$.
Furthermore, if the different is a principal ideal, then the above formula simplifies to

$$\frac{R_K}{w_K} = 2 \sum_{\mathfrak{a}} g_{r_1,r_2} \left(\frac{\mathrm{N}(\mathfrak{a}^2)}{|d_K|} \right). \tag{4.11}$$

4.3.3 Sketch of proof

Just as for Weil's formula, we present only the main stages of the proof of Formula (4.10): all the details can be found in the first pages of [22].

- Let C be a class in the class group Cl_K. Define the partial Dedekind Zeta function related to C as $\zeta_{K,C}(s) := \sum_{I \in C} \mathrm{N}(I)^{-s}$ and its corresponding completed Zeta function as $\Lambda_K(s, C) := |d_K|^{s/2}(\pi^{-s/2}\Gamma(s/2))^{r_1}((2\pi)^{-s}\Gamma(s))^{r_2}\zeta_{K,C}(s)$.
  Then $\Lambda_K(1-s, C) = \Lambda_K(s, C')$ where $C' := [\partial_K] \cdot C^{-1}$. Notice that if $C = [\mathcal{O}_K]$ then $C' = [\partial_K]$.
  Define $\xi_K(s) := \Lambda_K(s, [\mathcal{O}_K]) + \Lambda_K(s, [\partial_K])$. Then $\xi_K(1-s) = \xi_K(s)$

- Consider now the integral

  $$\frac{1}{2\pi i} \int_{\delta - i\infty}^{\delta + i\infty} (2s-1)\xi_K(s)\mathrm{d}s$$

  where $\delta > 1$ is fixed. Up to showing properties derived by the analytic behaviour of the inner function, one can shift the contour to the line $\mathrm{Re}\, s = 1/2$, and being $s = 1$ the only occurring pole, one gets the identity

  $$\frac{1}{2\pi i} \int_{\delta - i\infty}^{\delta + i\infty} (2s-1)\xi_K(s)\mathrm{d}s = \frac{2^{r_1} R_K c_K}{w_K} + \frac{1}{2\pi i} \int_{1/2 - i\infty}^{1/2 + i\infty} (2s-1)\xi_K(s)\mathrm{d}s \tag{4.12}$$

  where $c_K = 2$ if the different ideal ∂_K is not principal, otherwise is equal to 1.

- The function $(2s-1)\xi_K(s)$ is odd with respect to the transformation $s \to 1-s$: thus the last integral in Equation (4.12) is equal to 0.
  Friedman's formula follows now by decomposing ξ_K into the sum of the functions $g_{r_1,r_2}(x)$ defined in Equation (4.9) and exchanging the series with the integral.

Chapter 5

Classification of number fields via discriminants

5.1 The problem of minimum discriminant: a short review

5.1.1 Introduction

Given a number field K, we know that its discriminant d_K encodes the ramification behaviour of the prime numbers in K: in fact, a prime number p ramifies if and only if it divides d_K. Many are the questions and the problems historically arisen in the study of the discriminant: among these, in this chapter we will focus on the problem concerning the minimum size of a discriminant in specific families of number fields. As an example, whenever one considers a family $\{K_\alpha\}_{\alpha \in I}$ of number fields, one can wonder what is the minimum absolute value of the discriminants d_{K_α}. One of the families which were extensively studied is the set of number fields with fixed degree $n \in \mathbb{N}$: we begin its study introducing some preliminary examples.

Let us begin with the computation of the discriminants of number fields of degree 2: this is an easy problem, every quadratic field being of the form $\mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is a squarefree integer. Moreover, the discriminant of these fields is easily proven to be equal to

$$d_K = \begin{cases} 4d & \text{if } d \equiv 2, 3 \mod 4 \\ d & \text{if } d \equiv 1 \mod 4. \end{cases}$$

By checking with some small integers, we see that the minimum value for $|d_K|$ is 3, corresponding to the absolute value of the discriminant of $\mathbb{Q}(\sqrt{-3})$; the immediate next values of $|d_K|$ are $4, 5$ and 8, which come from the fields $\mathbb{Q}(i), \mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{2})$.
This computation immediately yields the minimum values of $|d_K|$ for the quadratic fields with fixed signature: these minima are 3 for the totally immaginary fields and 5 for the totally real ones.

Consider now the case of cubic fields: the search for minimum discriminants is again not difficult, because if the defining polynomial of a cubic field K is equal to $p(x) := x^3 + ax^2 + bx + c$, then its discriminant is $a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$, and if this number has the form p^2q where p and q are squarefree integers, then it coincides with the discriminant of the field.
The minimum values of $|d_K|$ for this family correspond then to 23 (with $a = 0, b = -1, c = 1$), 31 ($a = 0, b = 1, c = 1$), 44 ($a = -1, b = 1, c = 1$) and 49 ($a = -1, b = -2, c = 1$). Moreover, 23 and 49 are the minima for the subfamilies of fields with signature $(1, 1)$ and $(3, 0)$ respectively.

Remark 22. It must be noticed that the previous method is not the most efficient one for classifying the cubic fields with respect to their discriminant: Davenport and Heilbronn [15] showed that any isomorphism class of cubic fields corresponds to a binary cubic form modulo an equivalence given by the action of the group $SL_2(\mathbb{Z})$, and that this bijection transforms the discriminant of the cubic field into the discriminant of the associated cubic form. Several years later, Belabas [6] used this fact to provide a fast algorithm for the classification of cubic fields with low discriminant.

Our problem becomes much more complicated for higher degrees because of a plenty of factors: first of all, any closed formula for the discriminants must be computed with the aid of resultants and this process becomes much more expensive to deal with the higher the degree is. Secondly, if n is a composite number, then a field of degree n could be either primitive or with non-trivial subfields, and this can change the factorization properties of the discriminant. Lastly, as we will see immediately, the degree and the signature have a remarkable influence on the size of the discriminants, which makes these considerations difficult to be done without the aid of algorithmic procedures.

5.1.2 Results from Geometry of Numbers

The first general estimates on the size of the discriminants are due to Minkowski, who was the first, in the end of XIX-th century, to obtain results of this kind in the context of the so called *Geometry of numbers*: with this term one defines the mathematical theory which describes the ring of integers and its subgroups as discrete lattices in euclidean spaces, with the goal of obtaining results on the algebraic invariants of a number field from the geometric properties of the lattices and of the quadratic forms operating on them.
We have seen in Section 0.1 and 0.2 that, given a number field K of degree n, the ring of integers $\mathcal{O}_K$ can be thought as a full rank lattice in $\mathbb{R}^n$, and that $2^{-r_2}\sqrt{|d_K|}$ is the volume of the fundamental parallelotope. An estimate for d_K is thus equivalent to an estimate for this volume: the classical result by Minkowski accomplishes this goal by using convex sets with volumes related to the invariants of K.

Theorem 18 (Minkowski)**.** *Let K be a number field of degree n and signature (r_1, r_2). Then*

$$|d_K|^{1/2} \geq \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}. \tag{5.1}$$

Proof. The idea is to recover the result from Minkowski's Convex Body Theorem, which asserts that, for every full rank lattice $\Lambda \subset \mathbb{R}^n$ and for every convex symmetric set $S \subset \mathbb{R}^n$ with volume greater than $2^n \cdot d(\Lambda)$, then there exists $\lambda \in \Lambda \setminus \{0\}$ such that $\lambda \in S$ (see [10], Chapter 3, Section 2 for the proof of a generalized version of this theorem).
Then one applies this theorem to the lattice induced by $\mathcal{O}_K$ and the convex body given by the inequality

$$\sum_{i=1}^{r_1} |x_i| + 2\sum_{i=1}^{r_2} \sqrt{x_{r_1+i}^2 + y_{r_1+i}^2} < n! \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|d_K|}\, \mathrm{N}(I),$$

where $I \subset \mathcal{O}_K$ is a suitable ideal, and as a result one gets the existence of an element $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that

$$\mathrm{N}(\alpha\mathcal{O}_K) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \mathrm{N}(I)\sqrt{|d_K|}.$$

This inequality yields the existence of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ which satisfies the estimate

$$\mathrm{N}(\mathfrak{p}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|d_K|}. \tag{5.2}$$

Being $\mathrm{N}(\mathfrak{p}) \geq 1$, one gets finally (5.1) by shifting the non discriminant terms of (5.2) to the left. □

Remark 23. Estimate (5.2) can be used for proving that the class group Cl_K is finite: in fact, this result can be obtained by saying that for every class of ideals there exists a prime ideal $\mathfrak{p}$ belonging to the class which satisfies the inequality.

Minkowski's Inequality (5.1) yields the following consequences on the size of discriminants of number fields with degree n and signature (r_1, r_2):

1) First of all, it assures that for every number field K of degree $n \geq 2$ the discriminant is always greater than 1 in absolute value.
The claim is easily verifiable with direct computations when $n = 2$ and $n = 3$, and for $n \geq 3$ is true by induction on n and r_2, because

$$\left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!} \geq \left(\frac{n}{n-1}\right)^{n-1} \left(\frac{\pi}{4}\right) \cdot \underbrace{\frac{(n-1)^{n-1}}{(n-1)!} \left(\frac{\pi}{4}\right)^{r_2-1}}_{>1 \text{ by inductive hypothesis}} \geq \left(\frac{n}{n-1}\right)^{n-1} \left(\frac{\pi}{4}\right).$$

The last quantity is an increasing function in n, and for $n = 3$ it is equal to $(3/2)^2 \cdot (\pi/4) = (9\pi/16) > 1$.

2) If the degree n is fixed, Minkowski's lower bound increases the more r_2 decreases, i.e. the more r_1 increases. It is thus more natural to study minimum discriminants considering number fields wit fixed signature, instead of fields with fixed degree.

3) For any fixed choice of r_2, Stirling's Approximation Formula implies that Minkowski's bound increases exponentially in n. Thus, it is very likely that number fields with high degree cannot have small numbers as discriminants.

Minkowski's estimate proves that the family of number fields with fixed signature admits a minimum discriminant. However, from this result alone it is not clear to determine how many number fields of the family have absolute discriminant less than a given upper bound: their number could be infinite, a priori.
The following theorem, relying on Geometry of Numbers too, assures that this chance does not happen.

Theorem 19 (Hermite)**.** *Given any couple (r_1, r_2) of non negative integers, let $C > 0$. Then there are only finitely many number fields K with signature (r_1, r_2) such that $|d_K| < C$.*

Proof. The claim follows by proving that the result holds for number fields of fixed degree n. The idea of the proof is to show that, if $|d_K| < C$, then there exists an element $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ such that its corresponding element in the lattice induced by $\mathcal{O}_K$ in $\mathbb{R}^n$ satisfies Hermite's inequality (2), and that this condition in turn implies only a finite number of possibilities for the coefficients of the defining polynomial of α. See [51], Chapter III, Section 2 for further details. □

This fact yields the theoretical chance of classifying every number field of fixed signature with discriminant less than a given upper bound: furthermore, if the upper bound is reasonable in some suitable sense, the fact that this finite quantity of fields is given by a finite number of integer polynomials suggests that this goal could be attained by means of algorithmic procedures.
The question now is the following: if we are interested in classifying number fields of low discriminant, what is a "reasonable" value to choose for an upper bound in an algorithm? The setting introduced in the next sections will be helpful for providing an answer.

5.1.3 Lower bounds for discriminants from Weil's explicit formula

A different approach in the study of minimum discriminants was introduced in the 70's by Odlyzko, Poitou and Serre: the idea was to remember that $|d_K|$ appears as a factor in the function $\Lambda_K(s)$ associated to the Dedekind Zeta function of K, and from this fact they managed to get information about the magnitude of this number by exploiting Weil's explicit formula (4.7). The challenge in this process is to be able to evaluate the many terms involved in the formula with satisfying precision and to find a test function F which provides an optimal contribution to the estimate from below of $\log |d_K|$.
There are some facts and remarks which must be underlined.

- An idea for providing an explicit lower estimate is to look for test functions F such that their transform (as defined in Equation (4.6)) is a positive real function

on the critical strip $0 < \operatorname{Re} s < 1$: this is done in order to discard the sum over the non-trivial zeros of ζ_K, which is not easy to deal with without the assumption of the Generalized Riemann Hypothesis (GRH). The obtained inequality, although not very sharp compared to the real minimum values of discriminants, can be used unconditionally.

- If one assumes GRH, the fact that all non-trivial zeros have of ζ_K have real part equal to $1/2$ implies that the transforms occurring in Weil's formula are actually the classic Fourier tranforms, and so one can compute more precisely the contribution of the terms related to non trivial zeros instead of simply discarding them as in the previous lines.
  This process shows that a lower bound for the discriminants is higher whenever one assumes strong hypotheses like GRH, and a comparison with the actual known minima shows that these new lower bounds are not so far from the true minimum discriminants.

- The lower bound for $\log |d_K|$ increases also by assuming something on the arithmetic of the field: in fact, knowing a priori that K contains a fixed number of prime ideals of given norm allows to explicitly compute their contribution in Weil's Formula (4.7). In particular, ideals with very low norm produce great contributions, which in other words means that number fields of given signature with low discriminants cannot have prime ideals of small norm.

In this thesis, we will work unconditionally, i.e. without any assumption on the truth of GRH. In order to do so, we need good assumptions on the test function F: more in detail, we will suppose that

$$F(x) := \frac{f(x)}{\cosh(x/2)} \tag{5.3}$$

where $f : \mathbb{R} \to \mathbb{R}$ is defined such that:

- $f(x)$ is even, $f(0) = 1$ and $\int_0^{+\infty} f(x)\mathrm{d}x$ converges.
- The function $F(x)$ has bounded variation on $\mathbb{R}$ and satisfies the mean condition.
- The function $(1 - f(x))/x$ has bounded variation on $\mathbb{R}$.
- The (classical) Fourier transform of f is a positive function.

With these hypotheses and Weil's Formula, one can prove the following lower bound.

Theorem 20. *Let K be a number field of degree n and signature (r_1, r_2). Let f be a function as the one introduced in Equation (5.3). Then*

$$\frac{1}{n}\log|d_K| \geq \gamma + \log 4\pi + \frac{r_1}{n} - \int_0^\infty (1-f(x))\left(\frac{1}{\sinh x} + \frac{r_1}{n}\frac{1}{2\cosh^2(x/2)}\right)\mathrm{d}x$$
$$- \frac{4}{n}\int_0^\infty f(x)\mathrm{d}x + \frac{4}{n}\sum_{\mathfrak{p}\subset\mathcal{O}_K}\sum_{m=1}^{\infty}\frac{\log \mathrm{N}(\mathfrak{p})}{1+(\mathrm{N}(\mathfrak{p}))^m} f(m\log \mathrm{N}(\mathfrak{p}))$$

where γ is Euler-Mascheroni's constant.

Proof. Also this formula is proved in Poitou's paper [58]: in fact, the inequality obtained is nothing but the version of Weil's explicit formula with $F(x)$ as in Equation (5.3), which allows to discard the positive contribution given by the sum over the non-trivial zeros. □

This inequality can be even more refined by considering the function $g(x) := f(x\sqrt{y})$ as test function instead of $f(x)$, where $y > 0$ is a parameter. The reason for doing so is to be sought in the desire of obtaining sharper estimates depending on the different values of the parameter y; moreover, it allows to reduce the previous estimate (with a generic y) at the following form.

Theorem 21. *Let K be a number field of degree n, signature (r_1, r_2) and discriminant d_K. If $f(x)$ is Tartar's function (5.5), then*

$$\frac{1}{n}\log|d_K| \geq \gamma + \log 4\pi - L_1(y) - \frac{12\pi}{5n\sqrt{y}} + \frac{4}{n}\sum_{\mathfrak{p}\subset\mathcal{O}_K}\sum_{m=1}^{\infty}\frac{\log \mathrm{N}(\mathfrak{p})}{1+(\mathrm{N}(\mathfrak{p}))^m} f(m\sqrt{y}\log \mathrm{N}(\mathfrak{p})) \quad (5.4)$$

where

$$L_1(y) := L(y) + \frac{1}{3}L\left(\frac{y}{3^2}\right) + \frac{1}{5}L\left(\frac{y}{5^2}\right) + \cdots + \frac{r_1}{n}\left[L(y) - L\left(\frac{y}{2^2}\right) + L\left(\frac{y}{3^2}\right)\cdots\right]$$

and

$$L(y) := -\frac{3}{20y^2} + \frac{33}{10y} + 2 + \left(\frac{3}{80y^3} + \frac{3}{4y^2}\right)\left(\log(1+4y) - \frac{1}{\sqrt{y}}\arctan(2\sqrt{y})\right).$$

Again, the technical details for the proof of Theorem 21 are contained in [58].

At the present moment, the function f which has been proved to be the more effective in providing good lower bounds for the discriminants in the greatest number of cases is due to Tartar (see [52]) and it is the function

$$f(x) := \left(\frac{3}{x^3}(\sin x - x\cos x)\right)^2 \quad (5.5)$$

which is the square of the Fourier transform of the function

$$u(x) := \begin{cases} 1 - x^2 & |x| \leq 1 \\ 0 & \text{elsewhere.} \end{cases}$$

Many examples of lower bounds, both unconditional and with the assumption of GRH, can be found in Dyaz y Diaz' tables of discriminant lower bounds [16] and in Odlyzko's review [52]. As one can see from the tables, GRH improves consistently the lower bound for the discriminants, usually up to a value which is not far from the actual minimum value.

Remark 24. The numerical lower bounds obtained from (5.4) are usually presented as lower bounds for the **root discriminant** $|d_K|^{1/n}$ instead that for the discriminant d_K. One practical reason is that the root discriminants are easier numbers to deal with, being much smaller than the true discriminants especially in higher degrees. There is also an arithmetic motivation: in fact, if L/K is a finite unramified extension, then the discriminant ideal $\mathfrak{D}_{L/K}$ is trivial, and so we have the formula $|d_K|^{1/[K:\mathbb{Q}]} = |d_L|^{1/[L:\mathbb{Q}]}$, which implies that the root discriminant is a more convenient object to work with in the setting of unramified extensions. We will see a similar example in Chapter 6.
As a consequence of this fact, whenever one considers an infinite tower $\cdots \subseteq L_{i-1} \subseteq L_i \subseteq L_{i+1} \subseteq \cdots$ of number fields where every field is an unramified extension of the previous one, then the root discriminant is constant along this tower. Objects of this kind are known to exist, thanks to the work by Golod and Shafarevich [27].

5.1.4 Local corrections

If one studies low discriminants for fields with signature (r_1, r_2) with the aid of Weil's explicit formula, then it becomes clear that not only the non-trivial zeros but also the prime ideals are able to give a contribution to the lower bound of the discriminant. In fact, assuming the field K has a prime ideal of fixed norm $\mathrm{N}(\mathfrak{p})$, one can directly estimate the contribution of this ideal in the formula and obtain a higher lower bound, and the smaller is the norm the higher is the value obtained.
One can thus affirm that every field of fixed signature which is assumed to have some prime ideals of fixed norm is forced to have discriminant larger than a specific bound depending on the norm: this bound is called **local correction given by the prime ideal**.

Selmane [65] used the Estimate (5.4), where $f(x)$ is Tartar's function (5.5), in order to explicitly obtain local corrections for number fields of degree ≤ 14. In Table 5.1 and Table 5.2 we show the values she found for the local corrections to $|d_K|$ for number fields of degree 8 and 9, where every box presents the best known lower bound for $|d_K|$ assuming K has a given signature (r_1, r_2) and admits at least a prime ideal of norm $\mathrm{N}(\mathfrak{p})$. As an example, Table 5.1 affirms that any number field with signature $(0, 4)$ which admits at

least a prime ideal of norm 2 must have $|d_K| \geq 3379343$.
It must be noticed that, for every choice of (r_1, r_2) and $\mathrm{N}(\mathfrak{p})$, the optimal value of y which gives the corresponding numerical estimate may change depending on those parameters; furthermore, one observes that the ideals of very small norm like 2 and 3 produce a remarkable contribution.

Table 5.1: Local corrections for number fields of degree 8

(r_1, r_2)	(0,4)	(2, 3)	(4, 2)	(6, 1)	(8,0)
$\mathrm{N}(\mathfrak{p}) = 2$	3379343	11725962	42765027	163060410	646844001
$\mathrm{N}(\mathfrak{p}) = 3$	2403757	8336752	30393063	115852707	459467465
$\mathrm{N}(\mathfrak{p}) = 4$	1930702	6688609	24363884	92810084	367892401
$\mathrm{N}(\mathfrak{p}) = 5$	1656110	5726300	20829049	79259702	313918560
$\mathrm{N}(\mathfrak{p}) = 7$	1362891	4682934	16957023	64309249	254052210

Table 5.2: Local corrections for number fields of degree 9

(r_1, r_2)	(1,4)	(3, 3)	(5, 2)	(7, 1)	(9,0)
$\mathrm{N}(\mathfrak{p}) = 2$	81295493	301476699	1165734091	4679379812	19422150186
$\mathrm{N}(\mathfrak{p}) = 3$	57789556	214235371	828172359	3323651196	13792634200
$\mathrm{N}(\mathfrak{p}) = 4$	46348899	171694276	663330644	2660853331	11037921283
$\mathrm{N}(\mathfrak{p}) = 5$	39657561	146723910	566314434	2269968332	9410709985
$\mathrm{N}(\mathfrak{p}) = 7$	32371189	119294181	459066389	1835807996	7596751280

Another interesting consequence of the local corrections is the following: assume you have a number field K with signature (r_1, r_2) such that $|d_K|$ is less than the local correction given by a prime $\mathfrak{p}$. Then the ring $\mathcal{O}_K$ does not have any prime ideal of norm $\leq \mathrm{N}(\mathfrak{p})$. Consider for example the fields with signature $(2, 3)$: then any field with this signature having absolute discriminant less than 5762300 does not admit prime ideals of norm $2, 3, 4$ and 5.
For the same reason, there cannot exist elements $\alpha \in \mathcal{O}_K$ such that their absolute norm $\mathrm{Nm}(\alpha)$ is an exact multiple of $2, 3, 4$ and 5 (where we say that b is an exact multiple of a if $a|b$ and a does not divide b/a). If $p(x)$ is the defining polynomial of α, then for every $n \in \mathbb{Z}$ the evaluation $p(n) = \mathrm{Nm}(\alpha - n)$ cannot be an exact multiple of the previous numbers: this condition tells us that looking for number fields with discriminant less than a local correction seems convenient because of the many arithmetical conditions that can be put on the corresponding polynomials.

5.2 Hunter-Pohst-Martinet method

5.2.1 Newton sums and corresponding relations

In the previous section we pointed out some lower bounds for discriminants of number fields: in particular, we noticed that looking for number fields of fixed signature with discriminant less than the lower bound given by a local correction could be easier because of the conditions which must be satisfied by the defining polynomials. So assume that we have chosen such a correction as an upper bound for the discriminant; in this section we present some conditions depending on the upper bound of d_K which must be satisfied by the defining polynomials of these fields, which rely again on Geometry of Numbers and produce a finite list of polynomials to consider.

Let K be a number field of degree n and signature (r_1, r_2). Let $\alpha \in \mathcal{O}_K$, and let $\alpha_1 =: \alpha, \alpha_2, \ldots, \alpha_n$ be its conjugates via the embeddings $\sigma_1, \ldots, \sigma_n$ of K. Let $k \in \mathbb{Z}$. Define the **k-th Newton sum of** α as the function:

$$S_k(\alpha) := \sum_{j=1}^{n} \alpha_j^k.$$

Lemma 5. *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, and assume that $\alpha \in \mathcal{O}_K$. Let $f(x) := \prod_{i=1}^{n}(x - \alpha_i) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1}x + a_n$ be its defining polynomial. Then the Newton sums of α satisfy the following properties:*

1) $S_k(\alpha) \in \mathbb{Q}$ for every $k \in \mathbb{Z}$, and $S_k(\alpha) \in \mathbb{Z}$ for every $k \in \mathbb{N}$;

2) $S_0(\alpha) = n$;

3) $S_1(\alpha) = -\operatorname{Tr}_K(\alpha)$;

4) The following relations hold:

$$S_k(\alpha) = -ka_k - \sum_{j=1}^{k-1} a_j S_{k-j}(\alpha) \qquad \text{for every } 2 \leq k \leq n; \tag{5.6}$$

5) $a_{n-1} = -a_n S_{-1}(\alpha)$ and $a_{n-2} = (S_{-1}(\alpha)^2 - S_{-2}(\alpha))/2a_n$;

6) $\operatorname{Nm}(\alpha) = (-1)^n a_n$.

Proof.

1) The claim is immediate, because $\sigma_i(S_k(\alpha)) = S_k(\alpha)$ for every embedding σ_i of K.

2) This point is immediate, just like 3).

4) For $k = 2$, being $a_2 = \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j$, we have

$$-2a_2 - a_1 S_1 = -2 \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j + \left(\sum_{i=1}^{n} \alpha_i \right)^2 = \sum_{i=1}^{n} \alpha_i^2 = S_2(\alpha).$$

A similar proof for bigger exponents is given in [47].

5) Consider the reciprocal polynomial $g(x) := x^n f(1/x)/a_n = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + 1$. Then $b_1 = a_{n-1}/a_n$, $b_2 = a_{n-2}/a_n$ and applying the relations (5.6) to $g(x)$ the claim follows immediately.

6) It follows from the definition of norm of an element.

□

In order to set an algorithmic process for classifying number fields, the idea is to remember that every number field is generated by a monic polynomial with integer coefficients: so, instead of counting number fields, we would like to count polynomials.
Furthermore, enumeration of polynomials could be realized by counting their integer coefficients, which is a discrete process. The relations on Newton sums of algebraic integers imply that we can work with these functions instead that with coefficients.
Thus, if one knows upper bounds for the Newton sums depending on the discriminant, it is then possible to recover the finite number of polynomials which are defining polynomials for fields of fixed signature and bounded discriminant. The goal is now to provide these upper bounds.

5.2.2 Hunter-Pohst-Martinet's Theorems

Previously, we have defined Newton sums of algebraic integers. These functions have the good property of satisfying recursive relations, but it is not easy to directly estimate them, because of the cancellation phenomena that can occur: as an example, when $k = 1$ one can already have $S_1(\alpha) = 0$. Let us introduce a coarser yet more immediate estimate.
Given a number field K of degree n and $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$, in order to get an upper bound for the functions $S_k(\alpha)$ depending on $|d_K|$, define the **absolute Newton sums**:

$$T_k(\alpha) := \sum_{j=1}^{n} |\alpha_j|^k.$$

Obviously it is $|S_k(\alpha)| \leq T_k(\alpha)$ for every $k \in \mathbb{Z}$. These objects have the advantage of being real positive functions: in particular, the function T_2 is nothing but the standard quadratic form over the lattice induced by the integers $\mathcal{O}_K$. Conversely, the absolute functions have the problem of being much bigger in absolute value than the actual Newton sums, because their very definition eliminates the cancellation phenomenon.

Let us begin by looking for an upper bound for the Newton sums S_1 and S_2 in terms of the discriminant d_K: while for the first function one can operate directly on S_1, the second bound will follow from an upper bound of the absolute Newton sum T_2.
The estimate we look for can be obtained by means of the following theorem, proved in [55]:

Theorem 22 (Hunter-Pohst)**.** *Let K be a number field of degree n with discriminant $|d_K|$. Then there exists an element $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ which satisfies the following conditions:*

$$\begin{aligned} &A)\ 0 \leq \mathrm{Tr}(\alpha) \leq \left\lfloor \frac{n}{2} \right\rfloor; \\ &B)\ T_2(\alpha) \leq \frac{\mathrm{Tr}(\alpha)^2}{n} + \gamma_{n-1} \left(\frac{|d_K|}{n} \right)^{1/(n-1)} =: U_2, \end{aligned} \tag{5.7}$$

where γ_{n-1} is the Hermite constant of dimension $n-1$.

The number α is called a ***Hunter-Pohst-Martinet (HPM) element of*** *K.*

The existence of an algebraic integer satisfying condition A) of Theorem 22 alone is very easy to prove: in fact, given an algebraic integer $\beta \in \mathcal{O}_K$, there exists a unique integer $m \in \mathbb{Z}$ such that

$$-\left\lfloor \frac{n}{2} \right\rfloor \leq \mathrm{Tr}(\beta - m) \leq \left\lfloor \frac{n}{2} \right\rfloor$$

and this is due to the fact that $\mathrm{Tr}(1) = n = [K : \mathbb{Q}]$, so that any translation by a rational integer moves the trace of an algebraic integer within intervals of length n. If $\mathrm{Tr}(\beta - m)$ is not positive, take $m - \beta$.
It is instead more difficult to prove the existence of an element satisfying both conditions in Theorem 22; we will not prove it directly, but as a particular instance of a much more general theorem, proved by Martinet [45], who studied an analogous property in extensions K/F of number fields over any base field F.

Theorem 23. *[Martinet] Let K be a number field of degree n, containing a subfield F of degree m. Then there exists an element $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_F$ which satisfies the following conditions:*

$$\begin{aligned} &A)\ 0 \leq \mathrm{Tr}_K(\alpha) \leq \left\lfloor \frac{n}{2} \right\rfloor; \\ &B)\ T_2(\alpha) \leq \frac{m}{n} \sum_{i=1}^{m} |\,\mathrm{Tr}_i(\alpha)|^2 + \gamma_{n-m} \left(\frac{|d_K|}{|d_F|(n/m)^m} \right)^{1/(n-m)} \end{aligned} \tag{5.8}$$

where $\mathrm{Tr}_i(\alpha) := \sum_v \tau_v(\alpha)$, where each τ_v is an embedding of K and the sum runs on the set of all embeddings τ_v that, when restricted to F, coincide with the i-th embedding of F. Furthermore, if $\alpha \in \mathcal{O}_K$ satisfies B), then also $u(\alpha - a)$ satisfies B), where $u \in \mathcal{O}_F^*$ is a root of unity and $a \in \mathcal{O}_F$.

Proof. Let $\sigma : K \to \mathbb{R}^n$ the map given by the embeddings which transforms $\mathcal{O}_K$ into a lattice $\sigma(\mathcal{O}_K)$. Consider the sub-lattice $\sigma(\mathcal{O}_F)$, which has discriminant $4^{-r_2}(n/m)|d_F|$ in

this bigger real vector space (while its just $4^{-r_2'}|d_F|$ in $\mathbb{R}^m$, where r_2' is the number of complex embeddings of F). Consider the standard positive definite quadratic form on $\mathbb{R}^n$, which restricted to $\sigma(\mathcal{O}_K)$ is equal to $T_2(\alpha)$: the form defines a scalar product on $\mathbb{R}^n$, and we denote with Λ the lattice of dimension $n-m$ which is orthogonal to $\sigma(\mathcal{O}_F)$ with respect to this product.
A standard projection procedure shows that the restriction of the previous quadratic form to Λ defines a positive definite quadratic form

$$q(\alpha) := T_2(\alpha) - \frac{m}{n}\sum_{i=1}^{m} |\operatorname{Tr}_i(\alpha)|^2.$$

Being the discriminant of Λ equal to $d(\sigma(\mathcal{O}_K))/d(\sigma(\mathcal{O}_F))$, one uses Hermite's Theorem with q and Λ in order to find an element $\lambda \in \Lambda$ such that its corresponding element $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_L$ satisfies Inequality (5.8).
The element we have just found satisfies the condition B), but nothing guarantees that is satisfies also the condition A). In order to construct an element from α which satisfies both the conditions, let us prove first the last part of the claim, i.e. given α satisfying B), then every $u(\alpha - a)$ satisfies B), when $u \in \mathcal{O}_F^*$ is a root of unity and $a \in \mathcal{O}_F$. Let $\{\sigma_1, \dots, \sigma_m\}$ be the embeddings of F, which will be indexed with the letter i, and let $\tau_1, \dots, \tau_n$ be the embeddings of K, which will be indexed with the letter j.
If $\alpha \in \mathcal{O}_K$ satisfies B), then

$$\begin{aligned} T_2(u(\alpha - a)) &= \sum_{j=1}^{n} |\tau_j(u(\alpha - a))|^2 = \sum_{j=1}^{n} \underbrace{|\tau_j(u)|^2}_{=1} |\tau_j(\alpha) - \tau_j(a))|^2 \\ &= \sum_{j=1}^{n} |\tau_j(\alpha)|^2 - 2\sum_{j=1}^{n} \operatorname{Re}(\tau_j(\alpha)\overline{\tau_j(a)}) + \sum_{j=1}^{n} |\tau_j(a)|^2. \end{aligned} \tag{5.9}$$

Being $a \in \mathcal{O}_F$, for every $i \in \{1, \dots, m\}$ there exists n/m embeddings $\tau_{i,1}, \dots, \tau_{i,n/m}$ such that $\tau_{i,j}(a) = \sigma_i(a)$ for every $j \in \{1, \dots, n/m\}$; using also Inequality (5.8) for α, the right

hand side of Equation (5.9) becomes

$$\begin{aligned}
&\sum_{j=1}^{n} |\tau_j(\alpha)|^2 - 2\sum_{i=1}^{m} \mathrm{Re}(\mathrm{Tr}_i(\alpha)\sigma_i(a)) + \frac{n}{m}\sum_{i=1}^{m} |\sigma_i(a)|^2 \\
&\leq \left(\frac{m}{n}\sum_{i=1}^{m} |\,\mathrm{Tr}_i(\alpha)|^2 + \gamma_{n-m}\left(\frac{|d_K|}{|d_F|(n/m)^m}\right)^{1/(n-m)}\right) - 2\sum_{i=1}^{m} \mathrm{Re}(\mathrm{Tr}_i(\alpha)\sigma_i(a)) + \frac{n}{m}\sum_{i=1}^{m} |\sigma_i(a)|^2 \\
&= \frac{m}{n}\sum_{i=1}^{m} \left|\mathrm{Tr}_i(\alpha) - \frac{n}{m}\sigma_i(a)\right|^2 + \gamma_{n-m}\left(\frac{|d_K|}{|d_F|(n/m)^m}\right)^{1/(n-m)} \\
&= \frac{m}{n}\sum_{i=1}^{m} \underbrace{|\sigma_i(u)|^2}_{=1} |\mathrm{Tr}_i(\alpha) - \mathrm{Tr}_i(a)|^2 + \gamma_{n-m}\left(\frac{|d_K|}{|d_F|(n/m)^m}\right)^{1/(n-m)} \\
&= \frac{m}{n}\sum_{i=1}^{m} |\mathrm{Tr}_i(u(\alpha-a))|^2 + \gamma_{n-m}\left(\frac{|d_K|}{|d_F|(n/m)^m}\right)^{1/(n-m)}.
\end{aligned}$$

So, in order to find an element β which satisfies both A) and B), we pick the element $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_F$ found before which satisfies condition B) and then we look for the unique $a \in \mathbb{Z}$ such that $\mathrm{Tr}(\alpha) \in [-n/2, n/2]$, and we multiply $\alpha - m$ by $u = \pm 1$ depending on $\mathrm{Tr}(\alpha - m)$ being positive or negative. □

5.2.3 Upper bounds for higher degree Newton sums

We used Theorem 23 in order to provide an estimate of the Newton sum S_2 in terms of the discriminant: in fact, we have guaranteed the existence of an element $\alpha \in \mathcal{O}_K$ such that the opposite of its trace is between 0 and half the degree of the field, while its second Newton sum S_2 is bounded in absolute value by the trace and a lattice-constant depending only on the degree of the field and on the discriminant.
We would like now to find similar estimates for the other Newton sums: unfortunately, it is not known if there exists some HPM-element α satisfying, for example, a third strong condition related to $S_3(\alpha)$ in some sense similar to A) and B): this would be true if one could rely on a theory of cubic forms just as strong as the (more natural) one of quadratic forms. Nonetheless, there are ways to obtain an estimate for the absolute Newton sums $T_k(\alpha)$ (and so for the Newton sums) thanks to the knowledge of upper bounds for $S_1(\alpha)$ and $T_2(\alpha)$ alone.

Theorem 24. *Let T and N be two positive constants, and let $n \in \mathbb{N}$ such that $N \leq (T/n)^{n/2}$. Then, for any $m \in \mathbb{Z} \setminus \{0, 2\}$, the function $T_m(x_1, \ldots, x_n) := \sum_{i=1}^{n} x_i^m$ has an absolute maximum on the compact set*

$$S := \left\{(x_1, \ldots, x_n) \in \mathbb{R}^n \colon \sum_{i=1}^{n} x_i^2 \leq T;\ \prod_{i=1}^{n} x_i = N; x_i \geq 0 \text{ for } i = 1, \ldots, n\right\}$$

and the maximum is attained at a point $(y_1, \dots, y_n)$ which has at most two different coordinates.

Proof. The result is obtained by means of Lagrange's Multipliers Method, applying it to the function T_k and the boundary of S. The claim on the coordinates follows from the condition $\prod_{i=1}^n x_i = N$ and computations which are explained in all the details in [55]. The exclusion of $k = 0, 2$ derives from technical details of the proof.
Notice that the maximum point is surely attained on the constraint $\sum_{i=1}^n x_i^2 = T$, because the function T_k is radially increasing. □

Now, assume that $T_2(\alpha) \leq T$ and $\mathrm{Nm}(\alpha) = N$: let $(a, \dots, a, b, \dots, b)$ be a point of maximum for T_k with respect to the previous theorem. Being this point on the boundary, one gets the equation

$$0 = ta^2 + (n-t)b^2 - T = t\left(b^{t-n}N\right)^{2/t} + (n-t)b^2 - T \tag{5.10}$$

where $t \in \{1, 2, \dots, n-1\}$. For every value of t, call y_t the smallest positive value of b which solves the equation: then an estimate for $T_k(\alpha)$ is given by

$$U_k := \max_{t \in \{1,\dots,n\}} \{t\left(y_t^{t-n}N\right)^{k/t} + (n-t)y_t^k\}. \tag{5.11}$$

Thus we are able to bound any Newton sum (and so any coefficient of the defining polynomial) with functions depending on the discriminant of the fields.

Remark 25. The boundary condition $(T/n)^{n/2} \leq N$ corresponds to a precise arithmetical phenomenon: if α is an HPM-element with $T_2(\alpha) = T$ and $N = |\mathrm{Nm}(\alpha)|$, then the inequality between arithmetic and geometric means yields

$$N^2 = \prod_{i=1}^n |\alpha_i|^2 \leq \left(\frac{\sum_{i=1}^n |\alpha_i|^2}{n}\right)^n = \left(\frac{T}{n}\right)^n.$$

Thus it is natural to impose this condition on the previous optimization problem, in order to recall the arithmetic context in which it originates.

5.3 An algorithm for the classification of primitive number fields

5.3.1 Cases previously solved

The setting of Geometry of Numbers, and especially the works on Newton sums related to Hunter-Pohst-Martinet's Theorem, have been the key tool which allowed to provide minimum discriminants and complete tables of number fields for every degree $n \leq 7$. The majority of these achievements were accomplished between the 80's and the first years of the 90's, and some references on the particular instances of the used procedures can be found in the following list:

- [9] and [63] for quartic and quintic fields; although these are among the most recent papers, they present a classification of fields with small discriminant of degree 4 and 5 based on the use of Newton sums.

- [**?**] is part of a series of papers by Olivier about the classification of fields of degree 6.

- [18] is an instance contained in a series of paper by Diaz y Diaz which gives the classification in degree 7.

Results in higher degree were obtained too:

- [17] for totally immaginary octic fields;

- [56] and [72] for totally real fields of degree 8 and 9 respectively.

It is interesting to notice that the case of totally real octic fields was already solved in the past years: this is due to the fact that, although the discriminants for totally real fields are much higher than for other cases, it is in practice easier to find defining polynomials which generate them because, whenever an integer polynomial has only real roots, then there are even more relations between the coefficients and the Newton sums that can be exploited to reduce the ranges for the parameters where the algorithms have to be tested. Assuming to work just with non-primitive fields, many difficulties can be avoided also for high degrees, thanks to Martinet's Theorem 23 and to the fact that if K/F is a number field extension, then $|d_F|^{[K:F]}$ divides $|d_K|$. References about this specific problem are:

- [13] and [64], which give a complete classification of non-pimitive fields of degree 8 with signature $(2,3)$, $(4,2)$ and $(6,1)$ and $|d_K| \leq 6688609, 24363884$ and 92810082 respectively;

- [19] where Diaz y Diaz and Olivier gave a classification of non-primitive number fields of degree 9 with $|d_K| \leq 5 \cdot 10^7, 4 \cdot 10^9, 5 \cdot 10^9, 7 \cdot 10^9$, $6,3 \cdot 10^{10}$ for signature $(1,4), (3,3), (5,2), (7,1), (9,0)$ respectively.

The least signatures for which neither minimum discriminants nor tables of fields with low discriminants were known are the mixed signatures in degree 8, i.e. $(2,3)$, $(4,2)$ and $(6,1)$. In [4] the author was able to give such a classification for the signature $(2,3)$, choosing as upper bound the local correction given by the prime ideal of norm 5 corresponding to that signature. The method is based upon the ideas previously illustrated, but its algorithmic implementation was not effective enough to permit similar results in further signatures. Thanks to a joint work with Bill Allombert and Karim Belabas, we were finally able to write a program running on the computer algebra system PARI/GP [75] which provided minimum discriminants and complete classification of low discriminant number fields in the signatures $(4,2)$ and $(6,1)$, thus completing the degree 8 case, and signatures (1,4) and (3,3) in degree nine (thus for degree 9 only the signatures (5,2) and (7,1) for primitive fields remain to be explored). Although the theoretical ideas shared by the two approaches

are similar, the later approach is much faster and allows to recover the result in signature $(2, 3)$ in much less time.

In order to present the result, we illustrate the algorithmic procedure used, showing how to combine the ideas arising from Weil's explicit formula and Hunter-Pohst-Martinet's theorem to give a complete enumeration of number fields with fixed signature and absolute discriminant less than the local correction given by 5. The program will be presented first by a theoretical point view, with successive remarks on the computational aspects.

5.3.2 A description of the procedure

We want to detect all the number fields K of degree n, signature (r_1, r_2) and $|d_K| \leq C(r_1, r_2, 5)$, where $C(r_1, r_2, 5)$ is the local correction for the signature (r_1, r_2) given by the prime ideal of norm 5: in order to accomplish this, we construct all the polynomials of degree n with integer coefficients which are bounded by the values U_m's found with Theorems 22, 24 and (5.11). Because of this construction, it is clear that we are dealing with defining polynomials of HPM-elements.
The polynomials are generated ranging the values for the Newton sums S_m's in the intervals $[-U_m, U_m]$; from these values we create the coefficients of the polynomials with the help of the relations (5.6) and further conditions derived from the arithmetic nature of the problem, like the fact that any evaluation of the polynomial cannot be an exact multiple of 2,3,4 and 5.
Finally, one looks for additional conditions on the polynomial in order to save it as a generator of a field with the given signature and discriminant bounded by the chosen upper bound.

Remark 26. As stated above, our procedure assumes that we are looking for defining polynomials of HPM-elements. There is a problem, however: unless the number field K is primitive, there is nothing which assures us that the defining polynomial of an HPM element $\alpha \in K$ has degree exactly equal to n. In fact, α could be contained in a proper subfield of K.
So we can just say that this procedure gives a complete classification only for primitive fields, which for composite degrees is still a proper subset of the considered family (though being actually a very large subset).
Fortunately, the older works on non-primitive fields allowed to classify them completely up to bounds which are far higher than the local corrections $C(n, r_1, 5)$.

Let us present now the steps of the algorithm.

Step 0: Choose the value of the degree n and an integer value for S_1 between 0 and $n/2$. Put $a_1 = -S_1$.
Then compute U_2 as in Theorem 22 using $|d_K| = C(n, r_1, 5)$: for the precise values of γ_{n-1} whenever $n \leq 9$, see Section 0.1.2.
Next, call $T = U_2$ and compute $(T/n)^{n/2}$ as in the hypothesis of Theorem 24; choose a

positive integer $N \leq (T/n)^{n/2}$ and put either $a_n = N$ or $a_n = -N$; remember that N is the norm of an element of K, and so it cannot be an exact multiple of 2,3,4 and 5.
Afterwards, compute the upper bounds U_m as in Equation (5.11), for m between 3 and n and $m \in \{-1, -2\}$. We have now set the intervals $[-U_m, U_m]$ in which the Newton sums will range.

Step 1: Put S_2 equal to the maximum integer in $[-U_2, U_2]$ which is congruent to $-a_1 S_1$ modulo 2: if k_2 is the class of $-a_1 S_1$ modulo 2, then

$$S_2 := 2\left\lfloor \frac{U_2 - k_2}{2} \right\rfloor + k_2 \tag{5.12}$$

and put $a_2 := (-S_2 - a1S_1)/2$.
Now, put S_3 equal to the maximum value in $[-U_3, U_3]$ which is equal to $-a_1 S_2 - a_2 S_1$ modulo 3: in the same way, if k_3 is the class of $-a_1 S_2 - a_2 S_1$ modulo 3, then

$$S_3 := 3\left\lfloor \frac{U_3 - k_3}{3} \right\rfloor + k_3 \tag{5.13}$$

and we put $a_3 := (-S_3 - a_1 S_2 - a_2 S_1)/3$.
Do the same for S_4 up to S_{n-1}, always respecting the relations (5.6) and using definitions similar to (5.12) and (5.13), and create the coefficients a_4 up to a_{n-1}.
Finally define $p(x) := x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n$.

Remark 27. There are some checks that can be made already during this step: the polynomial $p(x)$ is kept if and only if it is constructed by Newton sums which satisfy the followings restraints:

$$\begin{aligned}
&\text{If } a_1 = 0, \text{ then } S_3 \geq 0, \\
&S_2 \geq -U_2 + \frac{2}{n} a_1^2, \\
&|S_3| \leq \left(\frac{S_2 + U_2}{2} (S_4 + 2(U_2 - S_2)^2) \right)^{1/2}, \\
&S_4 \geq -2(U_2 - S_2)^2.
\end{aligned} \tag{5.14}$$

The first two inequalities are proved in Cohen's book [12], Chapter 9.
The inequality (5.14) was used in [55] with the term $(U_2 - S_2)$ multiplied by a factor 1. However, the inequality was claimed to be proved by means of the Cauchy-Schwartz inequality, but this technique leads to the appearance of the factor 2, which seems not avoidable with this elementary method.
The fourth inequality is a trivial necessary condition for the validity of the third one.

Step 2: In this step of the algorithm one must check if the polynomial $p(x)$ just constructed satisfies a set of conditions: $p(x)$ is saved if and only if it satisfies each one of the followings conditions.

- $|p(1)| = |\,\mathrm{N}(\alpha - 1)| \leq ((T - 2S_1)/n + 1)^4$ and it cannot be an exact multiple of 2,3,4 and 5.
- a_{n-1}/a_n, being the number which defines S_{-1}, must be in $[-U_{-1}, U_{-1}]$. Similarly, $(a_{n-1}^2/a_n - 2a_{n-2})/a_n$ must be in $[-U_{-2}, U_{-2}]$.
- $|p(-1)| = |\,\mathrm{N}(\alpha + 1)| \leq ((T + 2S_1)/n + 1)^4$ and it cannot be an exact multiple of 2,3,4 and 5.
- The number $-na_n - \sum_{k=1}^{n-1} a_k S_{n-k}$ is equal to S_n and so it must belong to $[-U_8, U_8]$.
- $p(x)$ must be an irreducible polynomial.
- The field generated by $p(x)$ must not have prime ideals of norm less or equal than 5. This can be verified in a n algorithmic way (see the next section). Moreover, the signature of $p(x)$ must be equal to (r_1, r_2).
- Given an integer m, define coredisc(m) as the discriminant of the number field $\mathbb{Q}(\sqrt{m})$. Then we require $|\mathrm{coredisc}(\mathrm{disc}(p(x)))| < C(r_1, r_2, 5)$.

Step 3: In this step we describe how to move on to the next polynomial.
Suppose we have checked $p(x)$. Then the next polynomial is created by increasing a_{n-1} by one, which means that S_{n-1} is decreased by $n - 1$. We now have a new polynomial $p(x)$ that must be tested as described in Step 2.
This process of construction and testing is iterated until S_{n-1} becomes less than the number

$$L_{n-1} := -(n-1)\left\lfloor \frac{U_{n-1} - (n - 1 - k_{n-1})}{n-1} \right\rfloor - (n - 1 - k_{n-1})$$

which is the smallest number in $[-U_{n-1}, U_{n-1}]$ equal to k_{n-1} modulo $n-1$. If $S_{n-1} < L_{n-1}$ we delete a_{n-1} and S_{n-1} and we increase a_{n-2} by one, decreasing S_{n-2} of $n - 2$, then we go back to Step 1 and we create new numbers S_{n-1} and a_{n-1}; then we apply again the tests and the increasing process for a_{n-1} and S_{n-1}.
The number S_{n-2} gets lowered of $n - 2$ every time we repeat the previous sub-step and the process is iterated until S_{n-2} becomes less than

$$L_{n-2} := -(n-2)\left\lfloor \frac{U_{n-2} - (n - 2 - k_{n-2})}{n-2} \right\rfloor - (n - 2 - k_{n-2}).$$

If $S_{n-2} < L_{n-2}$ then we increase a_{n-3} by one, decreasing S_{n-3} of $n - 3$, and we compute new $S_{n-2}, a_{n-2}, S_{n-1}$ and a_{n-1}.
The test is then repeated verifying similar conditions from S_{n-3} up to S_2: the process terminates once we have S_2 less than $L_2 + 2a_1^2/n$ where

$$L_2 := -2\left\lfloor \frac{T - (2 - k_2)}{2} \right\rfloor - (2 - k_2).$$

Once this part of the algorithm is over, we have a list of monic polynomials with integer coefficients and this list depends on the chosen values for a_1 and a_n.

Step 4: We repeat the previous steps for every value of a_1 between 0 and $n/2$ and for every value of a_n which satisfies $|a_n| \leq (T/n)^{n/2}$ and is not an exact multiple of 2,3,4 and 5. We are left with a list of polynomials among which we select the ones generating a number field K with signature (r_1, r_2) with $|d_K| \leq C(n, r_1, 5)$.
The fields gathered are finally classified up to isomorphism and put in increasing order with respect to their absolute discriminant.

5.3.3 Computational remarks

Although the theoretical process described above is not so different by the one used in [4] and the previous papers on the subject, the novelties which allowed to get the minimum discriminants and classifications for further signatures rely all on practical and computational aspects. The first remarkable thing is that our program is now written only as a .gp file, needing only PARI/GP for its execution, while the previous version used for the signature $(2, 3)$ was implemented with a combination of MATLAB and PARI which resulted to be very heavy and time consuming. For example, the author's computations for the signature $(2, 3)$ in [4] required a week, while with this new setting they take no longer than 4 hours.
The reason why MATLAB was needed in the first formulation of the program was the necessity to find the least positive solutions of the Equation (5.10), which is one of the first main steps of the algorithm.

Other features and characteristics of our computations are the following:

- The only value of N which yields long runs of the program is $N = 1$; the possible higher values, which cannot be smaller than 7 thanks to the local correction, provide in fact fast cases which are solved in very few seconds.
  More information about these substeps can be found in the last pages of the Appendix.

- For the considered signatures in degree 9, $(1, 4)$ and $(3, 3)$, we decided to divide the process in further subcases in order to not occupy too much memory with a single run: together with the previous inputs, in these signatures we launched the programs by giving also a value for S_2 and S_3 (which must be obviously compatible with the relation (5.6)).
  Also with these further refinements, every run for a sub-case in the signature $(3, 3)$ examines a number of polynomials of order 10^9.

- Just like in the previous version of the program, an additional input is given by the parity value of the evaluation $p(1)$. This choice is based mainly on the desire to speed up and make lighter the runs of the algorithm, forcing the Newton sum S_{n-1}

to decrease of $2(n-1)$ instead of $n-1$; another reason, a posteriori, is the fact that almost every output polynomial arises from a run with $p(1)$ odd.

- The ordering of the tests to be executed on the candidate polynomials $p(x)$ was chosen so that a slower test arrives later with respect to the others. In fact, the first check to be made is always the one related to the size of $|p(1)|$, which is helpful in restricting the range of polynomials to be considered.

- The longest part of the test, and at the same time one of the most effective, is the check on the low norm ideals of the field generated by the candidate polynomials. In order to speed up the computation, so that one does not really have to create an instance of number field for every possible polynomial, Karim Belabas wrote a PARI function **ZpX-primedec()** which, given an irreducible integer polynomial $p(x)$ and a prime number p, returns the smallest norm of a prime ideal lying over p in the field generated by $p(x)$.
  The function is theoretically based upon the work by Ford, Pauli and Roblot ([21], Section 6) which use the so called Round 4 Algorithm in order to recover the factorization of a prime ideal from the p-adic factorization of a minimal polynomial of the field. For what concerns its efficiency, this function is an order of magnitude faster than the partial factorization given by **nfinit()** and faster than the usual decomposition function **idealprimedec()**: moreover, it is even faster whenever one deals with polynomials which give elements with small valuations for their indexes in $\mathcal{O}_K$. The **ZpX-primedec()** test, applied to the primes 2, 3 and 5, allows to reduce the number of candidate polynomials to a number around 10^6.

- The final check to be made is the one on the size of core(disc($p(x)$)): this test was added only some month after the signatures in degree 8 were solved. However, it is a very useful criterion, although quite slow, because almost every candidate polynomial $p(x)$ has in fact core discriminants of very big size, which would force the number field discriminant to be way over the desired upper bound.
  The number of polynomials surviving this last condition is very small, being at most of order 10^2.

- Once all the tests have been done, one computes the number field discriminant of the survived polynomials via the PARI function **nfdisc()** and later gathers the polynomials $p(x)$ with nfdisc($p(x)$) $\leq C(n, r_1, 5)$ in a list up to isomorphism. The isomorphism check is made using the PARI function **nfisisom()**.
  This last process can be very slow whenever the number of polynomials to be examined by it is around 10^6, and it requires a good amount of memory; the coredisc improvement, which was suggested by Bill Allombert, allowed to transfer this process in an earlier stage of the algorithm, so that for the same time of computation we have a much lighter run of the program.

5.3.4 Minimum discriminants in degree 8 and 9

We now present the results found by our program in the examined signatures. All the statements hold up to isomorphism and every upper bound is the local correction given by 5 for the corresponding signature.

Theorem 25. *There exist 56 number fields K with signature $(2,3)$ and with $|d_K| \leq 5672300$. The minimum value of $|d_K|$ is 4286875.*
There exist 41 number fields K with signature $(4,2)$ and with $|d_K| \leq 20829049$. The minimum value of $|d_K|$ is 15243125.
There exist 8 number fields K with signature $(6,1)$ and with $|d_K| \leq 79259702$. The minimum value of $|d_K|$ is 65106259.
There exist 67 number fields K with signature $(1,4)$ and with $|d_K| \leq 39657561$. The minimum value of $|d_K|$ is 29510281.
There exist 116 number fields K with signature $(3,3)$ and with $|d_K| \leq 146723910$. The minimum value of $|d_K|$ is 109880167.

We give some final remarks.

- With exceptions given by two fields with signature $(2,3)$ with same discriminant equal to -5365963 and two fields with signature $(3,3)$ and same discriminant equal to -142989047, every field in our lists is uniquely characterized by its signature and the value of its discriminant.

- Every field of degree 8 and every field with signature $(1,4)$ which is contained in our lists was already known: in fact, they are all gathered into the Klüners-Malle database of number fields [37], although they are missing in the LMFDB database [74].
  Our work allows to say that these are the only number fields in the examined signatures with discriminant less than the chosen upper bound.

- Concerning the fields of degree 9 and signature $(3,3)$, our procedure showed there exist 116 such fields with $|d_K| \leq 146723910$, while the Klüners-Malle database only contains 62 fields of this kind. Considering the additional 54 fields, we see that 52 of them have discriminant which match with Denis Simon's table of small polynomial discriminants [69]. The two remaining fields satisfy instead the following properties: one of them is the field of discriminant -142989047 which is not isomorphic to the one given by the polynomial in Simon's list; the other one has discriminant equal to -129079703, which is a value not contained in Simon's lists for polynomials of degree 9 with 3 real roots, thus providing a number field and a discriminant value which were not foreseen.

- Every field in the list has trivial class group, and most of them have Galois group of the Galois closure equal to S_8 or S_9.

- Although the algorithm classifies only primitive fields, every non-primitive field with $|d_K| \leq C(n, r_1, 5)$ appeared in the outputs.

- The groups in the table are presented according to the LMFDB notation: every group is denoted by $n\mathrm{T}q$, where n is the degree of the corresponding field and q is the label of the group as transitive subgroup of S_n: the choice of the label is based upon Hulpke's algorithm for the classification of transitive subgroups of S_n [30]. If the group has an easy form, like the dihedral group D_n or the symmetric group S_n, then the classic name of the group is written together with the LMFDB label.

- The tables shown in the next lines can be found as PARI/GP files at the website **www.mat.unimi.it/users/battistoni/index.html**, together with the programs written by the author and the collection of polynomials found as result of the iterations.

Table 5.3: Number fields $(2,3)$ with $|d_K| \leq 5726301$ (Part 1)

$\lvert d_K\rvert$	Factorization	$f(x)$	G
4286875	$5^4 \cdot 19^3$	$x^8 - 6x^6 - 7x^5 + 8x^4 + 19x^3 + 15x^2 + 6x + 1$	D_8 (8T6)
4296211	$199 \cdot 21589$	$x^8 - 2x^6 - x^5 + 2x^4 + 3x^3 - x - 1$	S_8 (8T50)
4297507	$2011 \cdot 2137$	$x^8 + x^6 - x^3 - x^2 - 1$	S_8 (8T50)
4364587	$29 \cdot 150503$	$x^8 - 6x^6 - 3x^5 + 9x^4 + 5x^3 - 4x^2 - 2x + 1$	S_8 (8T50)
4386467	$41 \cdot 83 \cdot 1289$	$x^8 - x^6 - x^5 + x^4 + 2x^3 - 2x - 1$	S_8 (8T50)
4421387	$1321 \cdot 3347$	$x^8 - 3x^6 - 3x^5 + 2x^4 + 4x^3 + x^2 - 2x - 1$	S_8 (8T50)
4423907	prime	$x^8 - x^7 - 2x^6 + 2x^5 + x^4 - 3x^3 + x^2 + x - 1$	S_8 (8T50)
4456891	prime	$x^8 - 2x^6 - 2x^5 + 2x^4 + 4x^3 + x^2 - 2x - 1$	S_8 (8T50)
4461875	$5^4 \cdot 11^2 \cdot 59$	$x^8 - 2x^7 + 3x^5 - 2x^4 - x^3 + 2x^2 - x - 1$	8T35
4505651	prime	$x^8 - 5x^6 - 3x^5 + 6x^4 + 4x^3 - 3x^2 - 2x + 1$	S_8 (8T50)
4542739	prime	$x^8 - 2x^6 - x^5 + x^4 - x^3 - x^2 + x + 1$	S_8 (8T50)
4570091	$1249 \cdot 3659$	$x^8 - 5x^6 - x^5 + 8x^4 + 3x^3 - 4x^2 - 2x + 1$	S_8 (8T50)
4570723	prime	$x^8 - 2x^6 - x^5 - x^3 + 2x^2 + x - 1$	S_8 (8T50)
4584491	$19 \cdot 101 \cdot 2389$	$x^8 - 4x^6 - 4x^5 + 3x^4 + 6x^3 - x^2 - 3x + 1$	S_8 (8T50)
4596992	$2^8 \cdot 17957$	$x^8 - x^7 + x^6 - 2x^4 + 4x^3 - 4x^2 + 3x - 1$	S_8 (8T50)
4603987	prime	$x^8 - x^7 + 2x^6 - 2x^5 + 4x^4 - 5x^3 + 4x^2 - 3x + 1$	S_8 (8T50)
4614499	prime	$x^8 - 2x^6 - 2x^5 + x^4 + 2x^3 + x^2 - x - 1$	S_8 (8T50)
4616192	$2^{12} \cdot 7^2 \cdot 23$	$x^8 - x^6 - 3x^5 + x^4 + 2x^3 - x^2 + x + 1$	8T35
4623371	$17 \cdot 31^2 \cdot 283$	$x^8 - x^6 - 2x^5 - 2x^4 + 2x^2 + 2x + 1$	S_8 (8T50)
4648192	$2^8 \cdot 67 \cdot 271$	$x^8 - 3x^5 - x^4 + 5x^3 + 2x^2 - 2x - 1$	S_8 (8T50)
4663051	$31 \cdot 359 \cdot 419$	$x^8 - 3x^6 - 3x^5 + 5x^4 + 4x^3 - 3x^2 - x + 1$	S_8 (8T50)
4690927	$443 \cdot 10589$	$x^8 - x^7 + x^6 + 2x^5 - 2x^4 + 2x^2 - x - 1$	S_8 (8T50)
4711123	$43 \cdot 331^2$	$x^8 - 3x^6 - 2x^5 + 3x^4 + 2x^3 - x^2 + 1$	8T44
4725251	$59 \cdot 283^2$	$x^8 - 2x^5 - 5x^4 - 5x^3 - 5x^2 - 2x - 1$	8T44
4761667	$23 \cdot 207029$	$x^8 - 2x^5 - x^4 + 5x^3 - 3x + 1$	S_8 (8T50)
4775363	$1931 \cdot 2473$	$x^8 - 2x^6 - 5x^5 + 9x^4 - 9x^3 + 9x^2 - 5x + 1$	S_8 (8T50)
4785667	$29 \cdot 59 \cdot 2797$	$x^8 - 3x^7 + x^6 + x^5 + 4x^4 - 4x^3 + x^2 - x - 1$	S_8 (8T50)
4809907	$19 \cdot 253153$	$x^8 - x^6 - x^5 + x^4 - x^3 - 2x^2 + x + 1$	S_8 (8T50)
4858379	$17^2 \cdot 16811$	$x^8 - x^7 + 2x^4 - x^3 - 2x^2 + 3x - 1$	S_8 (8T50)
4931267	$11 \cdot 67 \cdot 6691$	$x^8 - x^5 - 4x^4 - 3x^3 + 2x^2 + 3x + 1$	S_8 (8T50)
4960000	$2^8 \cdot 5^4 \cdot 31$	$x^8 - x^7 - x^6 + 3x^5 - x^4 - 3x^3 + 2x^2 - 1$	8T35
5040467	prime	$x^8 - 2x^7 + 4x^5 - 8x^4 + 10x^3 - 7x^2 + 4x - 1$	S_8 (8T50)
5040547	$37 \cdot 59 \cdot 2309$	$x^8 - 13x^6 - x^5 + 61x^4 + 6x^3 - 122x^2 - 8x + 89$	S_8 (8T50)
5103467	prime	$x^8 + x^6 - x^5 + 2x^4 - 4x^3 + 4x^2 - 3x + 1$	S_8 (8T50)
5107019	prime	$x^8 - 2x^6 - x^5 - 2x^4 + x^3 + 3x^2 - 1$	S_8 (8T50)

Table 5.4: Number fields $(2,3)$ with $|d_K| \leq 5726301$ (Part 2)

$\lvert d_K\rvert$	Factorization	$f(x)$	G
5118587	$29 \cdot 176503$	$x^8 - 2x^6 - x^5 + 2x^4 + 2x^3 - 2x - 1$	S_8 (8T50)
5149367	$47 \cdot 331^2$	$x^8 - x^7 - 4x^6 + 6x^5 + 3x^4 - 7x^3 - x^2 + 3x + 1$	8T44
5155867	$449 \cdot 11483$	$x^8 + 6x^6 - 2x^5 + 11x^4 - 7x^3 + 7x^2 - 6x + 1$	S_8 (8T50)
5165819	$641 \cdot 8059$	$x^8 + 2x^6 - 3x^5 + 3x^4 - 7x^3 + 9x^2 - 5x + 1$	S_8 (8T50)
5204491	prime	$x^8 - x^6 - x^5 - 4x^4 + 2x^3 + 5x^2 - 1$	S_8 (8T50)
5233147	prime	$x^8 - x^7 + x^6 - 3x^5 + 7x^4 - 6x^3 + x^2 + 2x - 1$	S_8 (8T50)
5272027	$317 \cdot 16631$	$x^8 - x^7 - x^6 + x^3 + x^2 - x - 1$	S_8 (8T50)
5286727	prime	$x^8 - x^7 - 4x^6 + 3x^5 + 5x^4 - 3x^3 - x^2 + 2x - 1$	S_8 (8T50)
5293867	$227 \cdot 23321$	$x^8 + 3x^6 - x^5 + 2x^4 - 3x^3 - 2x + 1$	S_8 (8T50)
5344939	$521 \cdot 10259$	$x^8 - 3x^6 - 3x^5 + 5x^4 + 6x^3 - 2x^2 - 4x - 1$	S_8 (8T50)
5346947	$839 \cdot 6373$	$x^8 - x^6 - x^5 + 2x^4 - x^3 - 2x^2 + 2x - 1$	S_8 (8T50)
5359051	prime	$x^8 - 4x^6 - 3x^5 + 6x^4 + 7x^3 - x^2 - 4x - 1$	S_8 (8T50)
5365963	$67 \cdot 283^2$	$x^8 - 5x^6 - 2x^5 + 9x^4 + 5x^3 - 5x^2 - 3x - 1$	8T44
5365963	$67 \cdot 283^2$	$x^8 - 2x^6 - x^5 + 3x^4 + 3x^3 - 2x - 1$	8T44
5369375	$5^4 \cdot 11^2 \cdot 71$	$x^8 - 4x^6 - 2x^5 + 7x^4 + 5x^3 - 3x^2 - 4x - 1$	8T35
5371171	$13 \cdot 413167$	$x^8 - x^7 - 3x^6 + 3x^5 + 5x^4 - 4x^3 - 3x^2 + 2x + 1$	S_8 (8T50)
5420747	prime	$x^8 - x^7 - 3x^6 + 5x^5 + 2x^4 - 6x^3 - x^2 + 3x + 1$	S_8 (8T50)
5525731	$17 \cdot 325043$	$x^8 - x^7 - 5x^6 + 4x^5 + 7x^4 - 6x^3 - 12x^2 - 6x - 1$	S_8 (8T50)
5635607	$61 \cdot 92387$	$x^8 - 3x^7 + 6x^6 - 9x^5 + 9x^4 - 9x^3 + 6x^2 - 3x + 1$	S_8 (8T50)
5671691	$193 \cdot 29387$	$x^8 - x^7 - x^5 + 2x^3 + x - 1$	S_8 (8T50)
5697179	prime	$x^8 + 6x^6 - 11x^5 + 14x^4 - 21x^3 + 18x^2 - 7x + 1$	S_8 (8T50)

Table 5.5: Number fields with signature (4,2) with $|d_K| \leq 20829049$ (Part 1)

$\lvert d_K\rvert$	Factorization	$f(x)$	G
15243125	$5^4 \cdot 29^3$	$x^8 - x^6 - 6x^5 + 3x^3 + x^2 + 2x - 1$	8T17
15297613	$37 \cdot 643^2$	$x^8 - 3x^5 - 3x^4 + 3x^3 + 1$	8T44
15908237	$43 \cdot 369959$	$x^8 - 2x^6 - 5x^5 - 11x^4 - 5x^3 - 2x + 1$	S_8 (8T50)
16324589	$149 \cdot 331^2$	$x^8 - 5x^6 - x^5 + 7x^4 + 4x^3 - 2x^2 - 4x - 1$	8T44
16374773	$1753 \cdot 9341$	$x^8 - 4x^6 - 2x^5 + x^4 + 3x^3 + 2x^2 - x + 1$	S_8 (8T50)
16526789	$19 \cdot 607 \cdot 1433$	$x^8 + 2x^6 - x^5 - 7x^4 - 3x^3 + 4x^2 + 4x + 1$	S_8 (8T50)
16623109	prime	$x^8 - 4x^6 - 3x^5 - x^4 + 13x^3 - 6x^2 + 2x - 1$	S_8 (8T50)
16643125	$5^4 \cdot 31 \cdot 859$	$x^8 - 3x^6 - 7x^5 - 7x^4 + 8x^3 + 8x^2 - 2x + 1$	8T47
16706269	$73 \cdot 228853$	$x^8 - 5x^6 - 3x^5 + 5x^4 + 5x^3 - 2x^2 - 3x + 1$	S_8 (8T50)
16877741	prime	$x^8 - 4x^6 - 2x^5 + 5x^4 + 5x^3 - 2x^2 - 3x + 1$	S_8 (8T50)
16981229	$3329 \cdot 5101$	$x^8 - 5x^6 - 4x^5 + 3x^4 + 11x^3 + 11x^2 + 5x + 1$	S_8 (8T50)
17025973	$67 \cdot 254119$	$x^8 - 7x^6 - 6x^5 + 7x^4 + 15x^3 + 11x^2 + 5x + 1$	S_8 (8T50)
17129069	prime	$x^8 - 6x^6 - 5x^5 + 5x^4 + 15x^3 + 14x^2 + 6x + 1$	S_8 (8T50)
17238125	$5^4 \cdot 27581$	$x^8 + 2x^6 - 7x^5 - 16x^4 - 7x^3 - x^2 + 2x + 1$	8T47
17318125	$5^4 \cdot 11^2 \cdot 229$	$x^8 - x^7 - 6x^6 + 6x^5 - 2x^4 + 7x^3 - 6x^2 + 3x - 1$	8T35
17383253	prime	$x^8 - x^6 - x^5 - 2x^4 + x^2 + 2x + 1$	S_8 (8T50)
17592581	$137 \cdot 128413$	$x^8 - 7x^6 - 8x^5 + 3x^4 + 10x^3 + 3x^2 - 2x - 1$	S_8 (8T50)
17712197	prime	$x^8 - 2x^6 - x^5 - x^4 - 3x^3 + 2x^2 + 4x + 1$	S_8 (8T50)
17919197	prime	$x^8 - 4x^6 - 8x^5 - 5x^4 - 5x^3 - 4x^2 + x + 1$	S_8 (8T50)
17949581	$13 \cdot 71 \cdot 19447$	$x^8 - 4x^6 - 8x^5 - 9x^4 - 9x^3 - 11x^2 - 6x - 1$	S_8 (8T50)
18031373	$17 \cdot 71 \cdot 14939$	$x^8 - 7x^6 - x^5 + 8x^4 + 2x^3 - 4x^2 - x + 1$	S_8 (8T50)
18340381	$229 \cdot 283^2$	$x^8 - 4x^6 - x^5 + 5x^4 + x^3 - 4x^2 + 1$	8T44
18416197	prime	$x^8 - 2x^6 - 3x^5 - 11x^4 - 3x^3 + x^2 - 3x + 1$	S_8 (8T50)
18441341	prime	$x^8 - 4x^6 - x^5 - 3x^4 - 11x^3 - 4x^2 + 2x + 1$	S_8 (8T50)
18553789	$59 \cdot 157 \cdot 2003$	$x^8 - 3x^6 + x^4 - 4x^3 + x^2 + 4x + 1$	S_8 (8T50)
18660737	$233 \cdot 283^2$	$x^8 - 3x^6 - 4x^5 + 5x^4 + 4x^3 - 3x^2 + 1$	8T44
19009909	$197 \cdot 96497$	$x^8 - 3x^6 - 3x^5 + 2x^4 + 4x^3 + 2x^2 - x - 1$	S_8 (8T50)
19129013	$131 \cdot 146023$	$x^8 - 6x^6 - 7x^5 + 4x^4 + 19x^3 + 8x^2 - 3x + 1$	S_8 (8T50)
19268125	$5^4 \cdot 30829$	$x^8 - 3x^6 - 3x^5 + 3x^4 + 2x^3 - 2x^2 + 2x + 1$	8T47
19360000	$2^8 \cdot 5^4 \cdot 11^2$	$x^8 - 7x^6 + 8x^4 - 2x^2 + 1$	8T18
19824653	prime	$x^8 - 5x^6 - x^5 + 5x^4 - x^3 - 2x^2 + x + 1$	S_8 (8T50)
19885949	prime	$x^8 - 6x^6 - 3x^5 + 6x^4 + 5x^3 + 5x^2 + 4x + 1$	S_8 (8T50)

Table 5.6: Number fields with signature (4,2) with $|d_K| \leq 20829049$ (Part 2)

$\lvert d_K \rvert$	Factorization	$f(x)$	G
20013373	prime	$x^8 - 6x^6 - 7x^5 - 4x^4 + 3x^3 + 8x^2 + 5x + 1$	S_8 (8T50)
20030653	$37 \cdot 541369$	$x^8 - 6x^6 - 5x^5 + 6x^4 + 7x^3 - 2x^2 - 3x + 1$	S_8 (8T50)
20099501	$31 \cdot 648371$	$x^8 + x^6 - 3x^5 - 8x^4 + x^3 + 4x^2 + 2x + 1$	S_8 (8T50)
20182493	prime	$x^8 - 3x^6 - 4x^5 + x^4 + 5x^3 + 3x^2 - x - 1$	S_8 (8T50)
20262517	$11 \cdot 23 \cdot 283^2$	$x^8 - 5x^6 - 3x^5 + 10x^4 - 2x^3 - 5x^2 + 4x - 1$	8T44
20268125	$5^4 \cdot 32429$	$x^8 - 2x^6 - x^5 + 3x^4 - 9x^3 + 12x^2 - 6x + 1$	8T47
20493125	$5^4 \cdot 32789$	$x^8 - 4x^6 - 5x^5 + 5x^3 + 3x^2 - 1$	8T47
20502784	$2^8 \cdot 283^2$	$x^8 - 7x^6 + 9x^4 - 5x^2 + 1$	8T39
20613077	prime	$x^8 - 5x^6 - x^5 + 2x^4 - 2x^3 + x^2 + 4x + 1$	S_8 (8T50)

Table 5.7: Number fields with signature (6,1) with $|d_K| \leq 79259702$

$\lvert d_K \rvert$	Factorization	$f(x)$	G
65106259	$89 \cdot 731531$	$x^8 - 5x^6 - x^5 + 7x^4 + 4x^3 - 4x^2 - 2x + 1$	S_8 (8T50)
68494627	$811 \cdot 84457$	$x^8 - x^7 - 7x^6 + 5x^5 + 9x^4 - 5x^3 - 4x^2 + 2x + 1$	S_8 (8T50)
68856875	$5^4 \cdot 29^2 \cdot 131$	$x^8 - 9x^6 - 8x^5 + 11x^4 + 21x^3 + 17x^2 + 7x + 1$	8T35
69367411	prime	$x^8 - x^6 - 3x^5 - 3x^4 + 6x^3 + 4x^2 - 2x - 1$	S_8 (8T50)
73061875	$5^4 \cdot 29^2 \cdot 139$	$x^8 - 4x^6 - 3x^4 - 5x^3 + 4x^2 + 5x + 1$	8T35
74671875	$3^4 \cdot 5^6 \cdot 59$	$x^8 - x^7 - 6x^6 + 3x^5 + 9x^4 - 4x^3 - 4x^2 + 2x + 1$	8T27
74906875	$5^4 \cdot 119851$	$x^8 - 3x^6 - 3x^5 + 3x^4 + 7x^3 - 2x^2 - 3x + 1$	8T47
75272867	$31 \cdot 2428157$	$x^8 - x^7 - 5x^6 + 9x^4 + 6x^3 - 5x^2 - 5x - 1$	S_8 (8T50)

Table 5.8: Number fields with signature (1,4) with $|d_K| \leq 39657561$ (Part 1)

$\lvert d_K\rvert$	Factorization	$f(x)$	G
29510281	$101 \cdot 292181$	$x^9 - 3x^7 - x^6 + 7x^5 - 10x^4 + 10x^3 - x^2 - 3x + 1$	S_9 (9T34)
30073129	$353 \cdot 85193$	$x^9 - 5x^7 - x^6 + 13x^5 + 11x^4 - x^3 - 2x^2 + 2x + 1$	S_9 (9T34)
30450401	$31 \cdot 982271$	$x^9 - 4x^7 - 2x^6 + 7x^5 + 3x^4 - 4x^3 - 2x^2 + x + 1$	S_9 (9T34)
30453593	$137 \cdot 222289$	$x^9 - 6x^7 - 4x^6 + 8x^5 + 12x^4 + 10x^3 + 6x^2 + x + 1$	S_9 (9T34)
30544313	$47 \cdot 649879$	$x^9 - 4x^7 - 5x^6 + 5x^5 + 8x^4 + 7x^3 + 5x^2 + x + 1$	S_9 (9T34)
30626693	prime	$x^9 - 2x^7 - 3x^6 + 4x^5 + 13x^4 + 16x^3 + 12x^2 + 5x + 1$	S_9 (9T34)
30861161	prime	$x^9 - 4x^7 - 2x^6 + 20x^5 - 6x^4 - 28x^3 + 26x^2 - 7x + 1$	S_9 (9T34)
31042889	$37 \cdot 47 \cdot 17851$	$x^9 - 6x^7 + 12x^5 + 8x^4 + 12x^3 + 18x^2 + 7x + 1$	S_9 (9T34)
31508353	$359 \cdot 87767$	$x^9 - x^7 - 4x^6 + 5x^5 + 4x^4 - 5x^3 - x^2 + x + 1$	S_9 (9T34)
31638601	prime	$x^9 - 4x^7 - 6x^6 + 2x^5 + 13x^4 + 17x^3 + 12x^2 + 5x + 1$	S_9 (9T34)
31759433	$179 \cdot 177427$	$x^9 - x^6 - x^5 - 2x^4 + 4x^3 + 3x^2 - 4x + 1$	S_9 (9T34)
32029433	prime	$x^9 - 2x^7 - x^6 - x^5 + 4x^4 + 5x^3 - 2x^2 - 2x - 1$	S_9 (9T34)
32031161	$61 \cdot 525101$	$x^9 - 2x^7 - 2x^6 + 9x^5 + 22x^4 + 15x^3 - x^2 - 2x + 1$	S_9 (9T34)
32058553	prime	$x^9 - 3x^7 + 2x^5 + 4x^4 + 10x^3 + 9x^2 + 5x + 1$	S_9 (9T34)
32206049	$23^3 \cdot 2647$	$x^9 - 2x^7 - 2x^6 + 5x^5 + 11x^4 + 12x^3 + 8x^2 + 3x + 1$	9T31
32344469	$53 \cdot 89 \cdot 6857$	$x^9 - 3x^7 - 4x^6 + 2x^5 + 10x^4 + 11x^3 + 8x^2 + 3x + 1$	S_9 (9T34)
32652713	prime	$x^9 - 3x^7 + 5x^5 + 6x^4 - 19x^3 + 15x^2 - 5x + 1$	S_9 (9T34)
32768213	$3413 \cdot 9601$	$x^9 - 3x^7 - 5x^6 + 13x^5 + 4x^4 - 13x^3 + 3x + 1$	S_9 (9T34)
32855993	$113 \cdot 290761$	$x^9 - 7x^6 - 3x^5 + 16x^4 + 19x^3 + 11x^2 + 5x + 1$	S_9 (9T34)
32894473	$17 \cdot 1934969$	$x^9 - x^7 - 2x^6 + 2x^5 + 4x^4 - 2x^3 - 3x^2 + x + 1$	S_9 (9T34)
32923873	$809 \cdot 40697$	$x^9 - 2x^7 + 2x^5 - 3x^4 + 2x^2 + 1$	S_9 (9T34)
32987233	prime	$x^9 - 6x^7 - 7x^6 + 10x^5 + 17x^4 + 13x^3 + 12x^2 + 6x + 1$	S_9 (9T34)
33121433	$1321 \cdot 25073$	$x^9 - 2x^7 - 7x^6 - 2x^5 + 12x^4 + 13x^3 + 6x^2 + 3x + 1$	S_9 (9T34)
33445561	$449 \cdot 74489$	$x^9 - 6x^7 - 3x^6 + 8x^5 + 12x^4 + 9x^3 + 6x^2 + 3x + 1$	S_9 (9T34)
33571261	$43 \cdot 857 \cdot 911$	$x^9 - 6x^7 - x^6 + 12x^5 + 3x^4 - 8x^3 - 2x^2 + x + 1$	S_9 (9T34)
33626161	$23 \cdot 67 \cdot 21821$	$x^9 - 6x^7 + 13x^5 + 2x^4 - 9x^3 - 3x^2 + 2x + 1$	S_9 (9T34)
33860761	$11^2 \cdot 23^4$	$x^9 + 2x^5 + 4x^4 + 4x^3 + 4x^2 + x + 1$	9T30
33984793	prime	$x^9 - 6x^7 - 5x^6 + 7x^5 + 12x^4 + 14x^3 + 13x^2 + 6x + 1$	S_9 (9T34)
34090153	$71 \cdot 480143$	$x^9 - 2x^7 - 2x^6 + 4x^5 - x^4 - x^3 + 2x^2 - x + 1$	S_9 (9T34)
34349041	prime	$x^9 - x^7 + 2x^5 - 2x^3 - x^2 + x + 1$	S_9 (9T34)
34405373	prime	$x^9 - 5x^7 - x^6 + 9x^5 + 4x^4 - 5x^3 - 4x^2 + x + 1$	S_9 (9T34)
34573709	prime	$x^9 - x^7 - 5x^6 - 8x^5 + 4x^4 + 15x^3 + 14x^2 + 6x + 1$	S_9 (9T34)
34590113	$509 \cdot 67957$	$x^9 + x^7 - 3x^5 + 3x^4 + 9x^3 + 7x^2 + 4x + 1$	S_9 (9T34)
34628113	$13 \cdot 2663701$	$x^9 - 3x^7 - 4x^6 - x^5 + 3x^4 + 11x^3 + 13x^2 + 6x + 1$	S_9 (9T34)

Table 5.9: Number fields with signature (1,4) with $|d_K| \leq 39657561$ (Part 2)

$\lvert d_K\rvert$	Factorization	$f(x)$	G
35028793	$23^3 \cdot 2879$	$x^9 - 3x^7 - 6x^6 + 2x^5 + 11x^4 + 10x^3 + 7x^2 + 4x + 1$	9T31
35050633	$43 \cdot 311 \cdot 2621$	$x^9 - x^7 - 2x^6 - 6x^5 + 4x^4 + 20x^3 + 19x^2 + 7x + 1$	S_9 (9T34)
35051893	$109 \cdot 321577$	$x^9 - 3x^7 - 5x^6 - x^5 + 7x^4 + 13x^3 + 11x^2 + 5x + 1$	S_9 (9T34)
35234033	$59 \cdot 347 \cdot 1721$	$x^9 - 3x^7 - 4x^6 - x^5 + 7x^4 + 16x^3 + 15x^2 + 5x + 1$	S_9 (9T34)
35357129	$41 \cdot 862369$	$x^9 + 2x^7 - 8x^6 + 7x^5 - 8x^4 + 6x^3 + 1$	S_9 (9T34)
35607973	$5501 \cdot 6473$	$x^9 - 4x^7 - 2x^6 + 6x^5 + 12x^4 - 26x^3 + 19x^2 - 6x + 1$	S_9 (9T34)
35666053	$787 \cdot 45319$	$x^9 - 6x^7 - x^6 + 12x^5 + 14x^4 + 9x^3 + 7x^2 + 4x + 1$	S_9 (9T34)
35678113	$199 \cdot 179287$	$x^9 - 3x^7 - 8x^6 + 4x^5 + 19x^4 + 15x^3 + 2x^2 - 2x + 1$	S_9 (9T34)
35686793	prime	$x^9 - 5x^7 - 6x^6 + 3x^5 + 15x^4 + 17x^3 + 11x^2 + 4x + 1$	S_9 (9T34)
35935321	$29 \cdot 337 \cdot 3677$	$x^9 - 4x^7 - 2x^6 + 5x^5 + 6x^4 - 2x^3 - 4x^2 + 1$	S_9 (9T34)
36055441	$41 \cdot 879401$	$x^9 - 2x^7 - x^6 + 11x^5 + 20x^4 + 15x^3 + x^2 - 3x + 1$	S_9 (9T34)
36155633	prime	$x^9 + x^7 - x^6 - x^3 + x^2 - x + 1$	S_9 (9T34)
36722413	$7^2 \cdot 13 \cdot 57649$	$x^9 - x^7 - x^6 - 7x^5 + 15x^4 - 13x^3 + 9x^2 - 3x + 1$	S_9 (9T34)
36743849	$37 \cdot 71^2 \cdot 197$	$x^9 + x^7 - x^6 + 3x^5 + 6x^4 + 2x^3 + 3x^2 + x + 1$	S_9 (9T34)
37009129	$839 \cdot 44111$	$x^9 + 4x^7 + 2x^5 + 4x^4 - 2x^3 + 10x^2 - 3x + 1$	S_9 (9T34)
37065113	$5849 \cdot 6337$	$x^9 - 4x^7 - 6x^6 + 4x^5 + 19x^4 + 24x^3 + 16x^2 + 6x + 1$	S_9 (9T34)
37086373	$23 \cdot 1612451$	$x^9 + x^7 - x^3 - x + 1$	S_9 (9T34)
37232393	$11 \cdot 157 \cdot 21559$	$x^9 - 5x^7 - x^6 + 6x^5 + 9x^4 + 11x^3 + 10x^2 + 5x + 1$	S_9 (9T34)
37354501	prime	$x^9 - 3x^7 - 3x^6 + 4x^5 + 8x^4 + 3x^3 - 4x^2 - 4x - 1$	S_9 (9T34)
37732753	prime	$x^9 - x^7 + 3x^5 - 4x^4 + x^3 + 3x^2 - 3x + 1$	S_9 (9T34)
38114257	$457 \cdot 83401$	$x^9 - 5x^7 + 7x^5 - x^3 - x^2 - x + 1$	S_9 (9T34)
38118173	$967 \cdot 39419$	$x^9 - 2x^7 - 5x^6 - 5x^5 + 8x^4 + 20x^3 + 18x^2 + 7x + 1$	S_9 (9T34)
38159713	$17 \cdot 2244689$	$x^9 - 3x^7 - 2x^6 + 7x^5 + 6x^4 - 12x^3 + 5x^2 - 2x + 1$	S_9 (9T34)
38525297	prime	$x^9 - 4x^7 - 4x^6 + 2x^5 + 9x^4 + 10x^3 + 7x^2 + 3x + 1$	S_9 (9T34)
38577961	$19 \cdot 2030419$	$x^9 - 4x^7 - 2x^6 + 3x^5 + 3x^4 + 4x^3 + 4x^2 + 3x + 1$	S_9 (9T34)
38600453	$1847 \cdot 20899$	$x^9 - 3x^7 - x^6 + 7x^5 + x^4 - 7x^3 - x^2 + 3x + 1$	S_9 (9T34)
38709673	prime	$x^9 - 2x^7 - 7x^6 + 14x^5 + x^4 - 15x^3 + 14x^2 - 6x + 1$	S_9 (9T34)
38817673	$31^3 \cdot 1303$	$x^9 - 6x^7 - x^6 + 15x^5 - 16x^4 + 17x^3 + 19x^2 + 7x + 1$	9T31
39067993	prime	$x^9 - 3x^7 - 3x^6 - 4x^5 + 3x^4 + 14x^3 + 14x^2 + 6x + 1$	S_9 (9T34)
39319073	$127 \cdot 309599$	$x^9 - 6x^7 - 6x^6 + 8x^5 + 17x^4 + 12x^3 + 6x^2 + 4x + 1$	S_9 (9T34)
39382961	prime	$x^9 - 4x^7 - 2x^6 + 7x^5 + 5x^4 - 4x^3 - 4x^2 + x + 1$	S_9 (9T34)
39388441	$1093 \cdot 36037$	$x^9 - 5x^7 - 4x^6 + 12x^5 + 21x^4 + 10x^3 - 3x^2 - 2x + 1$	S_9 (9T34)
39655225	$5^2 \cdot 1586209$	$x^9 - 6x^7 - 3x^6 + 5x^5 + 24x^4 + 17x^3 + 11x^2 + 3x + 1$	S_9 (9T34)

Table 5.10: Number fields with signature (3,3) with $|d_K| \leq 146723910$ (Part 1)

$\lvert d_K\rvert$	Factorization	$f(x)$	G
109880167	$367 \cdot 299401$	$x^9 - 5x^7 - 4x^6 + 3x^5 + 11x^4 + 13x^3 + 7x^2 + 4x + 1$	S_9 (9T34)
110852311	$31^3 \cdot 61^2$	$x^9 + x^7 - 3x^6 - 10x^5 + 5x^4 + 9x^3 - 2x^2 - x + 1$	9T20
111543479	prime	$x^9 - 6x^7 - 4x^6 + 14x^5 + 26x^4 + 12x^3 - 2x^2 + x + 1$	S_9 (9T34)
112700719	$7211 \cdot 15629$	$x^9 - 5x^7 - 8x^6 + 2x^5 + 20x^4 + 26x^3 + 17x^2 + 5x + 1$	S_9 (9T34)
112978759	$43 \cdot 2627413$	$x^9 - 4x^7 - 8x^6 + 4x^5 + 30x^4 - 28x^3 + 3x + 1$	S_9 (9T34)
112992391	prime	$x^9 - 7x^7 - 2x^6 + 13x^5 + 13x^4 - 2x^3 - 9x^2 - 5x - 1$	S_9 (9T34)
113501567	$53 \cdot 797 \cdot 2687$	$x^9 - 6x^7 - 3x^6 + 5x^5 + 4x^4 + x^3 - 2x^2 - 2x + 1$	S_9 (9T34)
113511599	$193 \cdot 727 \cdot 809$	$x^9 - 6x^7 - 9x^6 + 8x^5 + 22x^4 + 25x^3 + 22x^2 + 7x + 1$	S_9 (9T34)
113931487	$109 \cdot 389 \cdot 2687$	$x^9 - 4x^7 - 11x^6 - 9x^5 + x^4 - 2x^3 - 7x^2 - x + 1$	S_9 (9T34)
114479303	$23^3 \cdot 97^2$	$x^9 - 4x^7 - x^5 - 6x^4 + 2x^3 + 6x^2 + 2x + 1$	9T20
114807607	$29 \cdot 3958883$	$x^9 - 5x^7 - 3x^6 + 25x^5 - 31x^4 + 5x^3 + 8x^2 - 2x + 1$	S_9 (9T34)
115041127	$97 \cdot 229 \cdot 5179$	$x^9 - 5x^7 - 2x^6 + 14x^5 + x^4 - 9x^3 + 1$	S_9 (9T34)
115270559	$71 \cdot 79 \cdot 20551$	$x^9 - 7x^7 - x^6 + 14x^5 + 2x^4 - 9x^3 - x^2 + x + 1$	S_9 (9T34)
115691111	$47 \cdot 67 \cdot 36739$	$x^9 - 5x^7 - 4x^6 + x^5 + 5x^4 + 6x^3 - x^2 - 3x + 1$	S_9 (9T34)
116188367	prime	$x^9 - 6x^7 - x^6 + 12x^5 + 5x^4 - 9x^3 - 4x^2 + 2x + 1$	S_9 (9T34)
116817671	$53 \cdot 2204107$	$x^9 - 4x^7 - x^6 - 7x^5 + 26x^4 - 29x^3 + 18x^2 - 6x + 1$	S_9 (9T34)
117283087	prime	$x^9 - 5x^7 - 2x^6 + 8x^5 + 6x^4 - 4x^3 - 5x^2 + x + 1$	S_9 (9T34)
118246927	$31 \cdot 3814417$	$x^9 - 6x^7 - 5x^6 + 3x^5 + 4x^4 + 9x^3 + 12x^2 + 6x + 1$	S_9 (9T34)
118347967	$479 \cdot 247073$	$x^9 - 5x^7 - 4x^6 + 20x^5 - 15x^4 + 8x^3 - 5x^2 + 1$	S_9 (9T34)
118357559	$769 \cdot 153911$	$x^9 - 7x^7 - 3x^6 + 8x^5 + 13x^4 + 17x^3 + 10x^2 + 3x + 1$	S_9 (9T34)
118434167	$31 \cdot 3820457$	$x^9 - 7x^7 - 9x^6 + 9x^5 + 31x^4 + 20x^3 - 3x^2 - 2x + 1$	S_9 (9T34)
118795951	$167 \cdot 711353$	$x^9 - 6x^7 - x^6 + 13x^5 + 3x^4 - 12x^3 - 3x^2 + 3x + 1$	S_9 (9T34)
119070383	$53 \cdot 1327 \cdot 1693$	$x^9 + 3x^7 - 7x^6 - 2x^5 - 12x^4 + 5x^3 + 7x^2 + 5x + 1$	S_9 (9T34)
119278283	prime	$x^9 - 6x^7 - 8x^6 + x^5 + 15x^4 + 19x^3 + 13x^2 + 5x + 1$	S_9 (9T34)
119747759	$557 \cdot 214987$	$x^9 - 5x^7 - x^6 + 10x^5 + 3x^4 - 8x^3 - 4x^2 + 2x + 1$	S_9 (9T34)
119783879	$101 \cdot 1185979$	$x^9 - 3x^7 - 12x^6 - 18x^5 - 13x^4 - 2x^3 + 5x^2 + 4x + 1$	S_9 (9T34)
120155887	$23 \cdot 5224169$	$x^9 - 2x^7 - x^6 - 2x^5 + x^4 + 5x^3 - x^2 - x + 1$	S_9 (9T34)
120802519	prime	$x^9 - 7x^7 + 16x^5 - 10x^4 - 12x^3 + 17x^2 - 7x + 1$	S_9 (9T34)
121463543	prime	$x^9 - 2x^7 - 2x^6 + 7x^5 + 4x^4 - 15x^3 + 13x^2 - 6x + 1$	S_9 (9T34)
121510799	$2207 \cdot 55057$	$x^9 - 4x^7 - 12x^6 - 13x^5 - 2x^4 + 11x^3 + 13x^2 + 6x + 1$	S_9 (9T34)
122317991	$19^2 \cdot 79 \cdot 4289$	$x^9 - 6x^7 - 3x^6 + 6x^5 + 5x^4 + 9x^3 + 12x^2 + 6x + 1$	S_9 (9T34)
122854967	prime	$x^9 - 4x^7 - 6x^6 + x^5 + 10x^4 + 13x^3 + 9x^2 + 4x + 1$	S_9 (9T34)
122933791	$149 \cdot 825059$	$x^9 - x^7 - x^6 - 8x^5 + 10x^4 + x^3 - x^2 - 3x + 1$	S_9 (9T34)
123301207	$379 \cdot 325333$	$x^9 - 4x^7 + 2x^5 - 2x^4 + 2x^2 + x + 1$	S_9 (9T34)

Table 5.11: Number fields with signature (3,3) with $|d_K| \leq 146723910$ (part 2)

$\lvert d_K\rvert$	Factorization	$f(x)$	G
123396607	prime	$x^9 - 3x^7 - 4x^6 + 5x^5 + 6x^4 - 4x^3 - 3x^2 + 2x + 1$	S_9 (9T34)
123595631	$43 \cdot 2874317$	$x^9 - 6x^7 - 3x^6 + 13x^5 + 3x^4 - 22x^3 + 19x^2 - 7x + 1$	S_9 (9T34)
123636223	$17^2 \cdot 43 \cdot 9949$	$x^9 - 4x^7 - x^5 - 2x^4 + 9x^3 + 9x^2 + 4x + 1$	S_9 (9T34)
123668767	prime	$x^9 - 6x^7 - 8x^6 + 6x^5 + 31x^4 - 2x^3 + 21x^2 - 7x + 1$	S_9 (9T34)
123972119	prime	$x^9 - 6x^7 - 5x^6 + 3x^5 + 16x^4 + 25x^3 + 19x^2 + 7x + 1$	S_9 (9T34)
124007591	prime	$x^9 - x^7 - 2x^6 - 2x^5 + 3x^4 + 3x^3 - 2x^2 + 1$	S_9 (9T34)
124683371	prime	$x^9 - 6x^7 + 12x^5 + 2x^4 - 10x^3 - 3x^2 + 2x + 1$	S_9 (9T34)
124885927	$17 \cdot 7346231$	$x^9 - 6x^7 - 2x^6 + 9x^5 + 4x^4 - 5x^3 - 3x^2 + 1$	S_9 (9T34)
125535947	prime	$x^9 - x^7 - 7x^6 + 2x^5 + 8x^4 - 11x^3 + 10x^2 - 4x + 1$	S_9 (9T34)
125785223	$1013 \cdot 124171$	$x^9 - x^7 - 2x^6 - 4x^5 + 2x^4 + 6x^3 - x^2 - 3x + 1$	S_9 (9T34)
126100423	prime	$x^9 - 6x^7 - 10x^6 + 6x^5 + 28x^4 + 22x^3 + 8x^2 + 3x + 1$	S_9 (9T34)
126180871	$103 \cdot 569 \cdot 2153$	$x^9 - 6x^6 + 8x^5 + 17x^4 - 24x^3 + 3x^2 + x + 1$	S_9 (9T34)
126591211	prime	$x^9 - 4x^7 - x^6 + 4x^5 + 2x^4 + x^3 - x^2 - 2x + 1$	S_9 (9T34)
128374559	prime	$x^9 + x^7 - x^6 - 3x^5 - x^4 - x^3 + 2x + 1$	S_9 (9T34)
128467639	$131 \cdot 389 \cdot 2521$	$x^9 - 6x^7 - x^6 + 12x^5 + 4x^4 - 9x^3 - 4x^2 + x + 1$	S_9 (9T34)
128607823	$73 \cdot 1761751$	$x^9 - 2x^6 + 7x^4 - 8x^3 + 6x^2 - 4x + 1$	S_9 (9T34)
128781847	$983 \cdot 131009$	$x^9 - 5x^7 - x^6 + 8x^5 - 7x^3 + x^2 + 3x - 1$	S_9 (9T34)
128886647	prime	$x^9 + 4x^7 - 5x^6 - 11x^5 + 9x^4 + 7x^3 - 5x^2 - 2x + 1$	S_9 (9T34)
128892887	$43 \cdot 2997509$	$x^9 - 4x^7 - x^6 + 3x^5 + x^3 - 2x + 1$	S_9 (9T34)
128897287	$31 \cdot 719 \cdot 5783$	$x^9 - 4x^7 - 3x^6 + 6x^5 + 6x^4 - 3x^3 - 4x^2 + x + 1$	S_9 (9T34)
129079703	$23^3 \cdot 103^2$	$x^9 + 4x^7 - 9x^6 - 3x^5 + 6x^4 + x^3 + 2x^2 - 4x + 1$	9T20
129324487	$251 \cdot 515237$	$x^9 - 6x^7 - x^6 - 2x^5 + 19x^4 - 17x^3 + 5x^2 - x + 1$	S_9 (9T34)
129969659	prime	$x^9 - 6x^7 - 5x^6 + 4x^5 + 13x^4 + 12x^3 + 6x^2 + 3x + 1$	S_9 (9T34)
130251959	prime	$x^9 - 3x^7 - 6x^6 + 3x^5 + 8x^4 - x^3 - 3x^2 - x + 1$	S_9 (9T34)
130509671	prime	$x^9 - 6x^7 - 2x^6 + 12x^5 + 3x^4 - 9x^3 - 2x^2 + 3x + 1$	S_9 (9T34)
130531031	$3581 \cdot 36451$	$x^9 - 4x^6 - 6x^5 - 6x^4 - 4x^3 + x + 1$	S_9 (9T34)
130534871	$1361 \cdot 95911$	$x^9 - 2x^7 - 4x^6 + 2x^5 + 8x^4 - 2x^3 - 4x^2 + x + 1$	S_9 (9T34)
131123051	prime	$x^9 - 2x^7 - 5x^6 - 2x^5 + 6x^4 + 13x^3 + 13x^2 + 6x + 1$	S_9 (9T34)
131352751	$439 \cdot 547^2$	$x^9 - 6x^7 - 8x^6 - 2x^5 + 9x^4 + 16x^3 + 12x^2 + 6x + 1$	S_9 (9T34)
131662151	prime	$x^9 - 6x^7 - 7x^6 + 9x^5 + 24x^4 + 12x^3 + x^2 + 2x + 1$	S_9 (9T34)
131763119	$19 \cdot 6934901$	$x^9 - 3x^7 - 5x^6 + 4x^5 + 9x^4 + 2x^3 - 4x^2 - 4x - 1$	S_9 (9T34)
131768803	$37 \cdot 139 \cdot 25621$	$x^9 - 4x^7 - x^6 + 2x^5 + 6x^4 - 11x^3 + 9x^2 - 4x + 1$	S_9 (9T34)
131820967	prime	$x^9 - 4x^7 - 6x^6 + 25x^5 - 16x^4 - 3x^3 - x^2 + 2x + 1$	S_9 (9T34)
131855239	$137 \cdot 962447$	$x^9 + x^7 - 4x^6 + 3x^5 - 2x^4 + 5x^3 - x^2 - 3x + 1$	S_9 (9T34)

Table 5.12: Number fields with signature (3,3) with $|d_K| \leq 146723910$ (part 3)

$\lvert d_K\rvert$	Factorization	$f(x)$	G
132067367	$89 \cdot 1483903$	$x^9 - 6x^7 - 3x^6 + 5x^5 + 8x^4 + 16x^3 + 15x^2 + 6x + 1$	S_9 (9T34)
132611207	$1061 \cdot 124987$	$x^9 - 6x^7 - 6x^6 + x^5 + 10x^4 + 20x^3 + 16x^2 + 6x + 1$	S_9 (9T34)
132667183	$11^2 \cdot 1096423$	$x^9 - 7x^7 + 12x^5 - 4x^4 - 10x^3 + 11x^2 - 5x + 1$	S_9 (9T34)
133731799	$31^3 \cdot 67^2$	$x^9 - 7x^7 - 2x^6 + 3x^5 + 18x^4 + 21x^3 - x^2 - 3x + 1$	9T20
133962263	$181 \cdot 740123$	$x^9 - 7x^7 - x^6 + 7x^5 + 10x^4 + 14x^3 + 11x^2 + 5x + 1$	S_9 (9T34)
134479871	prime	$x^9 - 6x^7 - 3x^6 + 5x^5 + 10x^4 + 11x^3 + 8x^2 + 4x + 1$	S_9 (9T34)
135394019	$19 \cdot 31 \cdot 457 \cdot 503$	$x^9 - 6x^7 + 13x^5 + x^4 - 11x^3 - 3x^2 + 3x + 1$	S_9 (9T34)
135714671	$9011 \cdot 15061$	$x^9 - 7x^7 - 4x^6 + 10x^5 + 6x^4 - 6x^3 - 3x^2 + x + 1$	S_9 (9T34)
136007191	$17 \cdot 139 \cdot 57557$	$x^9 - 5x^7 - 4x^6 - 8x^5 - 18x^4 - 4x^3 + 7x^2 + x + 1$	S_9 (9T34)
136388159	$397 \cdot 343547$	$x^9 - 7x^7 - 5x^6 + 9x^5 + 19x^4 + 21x^3 + 14x^2 + 6x + 1$	S_9 (9T34)
136479463	$43 \cdot 107 \cdot 29663$	$x^9 - 6x^7 + 9x^5 + 2x^4 - 6x^3 - 2x^2 + 2x + 1$	S_9 (9T34)
136494559	prime	$x^9 - 5x^7 - 9x^6 - 10x^5 - 4x^4 + x^3 + x^2 + x - 1$	S_9 (9T34)
137049967	$8971 \cdot 15277$	$x^9 - 6x^7 - 8x^6 + 4x^5 + 25x^4 + 28x^3 + 12x^2 + 4x + 1$	S_9 (9T34)
137297807	$41 \cdot 67 \cdot 151 \cdot 331$	$x^9 - 5x^7 - 2x^6 + 9x^5 + 2x^4 - 8x^3 - x^2 + 2x + 1$	S_9 (9T34)
137310031	$137 \cdot 1002263$	$x^9 - 6x^7 - 4x^6 - 2x^5 - 13x^4 - 6x^3 + x^2 - x + 1$	S_9 (9T34)
137664647	prime	$x^9 - 6x^7 - 4x^6 - x^5 - 11x^4 - 16x^3 - 6x^2 + x + 1$	S_9 (9T34)
138028087	$83 \cdot 149 \cdot 11161$	$x^9 - 7x^7 - 12x^6 + 4x^5 + 37x^4 + 2x^3 + 11x^2 + 6x + 1$	S_9 (9T34)
138182311	prime	$x^9 - 3x^7 - 11x^6 - 17x^5 - 15x^4 - 6x^3 + x^2 + 2x + 1$	S_9 (9T34)
138260071	$211 \cdot 655261$	$x^9 - x^7 - 3x^6 + 7x^5 - 9x^4 - 3x^3 + 12x^2 - 4x + 1$	S_9 (9T34)
138370051	prime	$x^9 - 6x^7 - x^6 + 12x^5 + 5x^4 - 8x^3 - 6x^2 + x + 1$	S_9 (9T34)
138455407	$181 \cdot 764947$	$x^9 - 3x^7 - 10x^6 - 17x^5 - 14x^4 - 3x^3 + x^2 + x + 1$	S_9 (9T34)
138616811	prime	$x^9 - 7x^7 - 3x^6 + 7x^5 + 4x^4 - 3x^3 - 2x^2 + x + 1$	S_9 (9T34)
138975227	prime	$x^9 - 5x^7 + 6x^5 - 2x^4 + 2x^2 - 2x + 1$	S_9 (9T34)
139751219	prime	$x^9 - 4x^7 - 4x^6 + 29x^5 - 35x^4 + 13x^3 + 5x^2 - 5x + 1$	S_9 (9T34)
140598959	$17 \cdot 8270527$	$x^9 - 7x^7 - 5x^6 + 9x^5 + 9x^4 - 2x^3 - 5x^2 + 1$	S_9 (9T34)
140860891	prime	$x^9 - x^7 - 3x^6 + 3x^5 + 5x^4 - 3x^3 - 3x^2 - x + 1$	S_9 (9T34)
141056039	$43 \cdot 3280373$	$x^9 - 2x^7 - 3x^6 + 5x^5 + 3x^4 - 6x^3 - x^2 + 3x + 1$	S_9 (9T34)
141951959	prime	$x^9 - 3x^7 - 6x^6 + 18x^5 - 17x^4 + 7x^3 - 2x^2 + 1$	S_9 (9T34)
142325111	$607 \cdot 234473$	$x^9 - 6x^7 + 18x^5 - 3x^4 - 28x^3 + 23x^2 - 7x + 1$	S_9 (9T34)
142603319	prime	$x^9 - 5x^7 - 12x^6 - 7x^5 + 9x^4 + 21x^3 + 17x^2 + 6x + 1$	S_9 (9T34)
142625663	prime	$x^9 - 7x^7 - 2x^6 + 11x^5 - 6x^4 - 13x^3 + x^2 - x - 1$	S_9 (9T34)
142989047	$2281 \cdot 62687$	$x^9 - 4x^7 - 4x^6 + 2x^5 + 5x^4 + 6x^3 + 8x^2 + 4x + 1$	S_9 (9T34)
142989047	$2281 \cdot 62687$	$x^9 - 6x^7 - 9x^6 - 2x^5 + 21x^4 + 35x^3 + 23x^2 + 7x + 1$	S_9 (9T34)
143233399	$79 \cdot 1813081$	$x^9 - 5x^7 + 9x^5 + x^4 - 7x^3 - 3x^2 + 2x + 1$	S_9 (9T34)

Table 5.13: Number fields with signature (3,3) with $|d_K| \leq 146723910$ (part 4)

$\lvert d_K \rvert$	Factorization	$f(x)$	G
143332487	$37 \cdot 149 \cdot 25999$	$x^9 - 3x^7 - x^6 + 5x^5 + x^4 - 5x^3 - 2x^2 + 2x + 1$	S_9 (9T34)
143421247	prime	$x^9 - 6x^7 - 3x^6 + 14x^5 + 9x^4 - 11x^3 - 7x^2 + x + 1$	S_9 (9T34)
143792279	$3203 \cdot 44893$	$x^9 - 6x^7 + 12x^5 + x^4 - 8x^3 - 3x^2 + x + 1$	S_9 (9T34)
143859223	$4139 \cdot 34757$	$x^9 - 5x^7 + 9x^5 - 2x^4 - 8x^3 + 6x^2 - 3x + 1$	S_9 (9T34)
144146159	prime	$x^9 - 4x^7 - 11x^6 - 2x^5 + 38x^4 + 37x^3 + 2x^2 - 3x + 1$	S_9 (9T34)
144211751	$29 \cdot 2221 \cdot 2239$	$x^9 - 7x^7 + 2x^5 + 11x^4 - 14x^3 + 9x^2 - 4x + 1$	S_9 (9T34)
144417311	prime	$x^9 - 6x^7 + 9x^5 + 9x^4 - 10x^3 - 4x^2 - x + 1$	S_9 (9T34)
144895087	$10343 \cdot 14009$	$x^9 - 7x^7 - 11x^6 + 6x^5 + 31x^4 + 28x^3 + 8x^2 + 2x + 1$	S_9 (9T34)
144992879	$9613 \cdot 15083$	$x^9 + 4x^7 - 3x^6 + 2x^5 + 7x^4 - 23x^3 + 19x^2 - 7x + 1$	S_9 (9T34)
145289047	$37 \cdot 3926731$	$x^9 - 7x^7 - 6x^6 + 9x^5 + 12x^4 + x^3 - x^2 + 3x + 1$	S_9 (9T34)
145630367	prime	$x^9 - 5x^7 - 6x^6 - 7x^5 + 3x^4 - 7x^3 + 5x^2 - 2x + 1$	S_9 (9T34)
145849303	$109 \cdot 163 \cdot 8209$	$x^9 - 4x^7 - 3x^6 + 3x^5 + 4x^4 + x^3 - 3x^2 - x + 1$	S_9 (9T34)
145894103	$19 \cdot 7678637$	$x^9 - 7x^7 - 8x^6 + 10x^5 + 11x^4 - 6x^3 - 5x^2 + 2x + 1$	S_9 (9T34)
146063111	$29 \cdot 241 \cdot 20899$	$x^9 + 2x^7 - 11x^6 - x^5 - 4x^4 - 5x^3 + 8x^2 - 4x + 1$	S_9 (9T34)

Chapter 6

Classification of number fields via regulators

6.1 Analytic lower bounds for the regulator

6.1.1 Applying Friedman's explicit formula

In the previous chapter we studied the problem of minimum discriminants for number fields of given signature. Now, we turn our attention to a similar problem, which is to study and determine the number fields of given signature with regulator less than a given upper bound.
Let K be a number field of degree n and signature (r_1, r_2). In Chapter 4 we have presented Friedman's explicit formula (4.10), which express the regulator R_K as a series of an integral function over the ideals in two given classes of $\mathcal{O}_K$. In fact one has

$$\frac{R_K}{w_K} = \sum_{\mathfrak{a}} g_{r_1,r_2}\left(\frac{\mathrm{N}(\mathfrak{a})^2}{|d_K|}\right) + \sum_{\mathfrak{b}} g_{r_1,r_2}\left(\frac{\mathrm{N}(\mathfrak{b})^2}{|d_K|}\right) \tag{6.1}$$

where $\mathfrak{a}$ is the class of principal ideals of $\mathcal{O}_K$, $\mathfrak{b}$ is the class of ideals equivalent in Cl_K to the different ideal ∂_K and $g : (0, +\infty) \to \mathbb{R}$ is the smooth function depending on the signature given by the absolutely convergent integral

$$g_{r_1,r_2}(x) := \frac{1}{2^{r_1} 4\pi i} \int_{2-i\infty}^{2+i\infty} (\pi^n 4^{r_2} \cdot x)^{-s/2} \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} (2s-1) \mathrm{d}s.$$

As usual for this kind of problems, we would like to obtain an estimate of the invariant defined in Formula (6.1) (the regulator in this case) by means of the analytic object related to it (the series): in particular, one would like to detect an unbounded range $(a, +\infty)$ with $a > 0$ such that the function g is positive on that interval, in order to discard infinitely many terms of the series and obtaining a lower bound $R_K/w_K > \sum_{\mathfrak{J}} g(\mathrm{N}(\mathfrak{J})^2/|d_K|)$, where the last sum is finite.
The main properties of the function g were described by Friedman thanks to the concept of "total positivity".

Lemma 6. *Let $g := g_{r_1,r_2}$ be the function defined as above. Then it satisfies the following properties:*

- *g has a unique zero $x_0 \in (0, +\infty)$, $g(x) < 0$ for $x < x_0$ and $g(x) > 0$ for $x > x_0$.*
- *g has a unique critical point $x_1 \in (0, +\infty)$, which is a maximum point.*
- *For each open interval $(a, b) \subset (0, +\infty)$ and for every $x \in (a, b)$ one has $g(x) > min(g(a), g(b))$.*
- *For each ideal $\mathfrak{I}$ either principal or equivalent to ∂_K and such that $\mathrm{N}(\mathfrak{I}) \ll |d_K|$, the corresponding term in the series (6.1) is bounded up to constants by*

$$\exp(-n\pi(\mathrm{N}(\mathfrak{I})/\sqrt{|d_K|})^{2/n}) \cdot (\mathrm{N}(\mathfrak{I})/\sqrt{|d_K|})^{(3-r_1-r_2)/n}.$$

Proof. The first two points are proved in Friedman's dedicated paper [23] relying on the theory of Total Positivity presented by Karlin in his book [35].
The third point is a straightforward corollary of the two previous results.
The fourth one is actually an older statement, proved by Friedman in [22], and which is crucial in the numerical computation of the function g. □

In the following proposition, proved in [22], we give the numerical formula which allows to compute values of $g(x)$ with good accuracy.

Proposition 10. *One has $g(x) = 2^{-r_1}(2\sqrt{\pi})^{-r_2}F(x)$ where $F(x)$ is a suitable integral function such that for every $M \in \mathbb{N}$ it satisfies the bound*

$$\left| F(x) - \sum_{m=0}^{2M+1} x^m \sum_{l=0}^{L(m)} (-2\log x)^l \frac{A\left(\frac{m}{2}, l+1\right)}{l!} \right| < 4(M+1)\left(\frac{5}{M!}\right)^n x^{2M+1.5}$$

where $L(m) := r_1 + r_2 - 1$ if m is even, $L(m) = r_2 - 1$ if m is odd, and the coefficients $A(m/2, l+1)$ are the ones appearing in the Laurent series expansion

$$\Gamma(s)^{r_1+r_2}\Gamma\left(\frac{s}{2}\right)^{r_2}(4s-1) = \sum_{l=1}^{N(i)} \frac{A(i,l)}{(s+i)^l} + h(s)$$

where h is a function holomorphic at $s = -i$ and $N(i) := L(i) + 1$.

The properties presented in Lemma 6 are strong enough to give consistent lower bounds for the regulator R_K: in fact, being the trivial ideal $\mathcal{O}_K$ a principal ideal, it is enough to prove that $g(1/|d_K|) > 0$, so that any other term in the series (6.1) is positive and one obtains the easy lower bound $R_K \geq w_K g(1/|d_K|)$.
In the series (6.1) there are always the terms corresponding to the principal ideals $n\mathcal{O}_K$ with $n \in \mathbb{N}$: thus, if $g(1/|d_K|) < 0$, one can look for the minimum value n such that $g(n^{2[K.\mathbb{Q}]}/|d_K|) > 0$ and try to see if the sum over every ideal of norm less than a bound

not too much larger than $n^{2[K:\mathbb{Q}]}$ provides a positive lower bound for the function g: this setting requires an adaptation which will not be discussed here, but it can be found with every detail in [3].

Now, remember that the number of roots of unity w_K is always greater or equal than 2, and it is indeed equal to 2 for every number field K which is not totally complex. This fact, together with the previous considerations, yields the following result.

Proposition 11. *Let K be a number field of degree n and signature (r_1, r_2), and let $R_0 > 0$. Assume $d_1 < |d_K| < d_2$ and that $2g(1/d_1) > R_0$, $2g(1/d_2) > R_0$. Then*

$$R_K \geq 2g\left(\frac{1}{|d_K|}\right) \geq 2\min\left(g\left(\frac{1}{d_1}\right), g\left(\frac{1}{d_2}\right)\right) > R_0. \tag{6.2}$$

Moreover, if one knows that the different ∂_K is principal, then any factor 2 in the hypotheses and in the above inequalities can be replaced by a factor 4.

The last proposition provides us an interesting information: if we want to look for a range of discriminants $[d_1, d_2]$ such that any number field with fixed signature and $|d_K| \in [d_1, d_2]$ has regulator greater than a given lower bound R_0, it is then enough to look for numbers d_1 and d_2 which satisfy the right hand side of Inequality (6.2). If moreover we know, for some reason, that the fields we are looking for admit discriminant in a range where, for some arithmetical reason, they are forced to have principal different, then we can use the factor 4, which helps in the computations.
Thereby this process allows one to have an interval (d_1, d_2) such that any field of the given signature with $|d_K| \in (d_1, d_2)$ must have $R_K > R_0$. In the next section, we present some classic inequalities which allow to recover a similar restriction on the discriminants depending on the regulators, but over an unbounded interval.

Remark 28. There is a practical criterion, depending on the size of the discriminants, which allows to understand whether it is possible to say that ∂_K is principal. In fact, assume that this is not the case: then, being the class of ∂_K a square in Cl_K, one has the estimate $h_K \geq 3$ and from Class Field Theory there exists an unramified extension L/K of degree at least 3. But in an unramified extension the following identites are true, due to the triviality of the discriminant ideal of L over K:

$$\frac{1}{[K:\mathbb{Q}]}\log|d_K| = \frac{1}{[L:\mathbb{Q}]}\log|d_L|,$$
$$\frac{1}{[K:\mathbb{Q}]}r_1(K) = \frac{1}{[L:\mathbb{Q}]}r_1(L).$$

Thus, the root discriminant of K coincides with the one of a number field with at least three times its degree and three times its number of real embeddings: this forces $|d_K|$ to be quite big, larger than a lower bound d_∂ which is usually very far from the range of discriminants we will work with.
for every number field K of the given signature with $|d_K| \leq d_{\partial_K}$ we can use the factor 4 instead of the factor 2.

6.1.2 Geometric inequalities

We begin this section by recalling some notation.
For a number field K of degree n and signature (r_1, r_2), let ∞_K be the set $\{v_1, \dots, v_{r_1}, v_{r_1+1}, \dots, v_{r_1+r_2}\}$ of archimedean places, the first r_1 places being real and the remaining ones being complex. for every $\alpha \in \mathcal{O}_K$ define the corresponding absolute value

$$||\alpha||_{v_i} := \begin{cases} |\sigma_i(\alpha)| & \text{if } v_i \text{ real }, \\ |\sigma_i(\alpha)|^2 & \text{if } v_i \text{ complex }. \end{cases}$$

Let $r := r_1 + r_2 - 1$ be the rank of $\mathcal{O}_K^*$ as abelian group. For every unit $\varepsilon \in \mathcal{O}_K^*$ the **logarithmic length of** ε is defined as

$$m_K(\varepsilon) := \left(\sum_{i=1}^{r+1} (\log ||\varepsilon||_{v_i})^2 \right)^{1/2}$$

and this function can be thought as the square root of the restriction of the standard quadratic form $\sum_{i=1}^{r_1+r_2} x_i^2$ over the lattice of units $l(\mathcal{O}_K^*)$, where l is the map defined in Equation (3).

The following theorem, proved firstly by Remak [59] for number fields extensions over $\mathbb{Q}$ and generalized over any base number field by Friedman [22] many years later, gives an upper bound for the discriminants of number fields generated by some units depending on their logarithmic length.

Theorem 26 (Remak, Friedman)**.** *Let K/F be a finite number field extension, and assume $K = F(\varepsilon)$ with $\varepsilon \in \mathcal{O}_K^*$. Then*

$$\log |d_K| \leq [K : F] \log |d_F| + [K : \mathbb{Q}] \log[K : F] + m_K(\varepsilon) A(K/F) \tag{6.3}$$

where

$$A(K/F) := \sqrt{\frac{1}{3} \sum_{v \in \infty_F} ([H : L]^3 - [H : L] - 4r_2(v)^3 - 2r_2(v))}$$

and $r_2(v)$ is defined as the number of complex places of K over v whenever v is real, otherwise it is zero.

Corollary 5. *If $F = \mathbb{Q}$ and K has degree n and signature (r_1, r_2), then (6.3) becomes*

$$\log |d_K| \leq [K : \mathbb{Q}] \log[K : \mathbb{Q}] + m_K(\varepsilon) \sqrt{\frac{1}{3} (n^3 - n - 4r_2^3 - 2r_2)}. \tag{6.4}$$

We will not focus now on the proof of this result, leaving the corresponding considerations for later moments. Instead, we are now interested in showing how these inequalities provide an upper bound for the discriminant in terms of the regulator.

Let $\varepsilon_1 \in \mathcal{O}_K^*$ be the unit with minimum positive logarithmic length in $\mathcal{O}_K^*$: we know it exists from the considerations on quadratic forms of Section 0.1.2. Let $\varepsilon_2, \dots, \varepsilon_r$ be the successive minima for m_K over $\mathcal{O}_K^*$, and define $\mu_i := m_K(\varepsilon_i)$. By Minkowski's Theorem on successive minima, one gets the estimate

$$m_K(\varepsilon_1)^r = \mu_1^r \leq \prod_{i=1}^{r} \mu_i \leq [\gamma_r^r \cdot d(l(\mathcal{O}_K^*))]^{1/2} = \gamma_r^{\frac{r}{2}} \sqrt{r+1} R_K \tag{6.5}$$

where γ_r is the Hermite constant of dimension r.
Thus, if the field K is generated by the unit ε_1 with minimum logarithmic length, one can use Inequality (6.5) combined with Remak-Friedman's Inequality to obtain a lower bound for $|d_K|$ depending on the regulator. In particular, if $R_K \leq R_0$, then $|d_K|$ is bounded from above by a number depending on R_0, and one must look for fields with $R_K \leq R_0$ among the fields K with discriminant less than this number.
However, the previous assumption cannot be always guaranteed: there is no reason why the field $\mathbb{Q}(\varepsilon_1)$ must coincide with K, unless one knows that K is primitive. Besides, one knows that, up to a suitable reordering of the ε_j's, there is the tower of number fields

$$\mathbb{Q} \subseteq \mathbb{Q}(\varepsilon_{j_1}) \subseteq \mathbb{Q}(\varepsilon_{j_2}) \subseteq \cdots \subseteq \mathbb{Q}(\varepsilon_{j_r}) = K$$

and an iterated application of Remak-Friedman's inequality on this tower gives iterated estimates on the discriminants of the fields, which finally lead to an estimate of the form

$$\log |d_K| \leq A_0 + \sum_{j=1}^{r} A_j \mu_j, \qquad A_i \in \mathbb{R}. \tag{6.6}$$

This estimate can be optimized in terms of the regulator R_K, using some constrained optimization (see [3], Lemma 2 and 3) provided one is able to give a lower bound $\mu_1 \geq \delta$ for the length of $m_K(\varepsilon_1)$.
In the end, this process gives two inequalities of the form

$$\begin{aligned} &\log |d_K| \leq B_1(n, r_2, R_0) && \text{whenever } K = \mathbb{Q}(\varepsilon_1), \\ &\log |d_K| \leq B_2(n, r_2, R_0) && \text{depending on the subfield structure of } K \end{aligned}$$

and we can affirm that any field K with the given signature and $R_K \leq R_0$ must have $|d_K| \leq \max(\exp(B_1(n, r_2, R_0)), \exp(B_2(n, r_2, R_0))$. Usually, the bigger value is given by B_1, and this is precisely what happens in the specific cases we are going to consider.

6.1.3 Looking for number fields of minimal regulator

We now present the method used by Astudillo, Diaz y Diaz, Friedman and Ramirez-Raposo for classifying number fields with small regulators for all degrees ≤ 7 and for the signatures $(0,4), (8,0)$ and $(9,0)$. Further details of their computations can be found in [3] and [24].

1) Suppose you want to find the number fields with signature (r_1, r_2) and with $R_K \leq R_0$. Use Friedman-Remak's inequality to get an upper bound $\exp(B_1(n, r_2, R_0))$ for $|d_K|$ assuming the fields are primitive, and use its adaptation (6.6) to obtain another upper bound $\exp(B_2(n, r_2, R_0))$ for the non-primitive fields.
Then any number field with the given signature and $R_K \leq R_0$ must have $|d_K| \leq C(n, r_2, R_0) := \max(\exp(B_1(n, r_2, R_0)), \exp(B_2(n, r_2, R_0)))$. This gives an upper bound which is usually very large: as an example, $C(6, 4, 1.37) = \exp(23.73)$.

2) We would like to use the function g and Inequality (6.2) to reduce consistently the range of discriminants to be considered.
Assume $d_{\partial_K} < C(n, r_2, R_0)$: then one computes if $2g(1/d_{\partial_K}) > R_0$ and $2g(1/C(n, r_2, R_0)) > R_0$: if this is the case, we can use the factor 4 from now on.
If $d_{\partial_K} > C(n, r_2, R_0)$ instead, we can already use the factor 4 and verify if $4g(1/C(n, r_2, R_0)) > R_0$.

3) If any of the previous steps is satisfied, by Inequality (6.2) it is enough to look for a number d_1, usually not too far from the minimum value of $|d_K|$ for the considered signature, such that $4g(1/d_1) > R_0$. Then a number field K of the given signature (r_1, r_2) with $R_K \leq R_0$ must have $|d_K| \leq d_1$: the fields within this range are usually few enough to compute their regulators, and among these one classifies the fields with regulator less than the given upper bound.

Remark 29. The computation of regulators in the last step of the procedure can be done in PARI/GP: however, the correctness of the result given by the implemented algorithm assumes the truth of GRH. Nonetheless, there is a way to prove that the obtained value is unconditionally true: in fact, the PARI function for the computation of the regulators gives as output a number $\tilde{R}_K$ which is an integer multiple of the true value R_K.
Then, if $\tilde{R}_K = mR_K$ with $m \in \mathbb{N}$, assuming that $g(1/|d_K|) > 0$, we can use the lower bound (6.2) to estimate the quotient

$$m = \frac{\tilde{R}_K}{R_K} = \frac{\frac{\tilde{R}_K}{w_k}}{\frac{R_K}{w_K}} \leq \frac{\tilde{R}_K}{2g\left(\frac{1}{|d_K|}\right)}. \tag{6.7}$$

If this ratio is strictly less than 2, then $m = 1$ and the output value is the regulator of the field K.
In the following sections, every theorem concerning list of number fields with bounded regulator will be based on the fact that for every field in these lists the value of the regulator given by the PARI/GP procedure is in fact the actual value of the regulator, because either the examined fields satisfy (6.7) or a generalization of this condition which must be discussed in the few cases inequality (6.7) is not attained (see the remark at the end of the chapter).

6.2 Problems and improvements in totally real cases

6.2.1 The problem with further signatures of degree 8

In the previously illustrated method for classifying number fields with low regulator we pointed out in the last step that one needs a small value d_1 to reduce the search to the case where the number fields with $R_K \leq R_0$ have discriminant less than d_1 in absolute value, so that the regulators of the few fields that must be considered can be explicitly computed. But this last check cannot be executed if one does not have a complete list of number fields of the corresponding signature with $|d_K| \leq d_1$.
This was the reason that prevented the aforementioned authors to give a classification of the number fields with low regulators in the signatures $(2,3),(4,2)$ and $(6,1)$ in degree 8. The work described in chapter 5 gives the lists of number fields with these signatures which are complete up to some bound for the discriminant, and thus we can try to apply the classification method described in the previous section to these families.

Let us begin with the number fields with signature $(6,1)$: from Theorem 25 we know that there exist exactly 8 fields with this signature and $|d_K| \leq 79259702$. Using PARI/GP to compute their regulators, we see that their values are below 7.826, and the smallest one is attained by the field with minimum discriminant, being equal to 7.13506329... At this moment, let us content ourselves with the easier task of proving that this value is indeed the minimal one for the regulators in this signature.
Let us put then $R_0 := 7.14$: in our complete list, the only field such that $R_K \leq R_0$ is the field of minimum discriminant. Using Remak-Friedman's inequality and its adaptation, one obtains the upper bound $\exp(43.76972)$ for the discriminant. Using Diaz y Diaz' tables, one verifies that this value is smaller than the lower bound d_{∂_K} over which the fields of signature $(6,1)$ admit a non principal different ideal (d_{∂_K} corresponds to the lower bound for the root discriminant of number fields of degree 24 and signature $(6,9)$). This implies that we can already use the factor 4 in the Inequality (6.2) to verify that $4g(\exp(-43.76972)) > R_0$.
Unfortunately, this is not the case: in fact, $4g(\exp(-43.76972)) = -6926.4158..$ and not only this number is negative, but it also has a huge absolute value; this is a difficulty which cannot be overcome even with the adaptations proposed in [3]. Being $4g(1/79259702) = 7.487499\ldots$, one can just conclude that a field of signature $(6,1)$ with $R_K \leq 7.14$ is either the field of minimum discriminant or a field such that $|d_K| \in (79259702, \exp(43.76972))$, and this range is not only incomplete but also too much wide.
Similar problems occur also for the other signatures: considering the complete lists of Theorem 25, the minimum regulators for the fields in the lists with signature $(2,3),(4,2),(1,4)$ and $(3,3)$ have the values $0.83140.., 2.297796.., 0.680531..$ and $1.938363...$ respectively. We would like these values to be the minimum regulators for the respective signatures, using the classification method with $R_0 = 0.832, 2.298, 0.681$ and 1.939. Unfortunately, all the geometric inequalities provide upper bounds which are not practical to be put in the function in g, even with the factor 4: we always obtain negative values which have absolute

values too large to be overcome with adaptations of the method. Just like for the signature $(6,1)$, the method is only able to prove that for every considered signature the fields with $R_K \leq R_0$ are either the ones with minimum discriminants or fields with discriminant in a wide range between the upper bound of our tables and the upper bounds given by Remak-Friedman's inequality.

It has to be remarked, however, that this is not a new problem: in fact, the signature $(5,1)$ had a very similar bad behaviour whenever it was first studied in [3], and it required a different paper [24] to be solved properly. The reason of the difficulty was the same encountered here: applying the function $4g$ to the geometric upper bound given by Friedman-Remak's inequality gives a number which is unfeasible to be dealt with the proposed method. The resolution of this problem required ad hoc methods which led to give an improvement to the geometric inequality, so that the new upper bound d gave $4g(1/d) > R_0$.
Furthermore, as already mentioned in the previous section, minimum regulators in the signatures $(8,0)$ and $(9,0)$ have been already classified, which at first glance seems strange because these signatures give geometric bounds larger than the ones used for our signatures. As we will see later, the assumption on the fields being totally real allows to improve consistently the geometric inequalities.

The two facts exposed above suggest that our problems with the considered signatures could be solved by improving Remak-Friedman's inequality: the result on totally real fields in particular indicates that the signature of the field could give a more striking contribution to the estimates.

6.2.2 Considering the factors in the geometric inequality

In this section we focus on the proof of Remak-Friedman's inequality in order to understand which factors could be considered for an improvement.
Recall the fundamental hypothesis on the number field K, i.e. the fact that $K = \mathbb{Q}(\varepsilon)$ with $\varepsilon \in \mathcal{O}_K^*$; we can assume that ε is the unit with minimum logarithmic length in K. Let us suppose that $\varepsilon_1, \ldots, \varepsilon_n$ are the conjugates of ε with respect to the n embeddings of K, and that they are ordered such that $|\varepsilon_i| \leq |\varepsilon_j|$ if $i < j$. Then we know that $|d_K| \leq |D(\varepsilon)| := \prod_{1 \geq i < j \leq n} |\varepsilon_i - \varepsilon_j|^2$ and so

$$\begin{aligned}\log|d_K| \leq \log|D(\varepsilon)| &= \log\left(\prod_{1\leq i<j\leq n} |\varepsilon_i - \varepsilon_j|^2\right) \\ &= \log\left(\prod_{1\leq i<j\leq n} \left|1 - \frac{\varepsilon_i}{\varepsilon_j}\right|^2\right) + \sum_{j=2}^{n} 2(j-1)\log(|\varepsilon_j|).\end{aligned}$$

In the last sum we can add the null term with $j = 1$ and, from $\sum_{i=1}^{n} \log|\varepsilon_i| = 0$, we get

$$2\sum_{j=2}^{n}(j-1)\log|\varepsilon_j| = 2\sum_{v\in\infty_K} j(v)\log||\varepsilon||_v \tag{6.8}$$

where ∞_K is the set of archimedean places of K, and

$$j(v) := \begin{cases} j & \text{if } ||\varepsilon||_v = |\varepsilon_j| \text{ with } v \text{ real,} \\ \frac{j+k}{2} & \text{if } ||\varepsilon||_v = |\varepsilon_j|^2 \text{ with } v \text{ complex and } \varepsilon_k = \overline{\varepsilon_j}. \end{cases}$$

Notice that the index $j(v)$ is an integer between 1 and n if v is real, while $j(v)$ is an half-integer if v is complex.
Let λ be any real number: then the expression (6.8) is equal to

$$2\sum_{v\in\infty_K}(j(v)-\lambda)\log|||\varepsilon||_v \le 2\left(\sum_{v\in\infty_L}(\lambda-j(v))^2\right)^{1/2} m_K(\varepsilon)$$

where the inequality comes from a direct application of Cauchy-Schwarz inequality.
The factor $m_K(\varepsilon)$ is estimated by Inequality (6.5), but there seems to be no way to provide a better estimate which is also as general as the previous one. The minimum of the other factor, depending on λ, is estimated by $A(K/\mathbb{Q})$ given in Theorem 26, and the next lemma shows that this inequality is sharp for the fields of even degree.

Lemma 7. *Let K and $\varepsilon \in \mathcal{O}_K^*$ be as above, and assume that the degree n is even. Then there exist values of the indexes $j(v)$ and of λ such that $2(\sum_{v\in\infty_K}(\lambda-j(v)))^{1/2} = A(K/\mathbb{Q})$.*

Proof. Choose the indexes $j(v)$ so that the archimedean places which give integer values of $j(v)$ are labelled with the numbers $\{1, 2, \dots, r_1/2\}$ and $\{r_1/2+2r_2+1, \dots, r_1+2r_2 = n\}$. Define $S := \{j(v)\colon v \in \infty_K\}$: the cardinality of S is equal to $r_1 + r_2$ and

$$\sum_{v\in\infty_L}(\lambda-j(v))^2 = \sum_{j(v)\in S}(\lambda-j(v))^2. \tag{6.9}$$

The value of λ which minimizes this expression is given by $(\sum_{j(v)\in S} j(v))/(r_1+r_2)$: the specific choice of the indexes $j(v)$ is such that the numerator is equal to $(r_1+r_2)(n+1)/2$, and so the inequality is minimized with $\lambda = (n+1)/2$.
Denote now with S_2 the set of indexes $j(v)$ which are half-integers: we want to rearrange the sum (6.9) in order to get a term of the form $\sum_{i=1}^{n}(\lambda-i)^2$, and this can be done by adding and subtracting terms $(\lambda-(j(v)-1/2))^2$ and $(\lambda-(j(v)+1/2))^2$ for any half-integer

index $j(v) \in S_2$. Thus we obtain

$$\begin{aligned}
&\sum_{i=1}^{n}(\lambda-i)^2+\sum_{j(v)\in S_2}\left((\lambda-j(v))^2-\left(\lambda-\left(j(v)+\frac{1}{2}\right)\right)^2-\left(\lambda-\left(j(v)-\frac{1}{2}\right)\right)^2\right)\\
&=\sum_{i=1}^{n}(\lambda-i)^2+\sum_{j(v)\in S_2}\left((\lambda-j(v))^2-(\lambda-j(v))^2+(\lambda-j(v))-\frac{1}{4}-(\lambda-j(v))^2-(\lambda-j(v))-\frac{1}{4}\right)\\
&=\sum_{i=1}^{n}(\lambda-i)^2-\frac{r_2}{2}-\sum_{j(v)\in S_2}(\lambda-j(v))^2.
\end{aligned}$$

With $\lambda=(n+1)/2$, one immediately gets $\sum_{i=1}^{n}(\lambda-i)^2=(n^3-n)/12$. More difficult is considering the last sum; however, our choice of the half-integers in S_2 is such that one can verify the identity

$$\sum_{j\in S_2}(\lambda-j(v))^2=\sum_{\substack{j=0\\ j\equiv r_2-1 \bmod 2}}^{r_2-1}\left(\frac{n+1}{2}-\left(\frac{n+1}{2}-j\right)\right)^2=2\sum_{\substack{j=0\\ j\equiv r_2-1 \bmod 2}}^{r_2-1}j^2. \tag{6.10}$$

If r_2-1 is even, then the sum (6.10) becomes

$$8\sum_{j=0}^{(r_2-1)/2}j^2=8\frac{\frac{r_2-1}{2}\frac{r_2+1}{2}r_2}{6}=\frac{r_2^3-r_2}{3}.$$

If r_2-1 is odd, the sum (6.10) becomes

$$2\sum_{j=0}^{r_2}j^2-2\sum_{\substack{j=0\\ j=r_2-1 \bmod 2}}^{r_2-1}j^2=\frac{r_2(r_2+1)(2r_2+1)-(r_2+1)^3+(r_2+1)}{3}=\frac{r_2^3-r_2}{3}.$$

Collecting the results together, we finally get

$$2\left(\sum_{v\in\infty_K}(\lambda-j(v))^2\right)=2\left(\frac{n^3-n}{12}-\frac{r_2}{2}-\frac{r_2^3-r_2}{3}\right)^{1/2}=\sqrt{\frac{n^3-n-4r_2^3-2r_2}{3}}.$$

□

The two factors considered above are not easily improvable, so we look at what happens to the remaining factor. Actually, we will focus onto the study of a more general function. Let $\varepsilon_1,\dots,\varepsilon_n\in\mathbb{C}$ be complex numbers such that $|\varepsilon_i|\le|\varepsilon_j|$ for $i<j$. Define the function

$$P(\varepsilon_1,\dots,\varepsilon_n):=\prod_{1\le i<j\le n}\left|1-\frac{\varepsilon_i}{\varepsilon_j}\right|^2. \tag{6.11}$$

Observe that we can always assume that the numbers ε_j are less or equal than 1 in absolute value, because dividing every ε_i by $|\varepsilon_n|$ does not change the values of the function P. Thus, we can always think of P as a function defined on the set

$$\{0 \leq |\varepsilon_1| \leq |\varepsilon_2| \leq \cdots \leq |\varepsilon_n| \leq 1\}. \tag{6.12}$$

The following theorem proves the classic estimate of the function P, which is the one used in Remak-Friedman's inequality, by means of a proper change of variables, which shifts our problem to the estimate of a function defined over the $(n-1)$-dimensional hypercube $[-1,1]^{n-1}$.

Theorem 27 (Remak, Bertin)**.** *Let $P(\varepsilon_1, \ldots, \varepsilon_n)$ be defined as in Equation (6.11). Then $|P(\varepsilon_1, \ldots, \varepsilon_n)| \leq n^n$.*

Proof. Define the following change of variables:

$$\rho_i := \varepsilon_i/\varepsilon_{i+1} \quad \text{for } i = 1, \ldots, n-1.$$

The positive function $P(\rho_1, \ldots, \rho_{n-1})$ can be now thought as a function defined over $[-1,1]^{n-1}$, and an estimate over this larger set yields immediately the estimate we look for. In this new setting, P can be rewritten as

$$P(\rho_1, \ldots, \rho_{n-1}) := \prod_{i=1}^{n-1} \prod_{j=i}^{n-1} \left| 1 - \prod_{k=i}^{j} \rho_k \right|^2 .$$

The main part of the proof, which is explained with every detail in [7], is to show that $P(\rho_1, \ldots, \rho_{n-1})$ is the square of the determinant of a matrix M whose columns have euclidean norm less or equal than $\sqrt{n}$. As an example, when $n = 3$ the matrix M has the form

$$M := \begin{pmatrix} 1 & \rho_1 & \rho_1^2\rho_2 \\ 1 & 1 & \rho_2 \\ \rho_2 & 1 & 1. \end{pmatrix}$$

The claim follows then by Hadamard's Lemma ([61], Chapter 1, Section 1, Lemma IV), which affirms that the absolute value of $|\det M|$ is bounded by the product of the euclidean norms of its columns. □

Because of the difficulty given by the other two factors of Remak-Friedman inequality, it appears that the only worthy attempt to improve the upper bound given by the inequality is to get some upper bound for the function P which is better than n^n. An additional and helpful remark consists in observing that the function P should take into account the signature of the fields we are dealing with: this could be achieved by considering the set of Equation (6.12) but with the assumption that $n = r_1 + 2r_2$, that r_1 variables are real and the remaining $2r_2$ variables form r_2 couples of complex conjugated numbers.

6.2.3 An improvement for totally real fields

In this section we present a much better estimate for the function $P(\varepsilon_1, \ldots, \varepsilon_n)$ defined in Equation (6.11) assuming that the numbers ε_j are assumed to be real. The result is the key tool which allowed Astudillo, Diaz y Diaz and Friedman to get a classification of totally real fields with minimum regulator in degree 8 and 9.

Theorem 28 (Pohst)**.** *Let $n \leq 11$ and let $\varepsilon_1, \ldots, \varepsilon_n$ be real numbers in $[-1, 1]$ such that $|\varepsilon_i| \leq |\varepsilon_j|$ if $i < j$. Then*

$$P(\varepsilon_1, \ldots, \varepsilon_n) \leq 4^{\lfloor \frac{n}{2} \rfloor}.$$

Proof. Consider the change of variables $\rho_i := \varepsilon_i/\varepsilon_{i+1}$ for $i = 1, \ldots, n-1$ introduced previously and define

$$Q(\rho_1, \ldots, \rho_{n-1}) := \sqrt{P(\rho_1, \ldots, \rho_{n-1})}$$

which is still a positive function. We look for an estimate of Q, which has a simpler form than P, over the hypercube $[-1, 1]^{n-1}$.
Let us analyze some cases in low dimension:

$n = 2$: the function Q is simply

$$Q(\rho_1) = (1 - \rho_1)$$

which is obviously less or equal than 2, this value being attained in $\rho_1 = -1$.

$n = 3$: the function Q has now the form

$$\begin{aligned} Q(\rho_1, \rho_2) = (1 - \rho_1)&(1 - \rho_1\rho_2) \\ &(1 - \rho_2) \end{aligned}$$

where the right hand side is assumed to be a product of all the written factors. An easy optimization using the partial derivatives of Q shows that the global maximum is attained on the boundary, precisely on the point $\rho_1 = 0, \rho_2 = -1$ and that the maximum of Q is again equal to 2.

$n = 4$: the function now assumes the form

$$\begin{aligned} Q(\rho_1, \rho_2) = \quad (1 - \rho_1) \quad (1 - \rho_1\rho_2) \quad & (1 - \rho_1\rho_2\rho_3) \\ (1 - \rho_2) \quad & (1 - \rho_2\rho_3) \\ & (1 - \rho_3). \end{aligned}$$

Considering all the 8 sign possibilities for ρ_1, ρ_2 and ρ_3, one is able to show that for each of these subcases Q is not bigger than 4: this fact is trivial when all the variables are positive, being Q less than 1. For mixed signs, one can either gain information by using the fact that $(1 - \rho_i)(1 - \rho_i\rho_j)(1 - \rho_j)$ is less than 2 or showing that the block of four factors $(1-\rho_1\rho_2)(1-\rho_1\rho_2\rho_3)(1-\rho_2)(1-\rho_2\rho_3)$ is less than 1, up to assuming some specific

sign conditions on the ρ_j's.
The sharpest maximum, equal to 4, is attained on the boundary, in the point given by $\rho_1 = -1, \rho_2 = 0, \rho_3 = -1$.

For higher values of n up to 11, the sketch of the proof is the same: for any sign condition on the ρ_j's, one tries to estimate with the values 1 or 2 some blocks of four or three factors respectively, and from the check of every case the claim follows. See [54] for the details. □

Remark 30. The result was claimed to be true for every $n \in \mathbb{N}$: though this is very likely, unfortunately the proof gave by Bertin in [7] seems not to work, because of incorrect assumptions on the existence of the maximum points on the boundary of the hypercube.

This is indeed a consistent improvement for the function P, and consequently for Remak-Friedman inequality, whenever the considered numbers are real: this corresponds to a signature of the form $(n, 0)$. This better result was precisely the reason which allowed Astudillo, Diaz y Diaz and Friedman to classify the number fields with low regulator in the signatures $(8, 0)$ and $(9, 0)$.
On the other side, one realizes that the classic estimate with n^n is sharp for signatures which are very near to be totally complex. This fact is proved in the following lemma, for which there are no other references in the literature, and not just for totally complex fields.

Lemma 8. *Let $n \in \mathbb{N}$ be odd. Let ζ_n be a primitive n-th root of unity. Then*

$$P(1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}) = n^n.$$

Let $n \in \mathbb{N}$ be even, and let ζ_n and ζ_{2n} be primitive roots of unity of order n and $2n$ respectively. Then

$$P(1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}) = n^n = P(\zeta_{2n}, \zeta_{2n}^3, \dots, \zeta_{2n}^{2n-1}).$$

Proof. Assume that $n \in \mathbb{N}$ is odd. The powers ζ_n^j with $j \in \{0, 1, \dots, n-1\}$ are complex numbers with absolute value equal to 1, and so we do not have problems with their order of appearance in the function P: moreover, the value of every factor of P is unchanged by multiplication with $|\zeta_n^j|$ for some suitable j depending on the factor; thus

$$P(1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}) = \prod_{0 \le i < j \le n-1} \left| 1 - \frac{\zeta_n^i}{\zeta_n^j} \right|^2 = \prod_{0 \le i < j \le n-1} \left| \zeta_n^i - \zeta_n^j \right|^2$$

and the last term is identified as $|\mathrm{disc}(x^n - 1)|$, which is known to be equal to n^n. The procedure and the result are exactly the same if one assumes that n is even.
Now assume n to be even and consider the function $P(\zeta_{2n}, \zeta_{2n}^3, \dots, \zeta_{2n}^{2n-1})$: being $\zeta_{2n}^{2j} = \zeta_n^j$ for every $j \in \{0, \dots, n-1\}$, we have

$$P(\zeta_{2n}, \zeta_{2n}^3, \dots, \zeta_{2n}^{2n-1}) = \prod_{0 \le i < j \le n-1} \left| 1 - \frac{\zeta_{2n}^{2i+j}}{\zeta_{2n}^{2j+1}} \right|^2 = \prod_{0 \le i < j \le n-1} \left| 1 - \frac{\zeta_n^i}{\zeta_n^j} \right|^2$$

and this value is equal to n^n by the previous lines. □

Remark 31. Lemma 8 shows that the classic estimate for P is sharp in the signature $(1,(n-1)/2)$ when n is odd and in the signatures $(0,n/2)$ and $(2,(n-2)/2)$ when n is even.

So, on one side we have recalled a much better estimate whenever the signature of the fields is $(n,0)$; on the other, we have seen that the classical estimate is sharp for signatures which are very near to correspond to totally complex fields. It is then straightforward to wonder if for mixed signatures one could get sharp upper bounds which are intermediate between Pohst's bound $4^{\lfloor n/2 \rfloor}$ and n^n; moreover, the less real embeddings one takes into account, the more these upper bounds should increase. Such a behaviour, if confirmed, would provide not only improvements to Remak-Friedman inequality, but it would present a nice duality with the growth of the discriminant, which instead becomes bigger the more real embeddings one takes into account.

6.3 Conjectural improvementes

6.3.1 Signatures $(1,1),(2,1)$ and $(3,1)$

The goal of this section is to study the behaviour of the functions which we are interested in using for obtaining improvements on Remak-Friedman's inequality.
Let $n \in \mathbb{N}$ be an integer greater than 1 and let (r_1,r_2) be a couple of non-negative integers such that $n = r_1 + 2r_2$. Consider the set

$$A_{n,r_2} := \{(\varepsilon_1,\dots,\varepsilon_n) \in \mathbb{C}^n \colon 0 \le |\varepsilon_1| \le |\varepsilon_2| \le \cdots \le |\varepsilon_n| \le 1, r_1 \text{ of the } \varepsilon_j\text{'s being real,} \\ \text{the remaining ones forming } r_2 \text{ couples of complex conjugated numbers}\}.$$

Define then the function

$$Q(n,r_2,\cdot) : A_{n,r_2} \to \mathbb{R}$$

$$Q(n,r_2,(\varepsilon_1,\dots,\varepsilon_n)) := \prod_{1\le i<j\le n} \left|1 - \frac{\varepsilon_i}{\varepsilon_j}\right|.$$

The square of $Q(n,r_2,(\varepsilon_1,\dots,\varepsilon_n))$ is the number $P(\varepsilon_1,\dots,\varepsilon_n)$ defined in Equation (6.11). We call the couple (r_1,r_2) **the signature of the function** $Q(n,r_2,\cdot)$, in order to agree with the signature of number fields.
In the following we will always make a change of variables in order to obtain a function, which by abuse of notation will be denoted again with $Q(n,r_2,\cdot)$, defined on the hypercube $[-1,1]^{n-1}$. We define the number

$$M(n,r_2) := \max_{(x_1,\dots,x_{n-1})\in[-1,1]^{n-1}} Q(n,r_2,(x_1,\dots,x_n)),$$

the maximum of $Q(n,r_2,\cdot)$ over $[-1,1]^{n-1}$: thus $P(\varepsilon_1\dots,\varepsilon_n) \le M(n,r_2)^2$ for every choice of $(\varepsilon_1,\dots,\varepsilon_n) \in A_{n,r_2}$.

If the ε_j's are conjugates of a unit ε generating a number field of degree n and signature (r_1, r_2) we can replace the term $n \log n$ in Remak-Friedman's Inequality with $2 \log M(n, r_2)$.

Corollary 6. *By Pohst's theorem, one has $M(n, 0) = 2^{\lfloor n/2 \rfloor}$ for every $n \leq 11$.*
By Lemma 8 one has $M(n, (n-1)/2) = n^{n/2}$ for every odd integer n, and $M(n, n/2)$ $= M(n, (n-2)/2) = n^{n/2}$ for every integer even n.

In particular, from Corollary 6, we know that the maximum $M(n, r_2)$ of the function Q cannot be improved for the least non real signatures, which are $(1, 1), (2, 1)$ and $(0, 2)$. However, in the following lines we show how to recover the corresponding value of $M(n, r_2)$ with an approach different from the one used in Lemma 8, instead, we will try to imitate Pohst's proof for the totally real signatures, making some tricky change of variables and studying $Q(n, r_2, \cdot)$ analytically.

- Consider first the signature $(1, 1)$. Given $(\varepsilon_1, \varepsilon_2, \varepsilon_3) \in A_{3,1}$, let us assume for simplicity that ε_1 is real and $|\varepsilon_2| = |\varepsilon_3| = 1$ with $\varepsilon_2 = \bar{\varepsilon_3}$. Call $x := \varepsilon_1$ and $g = \cos\theta$ with $\exp(i\theta) = \varepsilon_2$; then $(x, g) \in [-1, 1]^2$ and the function $Q(3, 1, \cdot)$ is extended over $[-1, 1]^2$ assuming the form

$$Q(3, 1, (x, g)) := \frac{(1 - 2xg + x^2)}{2\sqrt{1 - g^2}}$$

  where the right hand side is assumed to be a product of all the written factors.
  Then $Q(3, 1, -x, -g) = Q(3, 1, x, g)$ and it is immediately seen to be maximized in the point $(1, -1/2)$ providing the value $3^{3/2}$, which is exactly $M(3, 1)$. One notices that, thanks to the previous change of variables, this choice of x and g corresponds exactly to the third roots of unity which are known to give the correct value of $M(3, 1)$ by Lemma 8.
  If one supposes instead that ε_3 is a real number and that $\varepsilon_1 = \bar{\varepsilon_2}$, then the boundary condition given by $A_{3,1}$ yields $\varepsilon_3 \in \{\pm 1\}$ and we can take $\varepsilon_3 = 1$ without loss of generality (otherwise, one simply changes the sign to all the ε_j's). Being $\varepsilon_1 = r \exp(i\theta)$ with $r \in [0, 1]$ and $g = \cos(\theta) \in [-1, 1]$, the function $Q(3, 1, \cdot)$ can be extended again over $[-1, 1]^2$ and becomes

$$Q(3, 1, (r, g)) := (1 - 2rg + r^2) \cdot 2\sqrt{1 - g^2}$$

  which again is maximized in the point $(r, g) = (1, -1/2)$ corresponding to the third roots of unity and provides a maximum equal to $3^{3/2}$.

- Let us check now what happens for the signature $(2, 1)$: for simplicity, we examine only the case when ε_1 and ε_2 are real, while ε_3 and ε_4 are complex conjugated. Define then $x := \varepsilon_1/\varepsilon_2$, $y := \varepsilon_2$ and $g := \cos(\theta)$ where $\varepsilon_3 = \exp(i\theta)$; we have $(x, y, g) \in [-1, 1]^3$ and again we can extend the function $Q(2, 1, \cdot)$ over the hypercube

obtaining the expression

$$Q(4,1,(x,y,g)) = \begin{array}{ccc} (1-x) & (1-2xyg+(xy)^2) \\ & (1-2yg+y^2) \\ & 2\sqrt{1-g^2}. \end{array}$$

We know that this function is estimated by $M(4,1) = 16$: one verifies that this value is attained precisely in the point $(x,y,g) = (-1,1,0)$, which corresponds to the 4-th roots of unity via the change of variables.
Studying the remaining cases given by the different choices for index representing the complex conjugated numbers and the corresponding change of variables (x,y,g), one verifies that the maximum of $Q(4,1,(x,y,g))$ is always attained in $(-1,1,0)$.

- For the signature $(0,2)$ we do not have to consider different subcases: in fact, we always have $\bar{\varepsilon}_1 = \varepsilon_2$ and $\bar{\varepsilon}_3 = \varepsilon_4$ and we can write $\varepsilon_1 = r\exp(i\theta)$, $\varepsilon_3 = s\exp(i\phi)$ with $0 \leq r \leq s \leq 1$. Defining $x := r/s, g := \cos\theta$ and $h := \cos\phi$, the function $Q(4,2,\cdot)$ assumes the form

$$Q(4,2,(x,g,h)) = \begin{array}{c} 4\sqrt{1-g^2}\sqrt{1-h^2}\cdot \\ ((1+x^2)^2 - 4x(1+x^2)gh + 4x^2(-1+g^2+h^2)). \end{array}$$

We know again that this function is maximized by $M(4,2) = 16$, and this value is precisely attained in the point $(x,g,h) = (1,1/\sqrt{2},-1/\sqrt{2})$ which corresponds exactly to the numbers $\varepsilon_j = \zeta_8^{2j+1}$ via the change of variables.

Signature $(3,1)$ is the first one for which we no longer have information due to Lemma 8, so let us begin its study by assuming again that ε_4 and ε_5 are complex conjugated: with the change of variables $x := \varepsilon_1/\varepsilon_2, y := \varepsilon_2/\varepsilon_3, z := \varepsilon_3, g := \cos(\theta)$ where $\varepsilon_4 = \exp(i\theta)$, the function $Q(5,1,\cdot)$ can be extended over $[-1,1]^4$ and assumes the form

$$Q(5,1,(x,y,z,g)) = \begin{array}{ccc} (1-x) & (1-xy) & (1-2xyzg+(xyz)^2) \\ & (1-y) & (1-2yzg+(yz)^2) \\ & & (1-2zg+z^2) \\ & & 2\sqrt{1-g^2}. \end{array}$$

Without any previous knowledge of $M(5,1)$, we are forced to study this function from an analytic point of view.

Lemma 9. *The maximum of $Q(5,1,(x,y,z,g))$ is attained at a point (x,y,z,g) with $z = 1$ and $g \neq \pm 1$.*

Proof. Observe that the function Q is not negative over $[-1,1]^4$ and is strictly positive in the interior $(-1,1)^4$, and so the maximum of Q coincides with the one of $\log Q$. Let us assume that the maximum is attained in a point (x,y,z,g) such that $(z,g) \in (-1,1)^2$. Then we have

$$\begin{cases} \partial_z \log Q = 0 \\ \partial_g \log Q = 0 \end{cases}$$

and this system of partial derivatives has the form

$$\begin{cases} \sum_{j=1}^{3} \frac{-2\alpha_j g + 2\alpha_j^2 z}{1-2\alpha_j z g + \alpha_j^2 z^2} = 0 & (I) \\ -\frac{g}{1-g^2} + \sum_{j=1}^{3} \frac{-2\alpha_j z}{1-2\alpha_j z g + \alpha_j^2 z^2} = 0 & (II) \end{cases}$$

where $\alpha_1 := xy$, $\alpha_2 := y$, $\alpha_3 := 1$.
Now we manipulate the lines of the system to get

$$\begin{aligned} 0 = z \cdot (I) - g \cdot (II) &= \sum_{j=1}^{3} \frac{-2\alpha_j g z + 2\alpha_j^2 z^2}{1-2\alpha_j z g + \alpha_j^2 z^2} + \frac{g^2}{1-g^2} + \sum_{j=1}^{3} \frac{2\alpha_j g z}{1-2\alpha_j z g + \alpha_j^2 z^2} \\ &= \frac{g^2}{1-g^2} + \sum_{j=1}^{3} \frac{2\alpha_j^2 z^2}{1-2\alpha_j z g + \alpha_j^2 z^2}. \end{aligned}$$

Every term in the above sum is non-negative, and so we must have $g = 0$ and $\alpha_j z = 0$ for every j; being $\alpha_3 = 1$, it must be $z = 0$. Thus the maximum should be attained in a point (x, y, z, g) which satisfies the condition $(z, g) = (0, 0)$: but $Q(5, 1, (x, y, 0, 0)) = 2Q(3, 0, (x, y))$, which by Pohst's Theorem is bounded by $2 \cdot 4 = 8$. This estimate is clearly in contradiction with the behaviour of $Q(5, 1, \cdot)$ because $Q(5, 1, (0, -1, 1, 0)) = Q(4, 1, (-1, 1, 0)) = 16$; thus the maximum point must have the parameters (z, g) on the boundary of $[-1, 1]^2$.
Now, the values $g = \pm 1$ force Q to be 0, and so we are left with $z = \pm 1$ and $g \neq \pm 1$. Being

$$G(x, y, z, g) = G(x, y, -z, -g)$$

we can finally assume $z = 1$ and $g \neq \pm 1$. □

Thanks to this lemma, the function $Q(5, 1, \cdot)$ assumes now the form

$$Q(5, 1, (x, y, 1, g)) = \begin{matrix} (1-x) & (1-xy) & (1-2xyg+(xy)^2) \\ & (1-y) & (1-2yg+(y)^2) \\ & & 4(1-g)\sqrt{1-g^2} \end{matrix}$$

and we study now its maximum.

Conjecture 1. *The maximum of $Q(5, 1, (x, y, 1, g))$ is $16.6965\ldots$ and is attained at the point $(x, y, z, g) = (1/\sqrt{7}, -1, 1, 1/(2\sqrt{7}))$.*

(Almost) proof:
Let us first define the function

$$R(x, y, 1, g) = \begin{matrix} (1-x) & (1-xy) & (1-2xyg+(xy)^2) \\ & (1-y) & (1-2yg+(y)^2) \end{matrix}$$

which satisfies the relation

$$Q(5, 1, (x, y, 1, g)) = R(x, y, 1, g) 4(1-g)\sqrt{1-g^2}.$$

This choice is done in order to study the partial derivatives with respect to x and y without carrying the factor which depends only on g. Let so $R_x(x,y,1,g) := \partial_x R(x,y,1,g)$ and $R_y(x,y,1,g) := \partial_y R(x,y,1,g)$.
The research of the maximum point of $Q(5,1,\cdot)$ is carried by starting a numerical search on PARI for the values that the function Q assumes over specified sub-regions of $[-1,1]^3$, each search depending on a value of g in a discrete, yet very refined finite set.
In fact, let us vary the value of g between -0.999 and 0.999, with steps of size $1/1536$: for any of these choices, one studies the following quantities:

- The maximum of $Q(5,1,(x,-1,1,g))$ over $x \in [-1,1]$: this condition means that we have assumed the only meaningful boundary condition on y (because the function is equal to zero if $y = 1$) and we look for the maximum value by selecting numerically, via the command **polrootsreal()**, the real roots of the partial derivative $R_x(x,-1,1,g)$ such that $|x| \leq 1$, and computing $Q(5,1,\cdot)$ for such values of x.

- The maximum of $Q(5,1,(-1,y,1,g))$ over $y \in [-1,1]$: the process is similar to the one described above and this time we look for the real roots of $R_y(-1,y,1,g)$, evaluating then $Q(5,1,\cdot)$ over the roots y such that $|y| \leq 1$.

- The maximum of $Q(5,1,(x,y,1,g))$ over the open set $\{(x,y) \in (-1,1)^2\}$: this study is carried by computing the common real roots of the polynomials $R_x(x,y,1,g)$ and $R_y(x,y,1,g)$ and evaluating then the function $Q(5,1,\cdot)$ over the roots (x,y) with $|x| < 1$ and $|y| < 1$. The numerical computation of the roots is done by studying the roots of the resultant of R_x and R_y with respect to the variable x: the needed PARI command is **polresultant()**.

For every choice of g in our interval, one plots the obtained values and looks for the regions where higher absolute values are obtained. By this process, one notices that higher values are obtained with the boundary condition $y = -1$, and we can just reduce our study on this boundary. In fact, even if we have studied just a finite set of values for g, the fact that $Q(5,1,\cdot)$ is the square root of a polynomial implies that studying its behaviour on an equi-distributed and very refined set of values for g should provide the previous maximum values with fair enough precision.
With this assumption the function $Q(5,1,(x,-1,1,g))$ becomes now

$$Q(5,1,(x,-1,1,g)) = 16(1-x^2)(1+2xg+x^2)(1-g^2)^{3/2}$$

and we now look for the maximum of this function, this time with a precise analytic study. Surely x must not be equal to ± 1, otherwise the function is zero, and thus we must look for $x \in (-1,1)$: in order to study the partial derivative with respect to x let us consider the factors which depend on x by defining

$$S(x,g) := (1-x^2)(1+2xg+x^2).$$

We have $S_x(x,g) := \partial S/\partial_x(x,g) = -4x^3 - 6gx^2 + 2g$ and we study $S_x(x,g) = 0$: this equation gives the condition

$$g = \frac{2x^3}{1-3x^2} \tag{6.13}$$

and one verifies that the function $g(x)$ above has positive derivative

$$g'(x) := 6x^2(1-x^2)/(1-3x^2)^2$$

over $x \in [-1,1]^2$, which in turn implies that the Equation (6.13) gives a bijective correspondence: thus, for every value of $g \in (-1,1)$, there is a unique $x := x(g) \in (-1,1)$ such that $S(x(g),g) = 0$.
We finally study $16S(x(g),g)(1-g^2)^{3/2}$: derive it in g to get

$$\left[\frac{\partial S}{\partial_{x_1}}(x(g),g)\frac{\partial x(g)}{\partial_g} + \frac{\partial S}{\partial_{x_2}}(x(g),g)\right](1-g^2)^{3/2} + S(x(g),g)(-3g)(1-g^2)^{1/2} = 0.$$

By definition of $x(g)$ we have $\frac{\partial S}{\partial_{x_1}}(x(g),g) = 0$ and so

$$\begin{aligned}&\frac{\partial S}{\partial_{x_2}}(x(g),g)(1-g^2) + S(x(g),g)(-3g)\\ &= 2x(1-x^2)(1-g^2) - 3g(1-x^2)(1+2xg+x^2) = 0.\end{aligned}$$

Being the maximum not attained for $x = \pm 1$, we reduce ourselves to study

$$2x(1-g^2) - 3g(1+2xg+x^2) = 0.$$

Using the relation (6.13) in this equation we finally get

$$\frac{-14x^7 + 30x^5 - 18x^3 + 2x}{9x^4 - 6x^2 + 1} = 0.$$

The numerator factorizes as $x(x^2-1)^2(7x^2-1)$, and the only zeros which do not annihilate the function are attained in $x = \pm 1/\sqrt{7}$, which from Equation (6.13) give $g = \pm 1/(2\sqrt{7})$: evaluating $Q(5,1,(1/\sqrt{7},-1,1,1/(2\sqrt{7})))$ we get the maximum value $16.6965\ldots$ □

Remark 32. The procedure shown above cannot be considered as a proof, because of the discrete process given by considering a finite, even if large, number of points instead of continuous intervals, and this is why we prefer refer to the lines above as part of a conjecture.

Remark 33. In the PARI program used for the computation, some errors resulted while evaluating the resultant over $y = 0$: however, this is not a real problem, because

$$Q(5,1,(x,0,1,g)) = (1-x)4(1-g)\sqrt{1-g^2} \leq 2 \cdot 3\sqrt{3} \leq 6\sqrt{3} < 12$$

and meanwhile we know that $Q(5,1,(0,-1,1,0)) = Q(4,1,(-1,1,0)) = 16$, so that surely an absolute maximum point for our original function cannot be over $y = 0$.

Remark 34. Even if the conjecture was actually proved, we could not conclude that $M(5,1) = 16.6965\ldots$ because we would have proved an estimate just for the rearrangement of the function $Q(5,1,(\varepsilon_1,\ldots,\varepsilon_5))$ given by the assumption that ε_4 and ε_5 are the unique complex non real numbers and are conjugated. Different choices for the ordering of the complex variables provide other change of variables for $Q(5,1,\cdot)$ which in turn give harder functions to estimate directly. The difficulty is given by the fact that we are not able to reduce the number of variables from 4 to 3, and this forces the algorithmic process to be too much heavy in the computation of the resultants.

6.3.2 Empirical tools and conjectures on the upper bounds

As described in the previous lines, we are currently not able to prove that $M(5,1) = 16.6965\ldots$ because we cannot make a good study of the different orderings which cover all the possibilities for the function $Q(5,1,\cdot)$. Whenever we increase the degree and we change the signature, the situation becomes more and more complicated: the functions $Q(n,r_2,\cdot)$ become polynomials of several variables with very bad shape, of which we are not able to prove anything in a rigorous way.
We decided then to content ourselves and to get only a conjectural estimate of the maxima $M(n,r_2)$, in order to see how these values would modify the study of minimum regulators given by Remak-Friedman's inequality.
We have pursued several ways for looking for good empirical approximations of $M(n,r_2)$: we present the two most fruitful and enlightening ones.

- First of all, we have tried some numerical simulation on PARI/GP, by simply computing many values of the functions $Q(n,r_2,\varepsilon_1,\ldots,\varepsilon_n)$ on random numbers in A_{n,r_2} (thus respecting all the ordering and complex conjugation requests). The tests were repeated several times, each time saving the maximum value obtained, and saving also the points in which these values were attained.

- We applied the Matlab Optimization Toolbox [46] to any variables ordering of any function $Q(n,r_2,\cdots)$ to guess the maximum values of these functions and the points in which they were attained. The test were repeated several times, changing the starting points for the algorithms.

The two procedures illustrated above gave almost identical values for the desired maxima and the points on which these values are attained. In Table 6.1 we give the conjectured upper bounds $M(n,r_2)$, and from that we form the following conjectures:

Conjecture 2. *The values proposed in Table 6.1 are the actual values of* $M(n,r_2)$.

Conjecture 3. *For every* $r_2 \in \mathbb{N}$ *there exists* $C(r_2) \in \mathbb{N}$ *such that* $M(n+2,r_2) = 2M(n,r_2)$ *for every* $n \geq C(n,r_2)$.

Conjecture 4. $C(0) = 2$ *and for every* $n \geq C(0)$*, after a suitable change of variables, the maximum value* $M(n,0)$ *is attained in the point* $(x_1,\cdots,x_n) = (0,-1,0,-1,\ldots,0,-1)$ *for* n *even and* $(-1,0,-1,\ldots,0,-1)$ *for* n *odd.*

Conjecture 5. *$C(1) = 4$ and for every $n \geq C(1)$, after a suitable change of variables, the maximum value $M(n,1)$ is attained in $(x_1, \dots x_{n-3}, x_{n-2}, g) = (-1, 0, -1, 0, \dots, -1, 0)$ for n even and $(x_1, \dots x_{n-3}, x_{n-2}, g) = (-1/\sqrt{7}, -1, -1/\sqrt{7}, -1, \dots, -1/\sqrt{7}, -1, 1, 1/(2\sqrt{7}))$.*

r_2 \ n	2	3	4	5	6	7	8
0	2	2	4	4	8	8	16
1		$3^{3/2}$	16	$16.6965\dots$	32	$2 \cdot 16.6965\dots$	64
2			16	$5^{5/2}$	$6^{6/2}$	$245.8193\dots$	$7^{7/2}$
3					$6^{6/2}$	$7^{7/2}$	$8^{8/2}$
4							$8^{8/2}$

Table 6.1: The conjectured values for $M(n, r_2)$.

6.3.3 Application to the minimum regulator problem

In this final section we present how we can apply the conjectural estimates for the numbers $M(n, r_2)$ to classify number fields of degree n and signature (r_1, r_2) with minimum regulator: if these estimates were true, the novelty of our result would consist in substituting the term $n \log n$ in Remak-Friedman's inequality with the term $2 \log M(n, r_2)$, which for several signatures could produce consistent improvements.

We begin by looking at signature $(6, 1)$: in Section 6.2.1, we pointed out that, assuming $R_0 = 7.14$, a number field with signature $(6, 1)$ and $R_K \leq R_0$ has discriminant d_K bounded in absolute value by $\exp(43.7698)$ thanks to Remak-Friedman's inequality, and that this quantity is unfeasible by the classification method because $4g(\exp(-43.7698))$ is a negative number with huge absolute value.
But now let us use the conjectural term $2 \log M(8, 1) = 2 \log 64 = 12 \log 2$ instead of the classic term $8 \log 8 = 24 \log 2$. Then, with the same choice of R_0, we get that a number field of the desired signature with $R_K \leq R_0$ must have $|d_K| \leq \exp(35.452)$: this result is much better because $4g(\exp(-35.452)) = 136.8956\dots > R_0$ and it allows to reduce the range of discriminants that should be considered. From the fact that we know that there exactly 8 fields with signature $(6, 1)$ and $|d_K| \leq 79259702$, and that $4g(1/79259702) = 7.48749\dots$, we get that a number field with $R_K \leq 7.14$ must be in our complete list of 8 fields, and the precise computation of the regulators show that there is a unique field of this kind, which is the one generated by the polynomial $x^8 - 5x^6 - x^5 + 7x^4 + 4x^3 - 4x^2 - 2x + 1$, which has minimum discriminant -65106259 and regulator $7.13506\dots$
We could actually get something more: in fact, the computation $4g(1/79259702) = 7.48749\dots$ suggest to try to use our conjectural improvement to detect the number fields with signature $(6, 1)$ and $R_K \leq 7.48$: then the improvement on Remak-Friedman's estimate would give $|d_K| \leq \exp(35.6632)$, and $4g(\exp(-35.6632)) = 102.264\dots > 7.48$.

Theorem 29. *Suppose the value of $M(8,1)$ given in Table 6.1 is correct. Then there exist exactly 4 number fields K of signature $(6,1)$ with regulator $R_K \leq 7.48$, and they are the 4 fields with this signature and $|d_K| = 65106259, 68494627, 68856875, 69367411$, having $R_K = 7.13506\ldots, 7.38088\ldots, 7.41473\ldots, 7.4303\ldots$ respectively.*

It seems however that $(6,1)$ is the only signature in degree 8 for which one can obtain results by the conjectural estimates. Surely signature $(2,3)$ is not affected because we know that $M(8,3) = 8^{8/2}$ by Lemma 8, so that in this case we are still stuck with the previous estimate given by Remak-Friedman's inequality.
For what concerns signature $(4,2)$, we would have an improvement given by using the (conjectured) correct value $2\log M(8,2) = 2\log\left(7^{7/2}\right) = 7\log 7$ instead of the upper bound $8\log 8$. Unfortunately, using again $R_0 = 2.298$ as in Section 6.2.1, the new estimate would imply that number fields with signature $(4,2)$ and $R_K \leq R_0$ must have $|d_K| \leq \exp(35.3463)$, and $4g(\exp(-35.3463)) = -166.2009\ldots$; not even the adaptations described in [3] seems to work.
The only thing we can conclude for signature $(4,2)$ is that a field K with $R_K \leq 2.298$ must be either the field generated by the polynomial $x^8 - x^6 - 6x^5 + 3x^3 + x^2 + 2x - 1$, having discriminant 15243125 and regulator $2.2977\ldots$ or some possible field K with $|d_K| \in (20829049, \exp(35.3463))$.

We could get some improvement for the signature $(3,1)$ by means of the conjectural value $M(5,1) = 16.6965\ldots$, and this application would give a better classification than the one used in [3].
In fact, suppose we want to detect all the number fields with this signature which have $R_K \leq 1.73$. The usual estimate by Remak-Friemdman's inequality would give the geometric bound $|d_K| \leq \exp(18.5126)$: being this upper bigger than $c_{\partial_K} := 391125.11$, which is the lower bound for which fields of signature $(3,1)$ admit non-principal different ideal, we must use the factor 2 instead of the factor 4 in our computations, and one has $2g(\exp(-18.)) = 1.5608\ldots$.
If instead we replace the factor $5\log 5$ with $2\log M(5,1) = 2\log(16.6965)\ldots$, the new geometric bound becomes $|d_K| \leq \exp(16.8961)$ and one has $2g(\exp(-16.8961)) = 3.404\ldots$
The paper [3] already presented the computation $2g(1/c_{\partial_K}) = 2.158\ldots$ and so we must just look for smaller upper bounds using the factor 4 in the computations. We have in fact $4g(1/48000) = 2.157\ldots$, and thus we get that any field of signature $(3,1)$ with $R_K \leq 2.15$ must have $|d_K| \leq 48000$. Studying the list containing these fields coming from the Klüners-Malle Database [37], we get the following result.

Theorem 30. *Suppose the value of $M(5,1)$ given in Table 6.1 is correct. Then any number field with signature $(3,1)$ and $|d_K| > 48000$ must have $R_K > 2.15$; among the 145 fields of this signature with $|d_K| \leq 48000$ there exist exactly 40 fields with $R_K \leq 2.15$, and they satisfy $|d_K| \leq 25679$.*

Remark 35. If one computes the regulators of the fields of signature $(3,1)$ with $|d_K| \leq 48000$ using the suitable command in PARI/GP, one notices that the sufficient condition

given by Inequality (6.7) is not always satisfied, because for some of these fields we get values of m which are greater than 2.
This problem can be avoided by looking at the decomposition of the prime 2 in $\mathcal{O}_K$: in fact, one can verify that for each one of these fields there exists at least one prime ideal of $\mathcal{O}_K$ with norm 2, and most of the times there are two ideals of norm 2: so one can replace the denominator of Inequality (6.7) with

$$4 \cdot \left(g\left(\frac{1}{|d_K|}\right) + c \cdot g\left(\frac{4}{|d_K|}\right)\right) \tag{6.14}$$

where $c \in \{1, 2\}$ depending on the number of ideals of norm 2 in K, and this replacement allows to get $m < 2$, so that the computed regulators are in fact the true ones.

Finally, let us see what would happen in the degree 7 and signature $(5, 1)$ if the value $M(7, 1) = 2 \cdot 16.6965\ldots$ is correct: we want to classify the number fields of signature $(5, 1)$ with $R_K \leq 8$.
Putting $R_0 := 8$, the geometric bound given by Remak-Friedman inequality would give the value $\exp(37.0334) > \exp(20.1) =: c_{\partial_K}$, which would not be useful because $2g(\exp(-37.0334)) = -527.6403\ldots$. By replacing the factor $7 \log 7$ with $2 \log M(7, 1) = 2 \log(2 \cdot 16.6965\ldots)$, we obtain instead the upper bound $|d_K| \leq \exp(30.4288)$ which is way better because $2g(\exp(-30.4288)) = 10.2565\ldots > R_0$.
Now, $2g(1/c_{\partial_K}) = 13.705\ldots$ and so we can use the factor 4: one verifies that $4g(1/(2 \cdot 10^7)) = 8.1578\ldots$, and so we must look at the 528 number fields of signature $(5, 1)$ with $|d_K| \leq 2 \cdot 10^7$. Just as for the previous remark, the values of the regulators of these fields given by PARI/GP are correct, because either the integer number m in Inequality (6.7) is less than 2, or it becomes less than 2 when one replaces the denominator of Inequality (6.7) with the term (6.14), and so we get the following theorem.

Theorem 31. *Suppose the value of $M(7, 1)$ given in Table 6.1 is correct. Then any number field with signature $(5, 1)$ and $|d_K| > 2 \cdot 10^7$ must have $R_K > 8$; among the 528 fields of this signature with $|d_K| \leq 2 \cdot 10^7$ there exist exactly 135 fields with $R_K \leq 8$, and they satisfy $|d_K| \leq 11755159$.*

This theorem would be an improvement to the result of [24].

Part IV

Appendix

Data from the algorithms

In this appendix section, we present some computational data related to the runs of the algorithmic procedure for the classification of number fields with bounded discriminant described in Chapter 5. We recall that the programs used by the author and the polynomials found during the runs of the procedure can be found at
http://www.mat.unimi.it/users/battistoni/index.html.
Every presented table depends on:

- Signature of the investigated fields;
- Value of the parameter N, which is the absolute value of either a_8 or a_9, depending on the degree of the fields being either 8 or 9;
- Parity of the evaluation in 1 of the polynomials $p(x)$ produced in the algorithm: the difference is chosen in order to expose that almost every polynomial providing the suitable fields derives from a case where $p(1)$ is odd.

Every table presents the following values:

- A value for the coefficient a_1, ranging from 0 to -4;
- A value for the coefficient a_8 (a_9) which can be either N or $-N$;
- The time spent for the computations in the run launched with the given data;
- The number of polynomials created in the corresponding run;
- The number of polynomials in the run which survived the test;
- The number of suitable fields (up to isomorphism) detected in the corresponding run.

The algorithm was launched on the computational cluster of the Institut de Mathématiques de Bordeaux, on the cluster HORIZON of Dipartimento di Matematica dell'Università degli Studi di Milano and on the cluster INDACO of Università degli Studi di Milano.

Remark 36. At some point in the tables, the number of polynomials surviving the test decrease drastically respect to the previous data. This difference is due to the introduction of the coredisc() condition described in Chapter 5, which was implemented during the Atelier PARI/GP which took place in Bordeaux during January 2019.

Signature (2,3)

Table 6.2: $N = 1, p(1)$ odd

a_1	a_8	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
0	1	9 m, 36 s	86675321	708698	46
0	-1	12 m, 47 s	87266074	1405030	51
1	1	18 m, 36 s	130082902	1365507	49
1	-1	23 m, 19 s	130837280	2422481	51
2	1	20 m, 40 s	125942700	1553596	53
2	-1	25 m, 15 s	126723535	2652440	53
3	1	28 m, 53 s	126267044	1569951	50
3	-1	32 m, 0 s	126759623	2495219	51
4	1	46 m, 8 s	153516283	1283199	56
4	-1	48 m, 39 s	153758399	1777727	54

Table 6.3: $N = 1, p(1)$ even

a_1	a_8	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
0	1	3 m, 55 s	21428574	1066	0
0	-1	4 m, 18 s	21563567	2662	1
1	1	8 m, 4 s	33563227	3061	0
1	-1	7m, 53 s	33744575	6067	1
2	1	10 m, 34 s	32889347	4734	0
2	-1	10 m, 9 s m	33079350	8864	0
3	1	16 m, 2 s	33130978	3708	0
3	-1	15 min, 48 s	33272615	5673	1
4	1	34 m, 51 s	35142317	3522	0
4	-1	35 m, 34 s	35190489	6572	1

Signature (4,2)

Table 6.4: $N = 1, p(1)$ odd

a_1	a_8	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
0	1	1 h, 37 m, 44 s	1277978266	1120766	31
0	-1	1 h, 40 m, 25 s	1280596696	601865	27
1	1	3h, 15 m, 10 s	1959119583	2706272	36
1	-1	3 h, 9 m, 1 s	1962391324	1222348	35
2	1	3h, 17 m, 26 s	1643511207	3045442	33
2	-1	3 h, 11 m, 9 s	1646498913	1047607	34
3	1	4 h, 5 m, 5 s	1618437106	3664299	35
3	-1	4 h, 54 m, 15 s	1621282936	1652741	35
4	1	6 h, 29 m, 48 s	1753331082	3606483	36
4	-1	6 h, 26 m, 44 s	1754659076	2721034	36

Table 6.5: $N = 1, p(1)$ even

a_1	a_8	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
0	1	1 h, 0 m, 50 s	306988761	2726	0
0	-1	55 m, 56 s	307590353	1310	0
1	1	2 h, 22 m, 34 s	521827017	6448	0
1	-1	2 h, 26 m, 58 s	522749091	2307	0
2	1	2h, 36 m, 34 s	400989306	7460	1
2	-1	2 h, 38 m, 11 s	401699553	2417	0
3	1	3 h, 34 m, 0 s	391723479	9779	0
3	-1	3 h, 8 m, 3 s	392393757	4991	0
4	1	5 h, 54 m, 50 s	455177646	11844	0
4	-1	5 h, 56 m, 39 s	455503227	9286	0

Signature (6,1)

Table 6.6: $N = 1, p(1)$ odd

a_1	a_8	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
0	1	19 h, 27 m, 3 s	15878290619	5853	4
0	-1	19 h, 40 m, 49 s	15889378178	17834	3
1	1	30 h, 50 m, 36 s	22999940351	9226	7
1	-1	29 h, 36 m, 42 s	23009638906	23145	4
2	1	34 h, 2 m, 24 s	21655304221	12714	6
2	-1	33 h, 11 m, 37 s	21670342460	20288	5
3	1	41 h, 59 m, 23 s	20669410904	18738	7
3	-1	41 h, 13 m, 59 s	20684431832	18290	4
4	1	80 h, 58 m, 12 s	21915140316	22900	5
4	-1	80 h, 52 m, 2 s	21926999910	12289	4

Table 6.7: $N = 1, p(1)$ even

a_1	a_8	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
0	1	12 h, 5 m, 31 s	4006752728	3	0
0	-1	10 h, 28 m, 57 s	4009593574	66	0
1	1	22 h, 44 m, 36 s	5550034483	5	0
1	-1	19 h, 47 m, 17 s	5552358577	83	0
2	1	25 h, 54 m, 10 s	5324018404	7	0
2	-1	25 h, 34 m, 37 s	5327751601	67	0
3	1	35 h, 44 m, 8 s	5281851819	19	0
3	-1	35 h, 8 m, 58 s	5285738866	58	0
4	1	78 h, 38 m, 51 s	5334734422	27	0
4	-1	77 h, 45 m, 14 s	5337685001	34	0

Signature (1,4)

Table 6.8: $N = 1, p(1)$ odd, $a_1 = 0, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
12	2 h, 49 m, 27 s	715088104	3089563	11
10	3 h, 9 m, 44 s	1201171516	4797023	8
8	5 h, 10 m, 20 s	1943438943	7976985	11
6	7 h, 4 m, 32 s	2462855901	10430195	18
4	7 h, 29 m, 11 s	2517993623	11044870	22
2	8 h, 8 m, 9 s	2643279263	11852922	24
0	7 h, 57 m, 47 s	2566834761	11891205	22
-2	8 h, 23 m, 43 s	2644627400	12215694	20
-4	7 h, 47 m, 57 s	2478820937	11490331	19
-6	8 h, 35 m, 18 s	2363593813	10583390	9
-8	7 h, 20 m, 52 s	1997283285	8714424	14
-10	5 h, 59 m, 20 s	1675247720	6703701	8
-12	5 h, 8 m, 50 s	1252879071	4710494	6

Table 6.9: $N = 1, p(1)$ odd, $a_1 = 0, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
12	3 h, 7 m, 18 s	715620502	3270302	9
10	4 h, 48 m, 9 s	1202988900	5170865	9
8	6 h, 21 m, 20 s	1943729657	8660083	19
6	7 h, 39 m, 34 s	2462847356	11644867	24
4	10 h, 20 m, 3 s	2519779091	12386930	29
2	10 h, 37 m, 56 s	2645640318	13281743	20
0	10 h, 8 m, 56 s	2568660876	13093053	36
-2	10 h, 11 m, 7 s	2645581822	13039021	29
-4	9 h, 9 m, 20 s	2478330191	11718153	23
-6	8 h, 19 m, 25 s	2361565243	10270425	25
-8	6 h, 5 m, 50 s	1994470283	8063187	18
-10	5 h, 6 m, 30 s	1672690064	5958283	5
-12	3 h, 36 m, 22 s	1251334957	3856259	11

Table 6.10: $N = 1, p(1)$ odd, $a_1 = -1, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
13	4 h, 41 m, 12 s	952047563	3866319	4
11	6 h, 37 m, 48 s	1558616154	5433798	19
9	10 h, 23 m, 20 s	2494921045	9435874	19
7	15 h, 22 m, 49 s	3557147123	14678721	30
5	16 h, 37 m, 9 s	3785641496	16679614	38
3	16 h, 46 m, 58 s	3828884005	17164254	41
1	17 h, 0 m, 10 s	3832830065	17940374	36
-1	16 h, 54 m, 12 s	3822877795	17923143	37
-3	18 h, 31 m, 58 s	3762853483	17907633	35
-5	13 h, 15 m, 17 s	3615234404	16778405	30
-7	10 h, 26 m, 50 s	3269688842	14600904	21
-9	11 h, 22 m, 23 s	2769039197	11623983	18
-11	9 h, 34 m, 16 s	2096497567	8258592	10

Table 6.11: $N = 1, p(1)$ odd, $a_1 = -1, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
13	5 h, 18 m, 48 s	950202957	5391690	15
11	7 h, 47 m, 53 s	1556110305	7643725	18
9	11 h, 24 m, 5 s	2493608996	12732997	33
7	15 h, 55 m, 38 s	3556887375	19429002	32
5	17 h, 41 m, 50 s	3785354697	22688277	47
3	18 h, 14 m, 38 s	3828868936	23761422	37
1	17 h, 15 m, 47 s	3832854314	24724536	49
-1	17 h, 0 m, 56 s	3823220237	24300024	41
-3	16 h, 21 m, 36 s	3764228299	23444963	48
-5	15 h, 9 m, 18 s	3618172259	21028595	40
-7	13 h, 26 m, 19 s	3274835793	17780238	35
-9	9 h, 46 m, 59 s	2773480926	13767779	29
-11	8 h, 6 m, 39 s	2099537336	9657739	21

Table 6.12: $N = 1, p(1)$ odd, $a_1 = -2, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
12	6 h, 13 m, 29 s	1239519400	2980012	20
10	9 h, 8 m, 9 s	1957520994	4985198	26
8	14 h, 0 m, 24 s	3123125685	8992737	31
6	16 h, 4 m, 36 s	3616843593	11059253	37
4	16 h, 54 m, 51 s	3825661728	12173850	36
2	16 h, 51 m, 16 s	3735947301	12344096	30
0	17 h, 14 m, 42 s	3825543375	13173928	35
-2	16 h, 39 m, 11 s	3674298427	12947661	30
-4	16 h, 14 m, 53 s	3643262296	13031280	25
-6	14 h, 43 m, 25 s	3281758174	11643263	21
-8	13 h, 34 m, 28 s	2978565941	10159860	13
-10	12 h, 19 m, 17 s	2416937863	7810868	17

Table 6.13: $N = 1, p(1)$ odd, $a_1 = -2, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
12	7 h, 23 m, 45 s	1233930720	5655239	18
10	11 h, 12 m, 1 s	1952394908	9124727	23
8	15 h, 27 m, 33 s	3121233139	15820322	33
6	17 h, 25 m, 25 s	3614703383	19917140	43
4	16 h, 27 m, 54 s	3823031427	22009048	37
2	20 h, 1 m, 30 s	3733483113	22361141	38
0	20 h, 19 m, 33 s	3822843586	23333309	44
-2	19 h, 40 m, 15 s	3671777272	22416200	47
-4	19 h, 7 m, 2 s	3641792420	21832704	34
-6	17 h, 7 m, 2 s	3641792420	21832704	34
-8	16 h, 5 m, 2 s	2981353759	16229576	40
-10	13 h, 45 m, 23 s	2418670854	12033190	30

Table 6.14: $N = 1, p(1)$ odd, $a_1 = -3, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
13	10 h, 3 m, 3 s	1269199540	3023598	13
11	13 h, 57 m, 20 s	1959314162	4854507	13
9	19 h, 17 m, 11 s	3091275511	7931980	31
7	24 h, 6 m, 31 s	4300233823	11250694	33
5	25 h, 31 m, 30 s	4673327487	12698948	32
3	25 h, 9 m, 57 s	4748218467	13272736	36
1	25 h, 21 m, 57 s	4658106986	13890402	37
-1	25 h, 20 m, 50 s	4464518947	14003141	26
-3	24 h, 56 m, 11 s	4185895829	13907828	30
-5	24 h, 29 m, 51 s	3834723637	13009017	23
-7	23 h, 31 m, 49 s	3422501725	11637493	17
-9	22 h, 40 m, 29 s	3021506300	9773606	12
-11	21 h, 16 m, 16 s	2564976695	7528537	5

Table 6.15: $N = 1, p(1)$ odd, $a_1 = -3, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
13	11 h, 13 m, 27 s	1264947933	4573313	15
11	15 h, 54 m, 33 s	1952998953	7389536	18
9	22 h, 29 m, 52 s	3085567875	13816914	23
7	33 h, 29 m, 46 s	4296889053	20951361	42
5	35 h, 12 m, 32 s	4668409371	24454171	46
3	35 h, 35 m, 12 s	4742328112	26063227	46
1	35 h, 44 m, 34 s	4653043055	27819797	47
-1	35 h, 15 m, 47 s	4460759238	27925149	56
-3	34 h, 22 m, 33 s	4182939868	27746647	46
-5	33 h, 18 m, 58 s	3833535936	25804470	42
-7	31 h, 5 m, 8 s	3421965105	22880311	43
-9	27 h, 50 m, 0 s	3021688014	18694662	25
-11	24 h, 35 m, 49 s	2564837262	13693046	18

Table 6.16: $N = 1, p(1)$ odd, $a_1 = -4, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
14	25 h, 53 m, 5 s	1770114944	2917701	11
12	30 h, 9 m, 5 s	2413918068	4051358	18
10	39 h, 47 m, 19 s	3808161747	6174230	17
8	55 h, 6 m, 37 s	5622079701	8812898	24
6	63 h, 41 m, 30 s	6685243469	10601811	30
4	62 h, 16 m, 55 s	6701517494	11153786	37
2	64 h, 58 m, 58 s	6713518838	11534049	31
0	61 h, 50 m, 58 s	6305445484	11411130	37
-2	63 h, 43 m, 30 s	6042332433	11279919	28
-4	60 h, 43 m, 18 s	5466644280	10606410	23
-6	60 h, 3 m, 59 s	5047862607	9849417	24
-8	62 h, 25 m, 42 s	4448941128	8595628	17
-10	61 h, 45 m, 49 s	3997796362	7081048	8

Table 6.17: $N = 1, p(1)$ odd, $a_1 = -4, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
14	26 h, 33 m, 10 s	1767371292	3261990	13
12	32 h, 31 m, 33 s	2410544431	5311697	17
10	45 h, 52 m, 16 s	3804347753	10410880	20
8	63 h, 46 m, 43 s	5619726696	18274683	43
6	74 h, 22 m, 24 s	6682574635	23255389	45
4	74 h, 33 m, 28 s	6696916509	26100742	50
2	70 h, 14 m, 33 s	6709680737	28628511	47
0	65 h, 6 m, 42 s	6303019661	29547537	51
-2	61 h, 55 m, 10 s	6041344065	30049853	10
-4	59 h, 20 m, 36 s	5466465207	28670509	43
-6	58 h, 34 m, 2 s	5048210948	26522248	37
-8	43 h, 59 m, 38 s	4448857827	22645529	36
-10	38 h, 2 m, 51 s	3995990083	18105752	20

Table 6.18: $N = 1, p(1)$ even, $a_1 = 0, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
12	0 h, 37 m, 12 s	180981151	4641	0
10	0 h, 56 m, 54 s	303920608	7069	0
8	1 h, 27 m, 4 s	4292097044	12068	0
6	1 h, 49 m, 4 s	623716942	15535	0
4	1 h, 50 m, 0 s	637577825	17437	0
2	1 h, 56 m, 28 s	669340606	18660	0
0	1 h, 54 m, 27 s	650072123	18546	0
-2	1 h, 57 m, 14 s	669757717	19321	0
-4	1 h, 46 m, 53 s	627773919	18178	0
-6	1 h, 46 m, 1 s	59868848	17113	1
-8	1 h, 41 m, 15 s	506084734	14211	2
-10	1 h, 35 m, 35 s	424585186	11356	2
-12	1 h, 21 m, 13 s	317543910	7894	0

Table 6.19: $N = 1, p(1)$ even, $a_1 = 0, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
12	0 h, 42 m, 39 s	181133619	4530	0
10	1 h, 7 m, 1 s	304409338	7504	0
8	1 h, 39 m, 9 s	492215007	12273	0
6	2 h, 1 m, 19 s	623768384	16857	1
4	1 h, 59 m, 7 s	638077079	17958	0
2	1 h, 58 m, 25 s	669979397	18965	0
0	1 h, 50 m, 27 s	650576166	18369	0
-2	1 h, 50 m, 27 s	650576166	18369	2
-4	1 h, 44 m, 13 s	627707321	16435	0
-6	1 h, 43 m, 36 s	598237613	14133	0
-8	1 h, 30 m, 17 s	505422221	11407	2
-10	1 h, 22 m, 31 s	423969933	7989	0
-12	1 h, 11 m, 33 s	317170785	5500	0

Table 6.20: $N = 1, p(1)$ even, $a_1 = -1, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
13	1 h, 14 m, 43 s	245056824	3289	0
11	1 h, 41 m, 42 s	400832110	5213	1
9	2 h, 34 m, 51 s	641745954	8448	0
7	3 h, 40 m, 7 s	915053718	16400	0
5	3 h, 53 m, 58 s	974040284	17183	0
3	3 h, 55 m, 23 s	985304904	19818	0
1	3 h, 55 m, 58 s	986380297	19101	0
-1	3 h, 52 m, 23 s	983701867	22014	2
-3	3 h, 47 m, 55 s	967948644	20122	1
-5	3 h, 39 m, 19 s	929569753	21246	3
-7	3 h, 26 m, 51 s	840245421	15930	1
-9	3 h, 12 m, 52 s	71125794	14888	0
-11	2 h, 56 m, 53 s	538842873	9462	0

Table 6.21: $N = 1, p(1)$ even, $a_1 = -1, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
13	1 h, 17 m, 1 s	244611064	8057	0
11	1 h, 46 m, 52 s	400260951	11869	0
9	2 h, 41 m, 54 s	641415737	18317	0
7	3 h, 45 m, 39 s	915049909	30517	0
5	4 h, 0 m, 10 s	974009096	33854	0
3	4 h, 2 m, 59 s	985323271	37540	2
1	4 h, 1 m, 59 s	986419342	37136	0
-1	3 h, 22 m, 46 s	983814157	38968	1
-3	3 h, 5 m, 6 s	968346418	25850	0
-5	3 h, 38 m, 38 s	930385463	35297	2
-7	3 h, 19 m, 33 s	841449497	28534	0
-9	3 h, 2 m, 27 s	712486628	24329	1
-11	2 h, 53 m, 1 s	539687890	15396	0

Table 6.22: $N = 1, p(1)$ even, $a_1 = -2, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
12	2 h, 9 m, 39 s	317413108	5655	0
10	3 h, 5 m, 32 s	501792213	1033	0
8	4 h, 44 m, 3 s	801565312	17442	0
6	5 h, 26 m, 21 s	928347526	22971	0
4	5 h, 35 m, 43 s	981955439	23432	0
2	5 h, 30 m, 43 s	958984102	26054	1
0	5 h, 34 m, 39 s	981941771	26167	1
-2	5 h, 22 m, 57 s	943092422	283851	0
-4	5 h, 23 m, 7 s	935193850	27016	1
-6	5 h, 4 m, 29 s	842599656	26194	2
-8	4 h, 49 m, 46 s	765071591	21484	1
-10	4 h, 31 m, 22 s	620688955	18116	0

Table 6.23: $N = 1, p(1)$ even, $a_1 = -2, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
12	2 h, 13 m, 1 s	315944916	13316	0
10	3 h, 9 m, 54 s	500418841	23190	1
8	4 h, 41 m, 27 s	801011779	37258	0
6	5 h, 23 m, 31 s	927741101	50810	0
4	5 h, 35 m, 41 s	981239279	51034	0
2	5 h, 31 m, 4 s	958325310	57759	1
0	5 h, 33 m, 6 s	981217781	56120	0
-2	5 h, 25 m, 7 s	942403257	59148	0
-4	5 h, 22 m, 4 s	934749306	53626	0
-6	5 h, 2 m, 4 s	842635024	51157	1
-8	4 h, 54 m, 26 s	765708280	41584	0
-10	4 h, 36 m, 21 s	621056508	33142	0

Table 6.24: $N = 1, p(1)$ even, $a_1 = -3, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
13	4 h, 21 m, 22 s	328683178	8334	0
11	5 h, 55 m, 9 s	507527427	14491	1
9	8 h, 58 m, 5 s	801177265	21270	0
7	12 h, 9 m, 52 s	1115365637	31847	1
5	12 h, 37 m, 44 s	1211890925	33224	1
3	12 h, 39 m, 50 s	1231298356	37086	0
1	12 h, 35 m, 20 s	1207979608	36242	0
-1	12 h, 21 m, 22 s	1158012599	39724	1
-3	12 h, 19 m, 48 s	1085735704	37661	0
-5	11 h, 58 m, 6 s	994951283	38210	0
-7	10 h, 17 m, 33 s	887939876	32494	0
-9	10 h, 4 m, 23 s	784126337	29508	0
-11	9 h, 49 m, 31 s	665427059	21914	0

Table 6.25: $N = 1, p(1)$ even, $a_1 = -3, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
13	4 h, 19 m, 12 s	327563950	17059	0
11	5 h, 51 m, 34 s	505857067	27001	0
9	8 h, 52 m, 58 s	799639423	50158	0
7	11 h, 43 m, 28 s	1114412118	76152	0
5	12 h, 12 m, 39 s	1210538290	89096	0
3	12 h, 10 m, 54 s	1229694740	95104	1
1	12 h, 8 m, 20 s	1206598841	100704	1
-1	11 h, 57 m, 46 s	1156982645	103803	1
-3	11 h, 52 m, 25 s	1084931296	101493	1
-5	11 h, 30 m, 21 s	994601295	97000	0
-7	10 h, 31 m, 2 s	887771189	82367	0
-9	9 h, 58 m, 4 s	784147769	71372	0
-11	9 h, 45 m, 42 s	665355587	49813	0

Table 6.26: $N = 1, p(1)$ even, $a_1 = -4, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
14	16 h, 6 m, 31 s	473049490	12729	0
12	18 h, 45 m, 10 s	645045967	18323	0
10	25 h, 7 m, 17 s	1017411515	25824	0
8	32 h, 27 m, 2 s	1501594083	39215	0
6	36 h, 18 m, 54 s	1785597226	44311	0
4	36 h, 2 m, 27 s	1790288412	49854	0
2	36 h, 56 m, 10 s	1793441875	48178	0
0	35 h, 19 m, 15 s	1684282951	51381	0
-2	34 h, 2 m, 36 s	1613829211	47633	0
-4	32 h, 34 m, 28 s	1459974737	49038	0
-6	34 h, 12 m, 51 s	1348064219	41976	0
-8	34 h, 26 m, 36 s	1188159088	10370	0
-10	35 h, 44 m, 52 s	1067873319	30257	0

Table 6.27: $N = 1, p(1)$ even, $a_1 = -4, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
14	12 h, 52 m, 30 s	472323970	10499	0
12	17 h, 55 m, 19 s	644159192	17844	0
10	26 h, 0 m, 21 s	1016393497	31285	0
8	40 h, 40 m, 16 s	1501017244	57368	0
6	44 h, 20 m, 6 s	1784965530	66788	0
4	43 h, 58 m, 43 s	1789127055	79544	0
2	41 h, 41 m, 52 s	1792456576	80997	0
0	40 h, 22 m, 4 s	1683670629	88620	0
-2	40 h, 54 m, 14 s	1613594274	83279	0
-4	39 h, 43 m, 50 s	1459954324	82931	0
-6	40 h, 45 m, 43 s	1348179317	69800	0
-8	29 h, 26 m, 50 s	1188161047	62998	0
-10	29 h, 52 m, 31 s	1067422097	45300	0

Signature (3,3)

Table 6.28: $N = 1, p(1)$ odd, $a_1 = 0, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
14	55 h	17015964408	45779640	17
12	80 h	30022075232	61032018	44
10	99 h	36237723088	77707862	41
8	120 h	53996268076	117327990	40
6	127 h	61785162223	138516643	30
4	158 h	57701291906	147005961	29
2	164 h	63219360099	156173710	25
0	149 h	62123299154	157407745	26
-2	150 h	63292940569	159883723	25
-4	138 h	61878281673	153280925	29
-6	152 h	62113020140	145335065	14
-8	155 h	58606399906	128557694	7
-10	117 h	55130750026	119915818	4
-12	108 h	47912891080	92121947	3
-14	97 h	41344192605	74619239	1

Table 6.29: $N = 1, p(1)$ odd, $a_1 = 0, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
14	52 h	20575378882	62392638	14
12	80 h	26618497796	80221561	27
10	124 h	40347460405	110804057	32
8	157 h	58582545203	142407810	38
6	138 h	61794588643	155202485	31
4	145 h	61830457113	146672107	36
2	215 h	63230831374	137597618	22
0	185 h	62131360703	122314500	28
-2	191 h	63298625016	109726743	23
-4	193 h	61879732650	93441580	21
-6	160 h	62105461945	79477910	10
-8	123 h	54374018265	63828674	18
-10	100 h	55096212663	51004031	7
-12	103 h	47875887120	40515250	6
-14	111 h	41313015452	32368372	3

Table 6.30: $N = 1, p(1)$ odd, $a_1 = -1, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
15	85 h	29095606403	99807888	31
13	120 h	38611699318	127777785	52
11	151 h	50781160750	174145749	63
9	220 h	72734577998	250859359	78
7	245 h	87439454679	292942337	76
5	267 h	88399788207	323180365	79
3	274 h	88417802130	332685782	51
1	275 h	91735747480	317272084	67
-1	271 h	124704524357	306796920	38
-3	268 h	88255909727	294249191	48
-5	252 h	87381267143	270658613	24
-7	231 h	88573154172	350682234	22
-9	215 h	79457871937	204656605	14
-11	196 h	77204082187	173977912	15
-13	192 h	66427919478	139708256	5

Table 6.31: $N = 1, p(1)$ odd, $a_1 = -1, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
15	114 h	29077911610	99179465	31
13	95 h	51988907711	123722988	54
11	182 h	51608602513	171930667	55
9	286 h	70180008167	229526371	71
7	230 h	86839133156	253826914	56
5	256 h	91714932556	279732771	85
3	252 h	91724941645	251992426	56
1	247 h	91735747480	265396072	63
-1	238 h	91730356718	245664322	50
-3	230 h	91565604647	238878100	48
-5	222 h	90897046131	204702550	32
-7	205 h	88600288625	182841140	26
-9	188 h	84045458498	152092880	8
-11	174 h	77239687368	125631725	10
-13	174 h	66451037133	95267201	3

Table 6.32: $N = 1, p(1)$ odd, $a_1 = -2, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
16	100 h	26288813372	111905517	20
14	113 h	32016720320	121057800	50
12	150 h	43616621966	166704490	52
10	209 h	55836571696	235694637	67
8	282 h	81063773550	322407478	71
6	321 h	88605033664?	355160899	75
4	327 h	9112941836	366596467	67
2	324 h	89674301116	356497435	64
0	318 h	91285059848	354416496	47
-2	318 h	89222564523	333955534	41
-4	316 h	89771652261	320704593	37
-6	296 h	86383152280	289849920	27
-8	278 h	83988000414	261651424	29
-10	253 h	76938408441	222402892	13
-12	235 h	70146406144	18689279	7
-14	196 h	59430450455	144171160	11

Table 6.33: $N = 1, p(1)$ odd, $a_1 = -2, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
16	94 h	26224800683	104432524	22
14	119 h	31970067935	131075842	38
12	156 h	44088681659	178223404	46
10	211 h	60402418070	224724733	57
8	270 h	80985624618	283388366	69
6	287 h	88593433768	274588021	79
4	290 h	91117926440	289076983	66
2	287 h	86555547198	273147896	59
0	279 h	91273044433	263608876	47
-2	290 h	89207697297	237761675	33
-4	282 h	89753710941	21766240	25
-6	240 h	86367783982	185353662	23
-8	231 h	84004207741	157760017	11
-10	208 h	76851647775	123356446	8
-12	192 h	69455927505	95140716	6
-14	171 h	59643849841	64189314	3

Table 6.34: $N = 1, p(1)$ odd, $a_1 = -3, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
15	124 h	28567207507	5050	43
13	158 h	40433919183	3957	50
11	213 h	56362376831	6282	62
9	298 h	78630037106	8358	82
7	350 h	93922206854	6355	67
5	357 h	98398730074	6530	58
3	359 h	98789808403	9151	69
1	406 h	98136982155	4999	56
-1	437 h	92194062297	5705	43
-3	422 h	93244611010	5754	27
-5	405 h	88925795473	3633	36
-7	333 h	80782784505	2886	18
-9	310 h	77529587310	3250	15
-11	340 h	71025607426	1265	8
-13	277 h	6364057276	1142	11

Table 6.35: $N = 1, p(1)$ odd, $a_1 = -3, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
15	125 h	29854787617	4828	31
13	203 h	40375529767	3448	46
11	208 h	56313791682	5297	58
9	284 h	79207983927	6867	61
7	355 h	93894229325	5332	56
5	339 h	91188000930	5472	51
3	344 h	98749398649	7269	63
1	335 h	96102585537	3890	43
-1	332 h	94261151607	4497	26
-3	314 h	93215701183	4297	29
-5	300 h	89002226922	2630	30
-7	291 h	83765445516	2064	16
-9	271 h	77518125614	2169	15
-11	262 h	70919224320	838	8
-13	248 h	66340066573	634	7

Table 6.36: $N = 1, p(1)$ odd, $a_1 = -4, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
16	248 h	41262980119	3367	35
14	287 h	51902260298	4376	28
12	391 h	59372936714	5265	75
10	526 h	83244965904	5265	68
8	654 h	108374289655	6001	71
6	782 h	117411732308	6568	59
4	721 h	119151108617	5992	81
2	710 h	111608757159	5711	56
0	691 h	108374289655	5042	73
-2	705 h	103445714410	4327	40
-4	659 h	99334260522	3562	42
-6	650 h	96244597564	2839	27
-8	661 h	89592742944	2087	15
-10	604 h	81654304873	1481	12
-12	613 h	73693483437	939	10

Table 6.37: $N = 1, p(1)$ odd, $a_1 = -4, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
16	237 h	33145786637	2886	43
14	294 h	42044593144	3809	30
12	382 h	83200045829	4203	51
10	521 h	83140593879	5145	48
8	607 h	108346909124	4993	49
6	676 h	117376838881	5065	58
4	693 h	156394540057	4714	49
2	669 h	114744318133	4394	49
0	668 h	113114459513	3687	49
-2	668 h	106928330483	3326	26
-4	912 h	96753160297	2508	27
-6	725 h	95235088343	1942	15
-8	586 h	89587293574	1538	16
-10	580 h	81649858105	953	5
-12	539 h	75617490742	624	8

Table 6.38: $N = 1, p(1)$ even, $a_1 = 0, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
14	17 h	5093036962	21	0
12	21 h	6862070214	69	0
10	28 h	9987839257	29	0
8	36 h	13370533269	75	1
6	45 h	15298403391	59	0
4	39 h	15306487920	73	0
2	77 h	15652930467	48	0
0	39 h	15380958920	85	0
-2	64 h	15670269893	24	0
-4	52 h	15319835462	59	2
-6	39 h	15377997425	27	0
-8	39 h	14509072036	34	0
-10	43 h	13646946739	14	0
-12	91 h	11859063158	31	0
-14	47 h	10232980070	3	0

Table 6.39: $N = 1, p(1)$ even, $a_1 = 0, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
14	18 h	5096983665	15	0
12	21 h	6867117886	61	0
10	36 h	9992655511	29	1
8	90 h	13373033399	64	0
6	45 h	15300627838	53	0
4	44 h	15309300182	68	0
2	44 h	15655703512	28	0
0	58 h	15382898690	46	0
-2	104 h	15671621008	18	0
-4	74 h	15320113657	50	0
-6	54 h	15375969901	36	1
-8	40 h	14503566777	24	0
-10	39 h	13638177444	13	0
-12	79 h	11849732065	19	0
-14	96 h	10225140873	2	0

Table 6.40: $N = 1, p(1)$ even, $a_1 = -1, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
15	34 h	7362299450	115	0
13	41 h	9772638801	78	0
11	80 h	13067535030	167	0
9	77 h	18414920982	237	0
7	143 h	22138917992	238	0
5	153 h	23217081098	152	1
3	100 h	23224473277	243	0
1	133 h	23227209720	231	1
-1	314 h	23225798547	212	0
-3	100 h	23183767426	130	0
-5	108 h	22962367844	139	1
-7	158 h	22428238666	128	0
-9	93 h	21274756135	107	0
-11	144 h	19551926516	43	0
-13	94 h	16818643596	45	0

Table 6.41: $N = 1, p(1)$ even, $a_1 = -1, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
15	33 h	7357562246	108	0
13	73 h	9769417571	103	0
11	57 h	13065517469	178	1
9	76 h	18413484262	194	0
7	125 h	22138776036	202	0
5	100 h	23217030066	167	0
3	100 h	22387113455	183	0
1	189 h	23227209720	202	0
-1	135 h	23225864456	156	0
-3	100 h	23184406829	118	1
-5	100 h	22964486908	124	0
-7	113 h	22432982385	109	0
-9	146 h	21282085713	72	0
-11	91 h	19560670883	36	0
-13	128 h	16825607202	32	0

Table 6.42: $N = 1, p(1)$ even, $a_1 = -2, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
16	65 h	6725582403	65	0
14	55 h	8189909019	43	0
12	67 h	11285305845	80	0
10	97 h	15451110605	63	0
8	140 h	20724347155	129	1
6	204 h	22652784610	80	0
4	229 h	23298374530	115	1
2	186 h	22926267255	81	0
0	130 h	23338284839	106	0
-2	218 h	22811218995	71	0
-4	132 h	22951618925	71	0
-6	194 h	22084610069	50	0
-8	156 h	21475351802	55	0
-10	295 h	19665653073	25	0
-12	243 h	17927761361	27	0
-14	130 h	15240926152	10	0

Table 6.43: $N = 1, p(1)$ even, $a_1 = -2, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
16	51 h	6714435168	67	0
14	66 h	8178119899	43	0
12	93 h	11275403715	85	0
10	90 h	15444501962	50	0
8	212 h	20720601429	112	0
6	170 h	22649898110	75	2
4	204 h	23295488515	102	0
2	200 h	22923807891	73	0
0	179 h	23335258055	84	0
-2	201 h	22807483572	46	0
-4	187 h	22947141205	66	0
-6	157 h	22080839980	33	1
-8	153 h	21474597811	37	0
-10	211 h	19669274051	18	1
-12	244 h	17934434667	26	1
-14	129 h	15244584506	3	0

Table 6.44: $N = 1, p(1)$ even, $a_1 = -3, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
15	203 h	6856769804	145	0
13	116 h	9272659704	93	0
11	259 h	12929827112	151	0
9	204 h	18158342547	270	0
7	258 h	21551444067	198	0
5	259 h	22576668438	173	0
3	302 h	22666289748	243	2
1	341 h	22517299137	170	0
-1	277 h	22094996893	189	1
-3	243 h	21395596559	136	0
-5	250 h	20404733350	101	0
-7	268 h	19225352797	96	0
-9	260 h	17791063493	95	0
-11	242 h	16295059035	31	0
-13	251 h	14604684396	31	0

Table 6.45: $N = 1, p(1)$ even, $a_1 = -3, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
15	121 h	6846015796	166	0
13	146 h	9259377197	65	0
11	154 h	12918526968	170	0
9	359 h	18151470806	244	0
7	325 h	21544855213	199	0
5	243 h	22567758756	109	0
3	306 h	22657440705	243	0
1	342 h	22509270797	166	1
-1	296 h	22087278009	160	0
-3	296 h	21388819004	104	0
-5	316 h	20398719789	92	1
-7	243 h	19221243662	81	0
-9	487 h	17788317796	64	0
-11	313 h	16293929181	22	0
-13	232 h	14604241346	17	0

Table 6.46: $N = 1, p(1)$ even, $a_1 = -4, a_9 = 1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
16	236 h	7984846055	68	0
14	244 h	10128629356	50	0
12	359 h	14292208560	125	0
10	465 h	20040884873	55	0
8	531 h	26094613692	123	0
6	625 h	28269606155	67	0
4	612 h	28687767576	107	0
2	594 h	27755117546	67	1
0	510 h	27241585766	101	0
-2	620 h	25750989627	43	0
-4	590 h	24713234278	67	0
-6	588 h	22934288800	27	0
-8	620 h	21573778690	43	0
-10	576 h	19662300856	19	0
-12	648 h	18209618118	32	0

Table 6.47: $N = 1, p(1)$ even, $a_1 = -4, a_9 = -1$

S_2	time	$\#p(x)$ created	$\#p(x)$ survived	# fields
16	311 h	7978463006	43	0
14	249 h	10120512516	38	0
12	408 h	14281552316	75	0
10	477 h	20030060252	52	1
8	581 h	26087762248	100	0
6	899 h	28261004687	61	0
4	545 h	28678669774	96	0
2	724 h	27747535540	43	0
0	584 h	27235756565	67	0
-2	578 h	25746672166	25	0
-4	588 h	24710103616	52	0
-6	562 h	22931917563	24	0
-8	619 h	21572433546	34	0
-10	556 h	19661174908	14	0
-12	582 h	18208597787	6	0

Higher values of N

The previous tables were all related to runs of the algorithm where the value for the parameter N was 1. A priori, this is not the only value of N which must be investigated: in fact, Theorem 24 holds for every value N such that $N \leq (T/n)^{n/2}$, where n is the degree of the studied fields and T is the upper bound for the second absolute Newton sum given by Hunter-Pohst-Martinet Theorem and depending on the choice of S_1. Thus, for every value of S_1 between 0 and 4, we should run the process for every value of N between 1 and $(T/n)^{n/2}$, and every iteration should be divided in four subcases depending on both the sign of $a_8(a_9)$ and the parity value of the generated polynomials..
Fortunately, many of these values of N can be immediately discarded thanks to assuming the local corrections, and this forces N, which is the absolute norm of an HPM-element, to be not an exact multiple of 2, 3 ,4 and 5. Thus, the number of checks that one should run is much more than expected, and furthermore the values of N are such that every run gives no number field as output, making thus this process just a security check which gives no fields.
In the following tables, we provide the values of N that must be studied by our programs for every considered signature and for every choice of S_1 between 0 and 4. Together with this, we indicate also the values of the parameter x_0 and x_1 which are needed by the author defined function **hpeqU** in order to work correctly with with the indicated values of N. Given that no number field occured as an output, we preferred not reporting any other data for this additional runs: we just say that any iteration can last between few seconds and 10 minutes circa, depending on the signature, the value of S_1 and the value of N. Empirically, the more time consuming runs occur when r_1, S_1 and N are quite big at the same time.

S_1	$(T/n)^{n/2}$	N	x_0, x_1
0	$5.8255\ldots$	\	\
1	$6.0634\ldots$	\	\
2	$6.8210\ldots$	\	\
3	$8.2387\ldots$	$7, 8$	$0, 1.3$
4	$10.5813\ldots$	$7, 8, 9$	$0, 1.3$

Table 6.48: Signature $(2, 3)$

S_1	$(T/n)^{n/2}$	N	x_0, x_1
0	$12.1839\ldots$	$7, 8, 9, 11$	$0, 1.3$
1	$12.5966\ldots$	$7, 8, 9, 11$	$0, 1.3$
2	$13.8979\ldots$	$7, 8, 9, 11, 13$	$0, 1.4$
3	$16.2875\ldots$	$7, 8, 9, 11, 13, 16$	$0, 1.4$
4	$20.1349\ldots$	$7, 8, 9, 11, 13, 16, 17, 19$	$0, 1.45$

Table 6.49: Signature $(4, 2)$

S_1	$(T/n)^{n/2}$	N	x_0, x_1
0	$26.1478\ldots$	$7, 8, 9, 11, 13, 16, 17, 19, 23, 25$	$0, 1.5$
1	$26.8780\ldots$	$7, 8, 9, 11, 13, 16, 17, 19, 23, 25$	$0, 1.5$
2	$29.1606\ldots$	$7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29$	$0, 1.52$
3	$33.2843\ldots$	$7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 33$	$0, 1.54$
4	$39.7737\ldots$	$7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 33, 37$	$0, 1.56$

Table 6.50: Signature $(6, 1)$

S_1	$(T/n)^{n/2}$	N	x_0, x_1
0	$6.2782\ldots$	$\setminus$	$\setminus$
1	$6.5135\ldots$	$\setminus$	$\setminus$
2	$7.2605\ldots$	7	$0, 1.23$
3	$8.6520\ldots$	$7, 8$	$0, 1.23$
4	$10.9390\ldots$	$7, 8, 9$	$0, 1.23$

Table 6.51: Signature $(1, 4)$

S_1	$(T/n)^{n/2}$	N	x_0, x_1
0	$13.1050\ldots$	$7, 8, 9, 11, 13$	$0, 1.34$
1	$13.5211\ldots$	$7, 8, 9, 11, 13$	$0, 1.34$
2	$14.8311\ldots$	$7, 8, 9, 11, 13$	$0, 1.34$
3	$17.2318\ldots$	$7, 8, 9, 11, 13, 16, 17$	$0, 1.36$
4	$21.0887\ldots$	$7, 8, 9, 11, 13, 16, 17, 19$	$0, 1.36$

Table 6.52: Signature $(3, 3)$

Bibliography

[1] L. V. Ahlfors. *Complex analysis*. McGraw-Hill Book Co., New York, third edition, 1978. An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics.

[2] G. E. Andrews, R. Askey, and R. Roy. *Special functions*, volume 71 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1999.

[3] S. Astudillo, F. Diaz y Diaz, and E. Friedman. Sharp lower bounds for regulators of small-degree number fields. *J. Number Theory*, 167:232–258, 2016.

[4] F. Battistoni. The minimum discriminant of number fields of degree 8 and signature $(2, 3)$. *J. Number Theory*, 198:386–395, 2019.

[5] F. Battistoni, S. Bettin, C. David, and C. Delaunay. Preprint.

[6] K. Belabas. A fast algorithm to compute cubic fields. *Math. Comp.*, 66(219):1213–1237, 1997.

[7] M. J. Bertin. Sur une conjecture de Pohst. *Acta Arith.*, 74(4):347–349, 1996.

[8] S. Bettin, C. David, and C. Delaunay. Non-isotrivial elliptic surfaces with non-zero average root number. *J. Number Theory*, 191:1–84, 2018.

[9] J. Buchmann, D. Ford, and M. Pohst. Enumeration of quartic fields of small discriminant. *Math. Comp.*, 61(204):873–879, 1993.

[10] J. W. S. Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[11] J. W. S. Cassels and A. Frölich. *Algebraic number theory: proceedings of an instructional conference*. Academic Pr, 1967.

[12] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[13] H. Cohen, F. Diaz y Diaz, and M. Olivier. Tables of octic fields with a quartic subfield. *Math. Comp.*, 68(228):1701–1716, 1999.

[14] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[15] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[16] F. Diaz y Diaz. *Tables minorant la racine n-ième du discriminant d'un corps de degré n*, volume 6 of *Publications Mathématiques d'Orsay 80 [Mathematical Publications of Orsay 80]*. Université de Paris-Sud, Département de Mathématique, Orsay, 1980.

[17] F. Diaz y Diaz. Petits discriminants des corps de nombres totalement imaginaires de degré 8. *J. Number Theory*, 25(1):34–52, 1987.

[18] F. Diaz y Diaz. Discriminant minimal et petits discriminants des corps de nombres de degré 7 avec cinq places réelles. *J. London Math. Soc. (2)*, 38(1):33–46, 1988.

[19] F. Diaz y Diaz and M. Olivier. Imprimitive ninth-degree number fields with small discriminants. *Math. Comp.*, 64(209):305–321, 1995. With microfiche supplement.

[20] T. Dokchitser. Notes on the parity conjecture. In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pages 201–249. Birkhäuser/Springer, Basel, 2013.

[21] D. Ford, S. Pauli, and X.F. Roblot. A fast algorithm for polynomial factorization over $\mathbb{Q}_p$. *J. Théor. Nombres Bordeaux*, 14(1):151–169, 2002.

[22] E. Friedman. Analytic formulas for the regulator of a number field. *Invent. Math.*, 98(3):599–622, 1989.

[23] E. Friedman. Regulators and total positivity. *Publ. Mat.*, (Proceedings of the Primeras Jornadas de Teoría de Números):119–130, 2007.

[24] E. Friedman and G. Ramirez-Raposo. Filling the gap in the table of smallest regulators up to degree 7. *J. Number Theory*, 198:381–385, 2019.

[25] A. Fuchs and G. Letta. Le problème du premier chiffre décimal pour les nombres premiers. *Electron. J. Combin.*, 3(2):Research Paper 25, approx. 7, 1996. The Foata Festschrift.

[26] F. Gassmann. Bemerkungen zur vorstehenden arbeit von hurwitz. *Math. z*, 25:665–675, 1926.

[27] E. S. Golod and I. R. Šafarevič. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:261–272, 1964.

[28] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[29] E. Hecke. *Lectures on the theory of algebraic numbers*, volume 77 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

[30] A. Hulpke. Constructing transitive permutation groups. *J. Symbolic Comput.*, 39(1):1–30, 2005.

[31] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[32] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[33] F. Jarvis. *Algebraic number theory*. Springer Undergraduate Mathematics Series. Springer, Cham, 2014.

[34] W. Jehne. Kronecker classes of algebraic number fields. *J. Number Theory*, 9(3):279–320, 1977.

[35] S. Karlin. *Total positivity. Vol. I.* Stanford University Press, Stanford, Calif, 1968.

[36] N. Klingen. *Arithmetical similarities*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998. Prime decomposition and finite group theory, Oxford Science Publications.

[37] J. Klüners and G. Malle. A database for number fields. Available at `http://galoisdb.math.upb.de/home`.

[38] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[39] S. Lang. *Complex analysis*, volume 103 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1999.

[40] S. Lang and A. Néron. Rational points of abelian varieties over function fields. *Amer. J. Math.*, 81:95–118, 1959.

[41] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[42] B. Linowitz, D. B. McReynolds, and N. Miller. Locally equivalent correspondences. *Ann. Inst. Fourier (Grenoble)*, 67(2):451–482, 2017.

[43] M. Lochter. Weakly Kronecker equivalent number fields. *Acta Arith.*, 67(4):295–312, 1994.

[44] M. Lochter. New characterizations of Kronecker equivalence. *J. Number Theory*, 53(1):115–136, 1995.

[45] J. Martinet. Methodes géométriques dans la recherche des petits discriminants. In *Séminaire de théorie des nombres, Paris 1983–84*, volume 59 of *Progr. Math.*, pages 147–179, 1985.

[46] Matlab optimization toolbox, 2018 B. The MathWorks, Natick, MA, USA.

[47] D. G. Mead. Newton's identities. *Amer. Math. Monthly*, 99(8):749–751, 1992.

[48] James S. Milne. Fields and galois theory (v4.60), 2018. Available at www.jmilne.org/math/.

[49] K. Nagao. $\mathbf{Q}(T)$-rank of elliptic curves and certain limit coming from the local points. *Manuscripta Math.*, 92(1):13–32, 1997. With an appendix by Nobuhiko Ishida, Tsuneo Ishikawa and the author.

[50] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Science & Business Media, 2013.

[51] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[52] A. M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Sém. Théor. Nombres Bordeaux (2)*, 2(1):119–141, 1990.

[53] R. Perlis. On the equation $\zeta_K(s) = \zeta_{K'}(s)$. *J. Number Theory*, 9(3):342–360, 1977.

[54] M. Pohst. Regulatorabschätzungen für total reelle algebraische Zahlkörper. *J. Number Theory*, 9(4):459–492, 1977.

[55] M. Pohst. On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields. *J. Number Theory*, 14(1):99–117, 1982.

[56] M. Pohst, J. Martinet, and F. Diaz y Diaz. The minimum discriminant of totally real octic fields. *J. Number Theory*, 36(2):145–159, 1990.

[57] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*, volume 30 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1997. Revised reprint of the 1989 original.

[58] G. Poitou. Sur les petits discriminants. In *Séminaire Delange-Pisot-Poitou, 18e année: (1976/77), Théorie des nombres, Fasc. 1 (French)*, pages Exp. No. 6, 18. Secrétariat Math., Paris, 1977.

[59] R. Remak. Über Grössenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers. *Compositio Math.*, 10:245–285, 1952.

[60] M. Rosen and J. H. Silverman. On the rank of an elliptic surface. *Invent. Math.*, 133(1):43–67, 1998.

[61] Raphaël Salem. *Algebraic numbers and Fourier analysis*. D. C. Heath and Co., Boston, Mass., 1963.

[62] M. Schütt and T. Shioda. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul 2008*, volume 60 of *Adv. Stud. Pure Math.*, pages 51–160. Math. Soc. Japan, Tokyo, 2010.

[63] A. Schwarz, M. Pohst, and F. Diaz y Diaz. A table of quintic number fields. *Math. Comp.*, 63(207):361–376, 1994.

[64] S. Selmane. Non-primitive number fields of degree eight and of signature $(2, 3)$, $(4, 2)$ and $(6, 1)$ with small discriminant. *Math. Comp.*, 68(225):333–344, 1999.

[65] S. Selmane. Odlyzko-Poitou-Serre lower bounds for discriminants for some number fields. *Maghreb Math. Rev.*, 8(1-2):151–162, 1999.

[66] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[67] C. L. Siegel. *Lectures on quadratic forms*. Notes by K. G. Ramanathan. Tata Institute of Fundamental Research Lectures on Mathematics, No. 7. Tata Institute of Fundamental Research, Bombay, 1967.

[68] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[69] D. Simon. Petits discriminants de polynomes irréductibles. available at `https://simond.users.lmno.cnrs.fr/maths/TableSmallDisc.html`.

[70] L. Stern. On the equality of norm groups of global fields. *J. Number Theory*, 36(1):108–126, 1990.

[71] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.

[72] K. Takeuchi. Totally real algebraic number fields of degree 9 with small discriminant. *Saitama Math. J.*, 17:63–85 (2000), 1999.

[73] G. Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.

[74] The LMFDB Collaboration. The L-functions and modular forms database. available at http://www.lmfdb.org, 2013.

[75] The PARI Group, Univ. Bordeaux. *PARI/GP version* 2.11.0, 2018. available at http://pari.math.u-bordeaux.fr/.

[76] N. Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.*, 95(1):191–228, 1926.

[77] WikiGroup. Groupprops. available at https://groupprops.subwiki.org/wiki/Main_Page.

Ringraziamenti/Acknowledgments

"After all, I've tried for three years
Seems like thirty"

I will surely remember these last three years as one of the most intense periods of my life; looking backwards, I clearly recognize how many people gave me their support, either in helping me with my work or in my everyday life as a Ph.D. student.

First of all, I want to thank my supervisor, Giuseppe Molteni. Thank you for your continuous interest and attention in my works and studies, for your patience in listening my seminars and reading my drafts, for your ever precise remarks and observations, for the knowledge and tricks you taught me and for every suggestion and clarification you gave me during these long, exciting three years. I could not ask for a better supervisor to work with.

I thank also my Ph.D. coordinator, Vieri Mastropietro, for allowing me to participate at every useful conference I had the luck to go at, and Stefania Leonardi, for all the bureaucratic help she gave me in these three years.

This thesis could not have been written without the precious help I received during my visits at Institut de Mathématiques de Bordeaux (IMB), especially from l'équipe Théorie des Nombres. I am very grateful for your interest in my computational efforts, and I would like to thank:

Karim Belabas, for supervising me during my visits in Bordeaux, for the afternoons spent in his office testing and sharpening my programs, and for writing the very helpful gp function **ZpX-primedec()**;

Bill Allombert, for the many PARI/GP tricks he taught me, both during the Ateliers and privately, which helped me speeding up my computations;

Aurel Page, for listening to every progress in my classification work and for involving me in other PARI projects;

Andreas Enge, for his crucial remark about the **solve()** function which allowed me to write simpler and faster programs for the discriminant classification problem;

Jacques Martinet, for his comments about my first paper and the insights he gave me about the problem of number fields classification;

Damien Robert, for inviting me to speak at the LFANT seminars;

Henri Cohen, for his interesting course on L-functions and Computational Number Theory;

Guillame Ricotta, for being my supervisor in my first visit at IMB.

My results could not have been accomplished without the computational resources that IMB and Università di Milano allowed me to exploit. Many thanks to Francesco Fichera, who helped me in setting my programs for the HORIZON cluster, and Alessio Alessi, for his precise instructions about the INDACO cluster.

My thesis work received benefits also from the suggestions and help of many people, and I would like to thank:

Löic Grenié, who first introduced me to the power of PARI/GP;

Schehrazad Selmane, for providing me her tables of local corrections;

Brian Conrey, for introducing me to the LMFDB database;

Jürgen Klüners and Gunter Malle, for answering my questions about their number fields database;

Francisco Diaz y Diaz, for his precise questions about my number field classification;

Eduardo Friedman, for helping me in understanding the technical difficulties of classifying number fields with small regulator;

Sandro Bettin, for introducing me to the problem of average ranks for families of elliptic curves;

Harry Smit, for his precious insights into arithmetic and Kronecker equivalence.

During these three years, I had the chance to meet and know many people working in Number Theory. I thank them for the courses they allowed me to attend, the seminars they invited me to speak at, their questions and interest about my work and especially the good times we had together at the conferences. I would thus like to thank, among the others:

Alberto Perelli, Giamila Zaghloul, Alessandro Fazzari, Mattia Righetti;

Alessandro Zaccagnini, Mattia Cafferata, Remis Tonon, Alessandro Gambini;

Francesco Pappalardi, Danilo Bazzanella, Nadir Murru, Carlo Sanna, Paolo Leonetti, Salvatore Tringali;

Giacomo Cherubini, Dimitris Xatzakos, Riccardo Maffucci, Ilaria Viglino, Asbjorn Nordentoft;

Dajano Tossici, Jared Asuncion, Emanuele Tron.

After being together in bachelor and master courses, many dear friends have been sharing with me the joys and the difficulties of being a Ph.D. student, and I would like to thank them for their friendship and help:

Andrea Anselli, Davide Di Micco, Emanuele Pavia, Davide Marangoni, Luca Giordano, for struggling with me in Milan;

Emiliano Ambrosi, Edoardo Bocchi, Filippo Riva, Luca Sabatini, Danica Basaric,

Matteo Levi, Francesca Gatti, Gregorio Baldi, Riccardo Pengo, Alberto Merici, Guido Mazzuca, Lorenzo Pagani, Simone Maletto, who are spread around Italy and the world.

I thank all my Ph.D. colleagues in Milan, the elders who welcomed me and the newcomers: with them I studied, followed useful courses and painful lessons on transferable skills, argued about delayed fundings, had noisy lunches, kebab fridays and football matches. A special thank goes to Simone Panozzo and Fan Yangyu, for sharing our passion for Number Theory in our office, and to Giulio Colombo, Beatrice Langella and Alberto Cattaneo, who teamed up with me for being representatives of the Mathematics Ph.D. students.

During these three years I had the chance to have some teaching experience at University of Milan: I thank Marco Vignati who chose me as tutor for his Calculus course. Thanks to the students who attended my lessons, hoping that I have been a valid help for them, and I want to thank also all the students with whom I discussed about Number Theory, especially Francesco Viganò and Ivan Andreoni.

Many thanks to my former university classmates and still good friends of Milan, for the good times we always have: Bizza, Ele, Pato, Vale, Ale, Chiara, Eli, Pav, Paolino, Iacopo.

Thanks to the new friends met in Via Saldini 50 who I had the luck to know better in these last few years, especially Gaia, Silvia, Giorgio, Benni, Chiara, Nena, Lori, Teo, Marta, Fede, Leo, Filippo, Anna, Michele, Nello.

Thanks also to the new friends I met in Bordeaux and who made my several visits in France so great: Sergio, Luigi, Marco, Nadia, Giovanni, Vassillis, Amelie, Cristina, Silvia, Paul, Corentin, Marius, Sally, Alessandro, Eva.

A special thank goes to Davide Castelnovo, for much more than the memes on category theory.

Thanks to Ava, Fede, Pietro, Emi, Tommi, Ale and all the members of the Clod League for distracting me every sunday with fantasy football.

Thanks to Simo, Ste, Gimmi, John, Piva and other mathematics friends for having distracted me so long with real football matches in Milan.

Thanks to the DLB friends, for all the fun we had together in the last years and for the pasta cooked with screams and songs. A special thank to Giachi, with whom I finally managed to play football after too many years.

Thanks to my classmates from section A of Galilei high school, for the strong bound we still have after all these years, despite the few occasions we had to meet each other in the last times.

Thanks to everybody I played music with in the few occasions I had the time and forces to do it, especially Lore F., Andre, Fabi, Tia, Ele, Silvi, Lore C. and Ste.

Thanks to Gianandrea for the night walks in Rome, the discussions over the several definitions of intuitionism and the confidences.

Thanks finally to all my relatives, either in Caravaggio, Treviglio and Rome, for their love and support, with a special thank for my parents Katia and Giuseppe, my sister Maria, my brother Paolo and my cousins Linda, Luca, Alberto and Lorenzo.