TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN

Fachbereich Mathematik

On the construction of number fields with solvable Galois group

Carlo Sircana

Vom Fachbereich Mathematik der Technischen Universität Kaiserslautern zur Verleihung des akademischen Grades Doktor der Naturwissenschaften (Doctor rerum naturalium, Dr. rer. nat.) genehmigte Dissertation

1. Gutachter: Prof. Dr. Claus Fieker

2. Gutachter: Prof. Dr. Jürgen Klüners

Datum der Disputation: 18. Dezember 2020

D386

Abstract

The construction of number fields with given Galois group fits into the framework of the inverse Galois problem. This problem remains still unsolved, although many partial results have been obtained over the last century. Shafarevich proved in 1954 that every solvable group is realizable as the Galois group of a number field. Unfortunately, the proof does not provide a method to explicitly find such a field. This work aims at producing a constructive version of the theorem by solving the following task: given a solvable group G and a $B \in \mathbf{N}$, construct all normal number fields with Galois group G and absolute discriminant bounded by B.

Since a field with solvable Galois group can be realized as a tower of abelian extensions, the main role in our algorithm is played by class field theory, which is the subject of the first part of this work. The second half is devoted to the study of the relation between the group structure and the field through Galois correspondence. In particular, we study the existence of obstructions to embedding problems and some criteria to predict the Galois group of an extension.

Zusammenfassung

Die Konstruktion von Zahlkörpern mit vorgegebener Galoisgruppe ist ein zentrales Problem der inversen Galoistheorie. Während das Problem in dieser Allgemeinheit weiterhin ungelöst ist, wurden im vergangenen Jahrhundert eine Reihe von Ergebnissen erzielt, welche das Problem zum Teil lösen. Im Jahr 1954 hat Shafarevich gezeigt, dass jede auflösbare Gruppe als Galoisgruppe eines Zahlkörpers realisiert werden kann. Jedoch liefert der Beweis keine Methode zum Finden eines solchen Körpers. Das Ziel dieser Arbeit ist es, eine konstruktive Version dieses Resultats zu erhalten, indem wir das folgende Problem lösen: Sei eine auflösbare Gruppe G und eine Schranke $B \in \mathbf{N}$ gegeben, bestimme alle normalen Zahlkörper mit Galoisgruppe G und absoluter Diskriminante beschränkt durch B.

Da ein Körper mit auflösbarer Galoisgruppe als Körperturm mit abelschen Teilerweiterungen realisiert werden kann, spielt in unserem Algorithmus die Klassenkörpertheorie eine wesentliche Rolle. Diese wird im ersten Teil der Arbeit behandelt. Der zweite Teil beschäftigt sich mit der Untersuchung des Zusammenhangs zwischen der Struktur der Gruppe und des Körpers, welche sich aus der Galoiskorrespondenz ergibt. Insbesondere analysieren wir die Existenz von Obstruktionen für Einbettungsprobleme und Kriterien, welche die Galoisgruppe einer Erweiterungen bestimmen.

Notation

Symbols

$\mathbf{Z}$	Ring of integral numbers
$\mathbf{Q}$	Field of rational numbers
$\mathbf{R}$	Field of real numbers
$\mathbf{C}$	Field of complex numbers
L/K	Field extension
$[L\colon K]$	Degree of the extension L/K
$\mathcal{O}_K$	Maximal order of the number field K
$N_{L/K}(x)$	Norm of the element $x \in L$ in L/K
$N_{L/K}(I)$	Norm of the ideal $I \subseteq \mathcal{O}_K$ in L/K
$\mathrm{Tr}_{L/K}(x)$	Trace of the element $x \in L$ in L/K
ζ_n	Primitive n-th root of unity
$\mathrm{Gal}(L/K)$	Galois group of the extension L/K
$\operatorname{disc} K$	Discriminant of the maximal order $\mathcal{O}_K$ of the number field K
$\operatorname{disc} \mathcal{O}$	Discriminant of the order $\mathcal{O}$
$\operatorname{disc} L/K$	Relative discriminant of the maximal order of L over K
$\mathcal{D}_{L/K}$	Different of L/K
Cl_K	Class group of the maximal order of K
$\mathcal{U}_K$	Unit group of the maximal order of K
$\mathrm{Cl}_{\mathfrak{m}}$	Ray class group modulo $\mathfrak{m}$
$\mathrm{Frob}_{\mathfrak{p},L/K}$	Frobenius automorphism of the ideal $\mathfrak{p}$ in the abelian extension L/K
$\Phi_{L/K}$	Artin map for the abelian extension L/K
$(x_1, \ldots, x_n)$	Ideal generated by the elements $x_1, \ldots, x_n$
$\langle x_1, \ldots, x_n \rangle$	Subgroup generated by the elements $x_1, \ldots, x_n$
G'	Derived subgroup of the group G
$Z(G)$	Center of the group G
C_n	Cyclic group of order n
D_n	Dihedral group of order $2n$
S_n	Symmetric group on n elements
A_n	Alternating group on n elements

Introduction

The construction of number fields with given Galois group fits into the framework of the inverse Galois problem, which consists in deciding whether every finite group G is realizable as the Galois group of a number field over the rationals. This problem remains still unsolved, although many partial results have been obtained over the last century, depending on the nature of G. For instance, abelian groups can be realized as subfields of cyclotomic fields; a deeper result is provided by the following theorem:

Theorem (Scholz–Reichardt, [61]). *Let G be a nilpotent group of odd order. Then there exists a number field K such that* $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$.

The theorem exploits the relation existing between subgroups of G and the structure of a field with Galois group G; in particular, a number field with nilpotent Galois group G can be constructed as a tower of cyclic extensions that are normal over $\mathbf{Q}$. In the case of a solvable group G, it is possible to construct a number field with Galois group G as a tower of abelian extensions that are normal over $\mathbf{Q}$, leading Shafarevich to prove the following theorem in 1954:

Theorem (Shafarevich, [66]). *Let G be a solvable group. Then there exists a number field K such that* $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$.

Unfortunately, its proof is not constructive and it does not provide a method to explicitly find a number field with Galois group isomorphic to G. This work aims at studying a constructive version of Shafarevich's theorem by addressing the following task:

> Given a solvable group G and a positive integer B, construct all normal number fields with Galois group G and absolute discriminant bounded by B.

For every number field, we provide a certificate for its correctness by producing a primitive element, identified by its minimal polynomial, the discriminant and generators for the Galois group.

Since a field with solvable Galois group can be constructed as a tower of abelian extensions, the main role in the algorithm that we will outline in the next section is played by class field theory, which provides a parametrization of abelian extensions of a given number field. For this reason, we focus in Chapter 1 on the algorithms to construct abelian extensions and compute their invariants, describing new algorithms to compute ray class groups and defining polynomials for an abelian extension. More specialized methods will be presented in Chapter 2, together with a characterization of abelian extensions that are normal over the rationals and a fast algorithm to compute generators of the Galois group.

While the improvements presented in Chapter 1 and 2 concern the construction of abelian extensions, the following chapters are dedicated to the analysis of the relation between the target group and the subfields we encounter during the execution of the algorithm. In particular, Chapter 3 is devoted to the algorithmic study of the solvability of a so-called embedding problem, in the spirit of the proofs of Shafarevich and Scholz-Reichardt. By using the properties of cohomology groups, we develop a method to decide whether a number field admits an extension with a given Galois group. In addition, the group structure gives also some constraints on the ramification of prime ideals, helping us to predict the correctness of the Galois group of an extension: this is the main subject of Chapter 4, together with an ad-hoc method to deal with decomposable groups. Finally, we show the effectiveness of the algorithm in Chapter 5 by presenting the fields with minimal discriminant and Galois group of order 16, 32 and 64. These results were out of reach for the previous methods: in the literature there are many examples of groups realizations (for example [20, 19, 27, 37, 38, 40, 41, 65]), mainly based on class field theory and on Hunter's method (see [15, 51, 56]). In contrast to our approach, the latter method is quite effective in the case of non-normal fields, as it does not require the computation of the normal closure. However, the results we present here would not be feasible for Hunter's method, since it becomes inefficient as the degree grows.

The range of applications of our algorithm is not limited to the computation of fields with minimal discriminants. For instance, the construction of fields with given Galois group is useful to find empirical confirmation of various heuristics involving the Galois group, such as

- the Cohen-Lenstra and Malle heuristic on the distribution of class groups [21, 22, 48],
- the Malle heuristic on the number of fields with a given Galois group and bounded discriminant [47].

Some of the numerical results supporting these predictions are outdated and the progress in the field of computational number theory allow to collect more examples to be tested. In particular, the existing databases (such as [46, 41, 39]) contain mainly fields of rather small degree or with small discriminant. Collecting data for larger input invariants is a challenging problem, motivating us to improve on the existing methods.

Outline of the algorithm

The task we want to solve requires a continuous dialogue between two different areas of mathematics: algebraic number theory and group theory. The main idea is to take advantage of the Galois correspondence in order to construct the fields as a tower of subfields.

Theorem (Galois correspondence). *Let K be a Galois field with Galois group G. Then there is a inclusion-reversing correspondence between subgroups of G and subfields of K.*

$$\begin{array}{rcl} \{\text{ Subfields of } K\} & \longleftrightarrow & \{\text{ Subgroups of } G\} \\ F & \longmapsto & \{g \in G \mid g(x) = x \quad \forall x \in F\} \\ \{x \in K \mid h(x) = x \ \forall h \in H\} & \longleftarrow\!\shortmid & H \end{array}$$

In particular, normal subfields of K correspond to normal subgroups of G.

Proof. See [50, Appendix 2, Theorem 6].

Consider a chain of subgroups of G, ending with the trivial subgroup:

$$G = G_0 \supsetneqq G_1 \supsetneqq G_2 \supsetneqq \ldots \supsetneqq G_{n-1} \supsetneqq G_n = \{e\}$$

Given a number field K with Galois group $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$, it determines a chain of subfields of K:

$$\mathbf{Q} = K_0 \subsetneqq K_1 \subsetneqq K_2 \subsetneqq \ldots \subsetneqq K_{n-1} \subsetneqq K$$

Thus, we can construct a field with Galois group G by choosing a tower of subfields corresponding to a series of subgroups of G. Here is where the hypothesis of G being solvable comes into play:

Definition. *A finite group G is solvable if it admits a chain of subgroups*

$$G = G_0 \supsetneqq G_1 \supsetneqq G_2 \supsetneqq \ldots \supsetneqq G_{n-1} \supsetneqq G_n = \{e\}$$

such that G_i is normal in G for all $i \in \{0, \ldots, n\}$ and the quotient G_i/G_{i+1} is abelian for all $i \in \{0, \ldots, n-1\}$.

Example 1. The alternating group A_4 of order 12 is solvable, as it admits a normal subgroup H isomorphic to $C_2 \times C_2$. H is the only proper normal subgroup of A_4: therefore $\langle e \rangle \subsetneqq H \subsetneqq A_4$ is the only normal series of A_4 satisfying the conditions of the definition.

Since we want to construct a field with solvable Galois group G, we can exploit the existence of a series as in the definition in order to obtain the following result.

Proposition. *Let K be a number field with solvable Galois group. Then K admits a chain of normal subfields $\mathbf{Q} = K_0 \subsetneq K_1 \subsetneq \ldots \subsetneq K_{n-1} \subsetneq K_n = K$ with the property that K_{i+1}/K_i is abelian for every $i \in \{0, \ldots, n-1\}$ and K_i is normal over $\mathbf{Q}$ for all $i \in \{0, \ldots, n\}$.*

Inspired by this proposition, we adopt a recursive approach: given a number field K_i with Galois group G/G_i, we construct abelian extensions with Galois group over K_i isomorphic to G_i/G_{i+1} and then test whether they have Galois group isomorphic to G/G_{i+1} over $\mathbf{Q}$. As we want the extensions to have absolute discriminant bounded by an integer B, we have a bound on the discriminant of the intermediate extensions we compute.

Lemma. *Let L/K be an extension of number fields. Then*

$$|\operatorname{disc} L| = |\operatorname{disc} K|^{[L:\,K]} N_{K/\mathbf{Q}}(\operatorname{disc} L/K).$$

Proof. See [60, Chapter III, Proposition 8].

Corollary. *Let L/K be a number field extension. If $|\operatorname{disc} L| \leq B$, then $|\operatorname{disc} K| \leq \sqrt[[L:K]]{B}$ and the bound is sharp.*

Proof. The bound comes from the lemma by using that $N_{K/\mathbf{Q}}(\operatorname{disc} L/K) \geq 1$. The bound is sharp as $N_{K/\mathbf{Q}}(\operatorname{disc} L/K) = 1$ when L/K is unramified.

We summarize the general strategy in the following pseudocode.

Algorithm 1 Construction of number fields with given solvable Galois group

```
Input: A solvable group $G$ together with a normal series $\{G_i\}_{i \in \{0,\ldots,n\}}$ with
    abelian quotients and a positive integer $B$.
Output: The set of all the number fields having Galois group isomorphic to
    $G$ and absolute discriminant lower than $B$.

1. Construct $H = G/G_{n-1}$.
2. Set $B_1 = \sqrt[\frac{|G|}{|H|}]{B}$.
3. Compute recursively the set $L_{n-1}$ of number fields with Galois group $H$
   and discriminant bounded by $B_1$.
4. Initialize an empty set of number field $L_n$.
5. For every field $K$ in $L_{n-1}$,
     • Compute the set $L_K$ of abelian extensions of $K$ with Galois group
       over $K$ isomorphic to $G_{n-1}/G_n$.
     • Append to $L_n$ the subset of $L_K$ given by the number field with Galois
       group isomorphic to $G$.
6. Return $L_n$.
```

Issues

The description of Algorithm 1 is quite simple; however, it suffers from some mathematical and algorithmic problems that we will address in the following chapters.

Obstructions Let K be a number field with Galois group G and assume that we are searching for an extension with Galois group E. Even if Shafarevich theorem ensure the existence of a number field with Galois group E, it might happen that none of these fields is an extension of K.

Example 2 ([61, Theorem 1.2.4]). We study the existence of an embedding of a quadratic field K into a C_4 extension of $\mathbf{Q}$. Suppose that such an extension exists and denote it by L. Chosen a primitive element $\sqrt{\alpha}$ for K, where $\alpha \in \mathbf{Z}$, we can write $L = K(\beta)$ with $\beta = \sqrt{a + b\sqrt{\alpha}}$ for $a, b \in \mathbf{Z}$. As $\mathrm{Gal}(L/\mathbf{Q}) \simeq C_4$, there exists a generator σ of $\mathrm{Gal}(L/\mathbf{Q})$ sending β to $\gamma = \sqrt{a - b\sqrt{\alpha}}$. Denote by x the element $\beta\gamma/\sqrt{\alpha}$. We notice that σ fixes x, as

$$\sigma(x) = \frac{\sigma(\beta)\sigma(\gamma)}{\sigma(\sqrt{\alpha})} = \frac{\gamma \cdot (-\beta)}{-\sqrt{\alpha}} = x.$$

Since σ generates $\mathrm{Gal}(L/\mathbf{Q})$, this means that $x \in \mathbf{Q}$. By the definition of x,

$$\sqrt{\alpha} \cdot x = \sqrt{a^2 - b^2\alpha}.$$

Squaring both sides and isolating α we get

$$\alpha = \frac{a^2}{x^2 + b^2} = \Big(\frac{ax}{x^2 + b^2}\Big)^2 + \Big(\frac{ab}{x^2 + b^2}\Big)^2.$$

Therefore if $K = \mathbf{Q}(\sqrt{\alpha})$ admits a C_4-extension, then α must be the sum of two rational squares. In particular, $\mathbf{Q}(\sqrt{3})$ can not be embedded into a C_4-extension.

This phenomenon has been studied extensively from a theoretical point of view. We will develop an algorithm to check whether there is an obstruction to the existence of an extension in Chapter 3.

Sieving the abelian extension The first issue we have presented concerned the number of fields we have to analyze in Step (5) of Algorithm 1. This second problem is related to the number of fields we construct inside the loop. Indeed, in the same notations of Algorithm 1, we first construct abelian extensions of K with Galois group over K isomorphic to G_{n-1}/G_n and then sieve them in order to find which of them has Galois group isomorphic to G. It is crucial to compute as few abelian extensions as possible by imposing the constraints given by the discriminant bound and the group structure, in particular the normality: the abelian extensions of K we are searching for must be normal over $\mathbf{Q}$. We will address this problem mainly in Chapter 2, together with some algorithms to compute abelian extensions, while we will deal with the constraints coming from the group structure in Chapter 4.

Coefficient growth The methods to compute an abelian extension of a given number field suffers from a coefficients growth. More specifically, the minimal polynomials over the primitive elements that we find tend to be quite large and the successive computations become then infeasible.

Example 3. The polynomials $f = x^4 + 220x^3 + 20038x^2 + 884652x + 15744357$ and $g = x^4 - 2x^3 + 115x^2 - 114x + 3966$ define the same biquadratic field. g is preferable over f, as its coefficients are smaller.

We deal with this technical aspect in two different ways:

- we will search for small primitive elements for the abelian extensions during the construction;
- we will reduce the size of the primitive element of the whole field after the computation.

The two methods are quite different from each other: the first one is based on the so-called "compact representation" of an algebraic integer and we will illustrate this method in Section 1.5. The second idea is instead well-known and it is based on the LLL algorithm: we will present the details in Section 2.4.

Contents

CHAPTER 1

Abelian extensions

In this chapter, we focus on class field theory, which provides a way to parametrize abelian extensions of a number field. In particular, this correspondence can be made constructive: we are going to analyze the algorithms that are necessary to construct a given abelian extension and present new strategies to overcome some of the issues and bottlenecks, improving the performance.

1.1 Class field theory: a short summary

In order to set the notations, we briefly recall the main theorems of class field theory and the main results about ramification groups that we are going to use in the algorithms. We refer the reader to [36, 60, 42] for a detailed description of the topic and proofs.

Ramification groups

Ramification groups are one of the main tools to study ramification in normal extensions, as they encode the local behaviour of primes.

Definition 1.1. *Let L/K be a normal extension of number fields with Galois group G and let $\mathfrak{p}$ be a prime ideal of L. We define the decomposition group $G_\mathfrak{p}$ of $\mathfrak{p}$ as the stabilizer of $\mathfrak{p}$ in G under the Galois action on the ideals, i.e.*

$$G_\mathfrak{p} = \{\sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Remark 1.2. The decomposition group $G_\mathfrak{p}$ can be identified with the Galois group of the completion at $\mathfrak{p}$.

Let $\sigma \in G_\mathfrak{p}$ be an element of the decomposition group of a prime ideal $\mathfrak{p}$. Then σ preserves the valuation at $\mathfrak{p}$, i.e. $v_\mathfrak{p}(\sigma(x)) = v_\mathfrak{p}(x)$ for all $x \in \mathcal{O}_K$.

Definition 1.3. *The i-th ramification group $G_{\mathfrak{p},i}$ for $i \geq -1$ is the subgroup of $G_{\mathfrak{p}}$ given by the elements with the property that, for all $x \in K$,*

$$v_{\mathfrak{p}}\left(\sigma(x) - x\right) \geq i + 1$$

Remark 1.4. Notice that $G_{\mathfrak{p}}$ coincides with $G_{\mathfrak{p},-1}$ by definition. In the literature, $G_{\mathfrak{p},0}$ is usually called inertia group and its cardinality coincides with the ramification index of $\mathfrak{p}$ in L/K.

If the prime ideal $\mathfrak{p}$ is clear from the context, we will just write G_i instead of $G_{\mathfrak{p},i}$.

Notice that $G_{i+1} \subseteq G_i$ for all indices $i \geq -1$ and that G_i is the trivial subgroup eventually. In particular, the ramification groups provide a filtration of the decomposition group and in general some of the ramification properties of $\mathfrak{p}$ are encoded in the indices i such that $G_{i+1} \neq G_i$; these indices are called "jumps". The quotients G_i/G_{i+1} must satisfy some rigid properties:

Proposition 1.5 ([60, Chapter IV, Corollary 1, 3]). *Let L/K be a normal extension of number fields and let $\mathfrak{p}$ be a prime ideal of L. Let $G_{-1} = G_{\mathfrak{p}} \supseteq G_{\mathfrak{p},0} \supseteq G_{\mathfrak{p},1} \supseteq \cdots \supseteq G_{\mathfrak{p},n} = \{e\}$ be the ramification groups of $\mathfrak{p}$. Let p be the prime number lying underneath $\mathfrak{p}$. Then:*

- *G_0/G_1 is cyclic of order coprime to p,*
- *G_i/G_{i+1} has exponent p for $i > 0$.*

Notice that, by virtue of this proposition, in the case of a cyclic extension the knowledge of the jumps are enough to determine all the ramification groups.

Ramification groups behave well with respect to subextensions L/K' ([60, Chapter IV, Proposition 2]). In the case of intermediate subextensions, we have the following result:

Lemma 1.6. *Let L/K be a normal extension of number fields and let K'/K be a normal subextension. Let $\mathfrak{p}$ be a prime ideal of L and let $\mathfrak{p}'$ be the prime ideal of K' lying underneath $\mathfrak{q}$. Consider the restriction* $\mathrm{res}\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(K'/K)$. *Then $\pi(\mathrm{Gal}(L/K)_{\mathfrak{p},i}) = \mathrm{Gal}(K'/K)_{\mathfrak{p}',i}$ for $i = -1, 0$.*

Proof. The statements about the decomposition groups follow by noticing that the decomposition group correspond to the Galois group of the completion and by the containment $L_{\mathfrak{p}} \supseteq K'_{\mathfrak{p}'}$. Thus, we now focus on the inertia group. First of all, we notice that the restriction map is well defined. Let $\varphi \in \mathrm{Gal}(L/K)_0$ and let b be a generator of the valuation ring of the completion of K' at $\mathfrak{p}'$. Then $v_{\mathfrak{p}}(\frac{\varphi(b)}{b} - 1) \geq 2$, and, passing to the valuation at $\mathfrak{p}'$, this means that $v_{\mathfrak{p}'}(\frac{\varphi(b)}{b} - 1) \geq 2$, as we wanted to show. Now, we prove the surjectivity of the maps. The restriction $\pi|_{\mathrm{Gal}(L/K)_0}\colon \mathrm{Gal}(L/K)_0 \to \mathrm{Gal}(K'/K)_0$ has as kernel the inertia subgroup $\mathrm{Gal}(L/K')_0$ of the intermediate extension L/K'. The surjectivity follows by an easy cardinality check and the fact that the order of the inertia group coincides with the ramification index.

Example 1.7. Let $L = \mathbf{Q}(\zeta_5)$ be the cyclotomic field of order 5 and let K be its subfield of order 2. The ramification groups for the prime ideal $(7) \subseteq \mathcal{O}_L$ are $G_{-1} = \mathrm{Gal}(L/\mathbf{Q})$ and $G_i = \{e\}$ for $i \geq 0$. Thus, according to the lemma, the ramification group $\mathrm{Gal}(K/\mathbf{Q})_{(7),-1}$ is isomorphic to the whole Galois group $\mathrm{Gal}(K/\mathbf{Q})$.

However, if K'/K is an intermediate normal subextension of L/K, the filtrations might not compatible for the other ramification groups: this is the reason why we define the upper numbering ramification groups, which is just a renumbering of the lower numbering ramification groups.

Definition 1.8. *Consider the function defined on* $\mathbf{R}_{\geq -1}$

$$\varphi(u) = \int_0^u \frac{1}{[G_\mathfrak{p} : G_t]} dt$$

where the definition of G_i *is extended to* $\mathbf{R}$ *as* $G_i = G_{\lceil i \rceil}$ *for* $i \in \mathbf{R}$*. Given a real number* $u \in \mathbf{R}$*, we define the upper numbering ramification group* G^u *as* $G_{\varphi(u)}$*.*

The function φ is monotonically increasing (because $[G_\mathfrak{p} : G_i] \geq 0$) and provide a renumbering of the lower numbering ramification groups. In particular, the groups $\{G^v\}_{v \in \mathbf{R}_{\geq -1}}$ provide again a filtration of $G_\mathfrak{p}$. It is interesting to study the jumps in this filtration: in this case, since we are working with real numbers, a jump is an index v such that $G^v \supsetneq G^{v+\varepsilon}$ for every $\epsilon > 0$.

In the case of abelian extensions, there is a strong connection between the jumps of the two filtrations, given by the celebrated Hasse-Arf theorem:

Theorem 1.9 (Hasse-Arf). *Let* L/K *be an abelian extension. If* $G_i \neq G_{i+1}$*, then* $\varphi(i)$ *is an integer.*

Proof. See [60, Theorem 1, Chapter V].

Ray class fields

We now present the main results on class field theory, which studies the abelian extensions of a given number field and classifies them. We consider a number field K with ring of integers $\mathcal{O}_K$.

Definition 1.10. *A modulus* $\mathfrak{m}$ *of* K *is a pair* $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ *consisting of a nonzero ideal* $\mathfrak{m}_0$ *of* $\mathcal{O}_K$ *and a set* $\mathfrak{m}_\infty$ *of real embeddings of* K*. In this case we also write* $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$*.*

The definition of modulus extends the definition of ideals in the ring of integers by taking into account the infinite places. In particular, we can extend some of the operations to them, as well as the notion of divisibility:

Definition 1.11. *Given two moduli $\mathfrak{m}$, $\mathfrak{n}$, we say that $\mathfrak{n}$ divides $\mathfrak{n}$ if $\mathfrak{n}_0 \mid \mathfrak{m}_0$ and $\mathfrak{n}_\infty$ is contained in $\mathfrak{m}_\infty$. Accordingly, we define the greatest common divisor of $\mathfrak{m}$ and $\mathfrak{n}$ as the modulus $\mathfrak{f}$ with the property that, for every modulus $\mathfrak{f}'$ such that $\mathfrak{f}' \mid \mathfrak{m}$ and $\mathfrak{f}' \mid \mathfrak{n}$, it holds $\mathfrak{f}' \mid \mathfrak{f}$. Similarly, the least common multiple of $\mathfrak{m}$ and $\mathfrak{n}$ is the modulus $\mathfrak{f}$ with the property that, for every modulus $\mathfrak{f}'$ such that $\mathfrak{m} \mid \mathfrak{f}'$ and $\mathfrak{n} \mid \mathfrak{f}'$, it holds $\mathfrak{f} \mid \mathfrak{f}'$.*

Given a modulus $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$, we denote by $I_\mathfrak{m}$ the group of fractional ideals of K generated by the prime ideals coprime to $\mathfrak{m}_0$. Infinite primes do not play a role in the definition of $I^\mathfrak{m}$, but they are important in the definition of the so called "ray subgroups". For $x \in K$, we define $x \equiv 1 \pmod{\mathfrak{m}}$ if and only if $v_\mathfrak{p}(x-1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$ for all prime ideals $\mathfrak{p}$ dividing $\mathfrak{m}_0$ and $\sigma(x) > 0$ for $\sigma \in \mathfrak{m}_\infty$.

Definition 1.12. *Let $\mathfrak{m}$ be a modulus of K. We define the ray group $P_\mathfrak{m} = \{xK \mid x \equiv 1 \bmod \mathfrak{m}\} \subseteq I_\mathfrak{m}$ and call the finite abelian group $\mathrm{Cl}_\mathfrak{m} = I_\mathfrak{m}/P_\mathfrak{m}$ the ray class group of K modulo $\mathfrak{m}$.*

A subgroup $P_\mathfrak{m} \subseteq U \subseteq I_\mathfrak{m}$ is called a *congruence subgroup* modulo $\mathfrak{m}$. By abuse of notation, we will also call $\overline{U} = U/P_\mathfrak{m}$ a congruence subgroup.

Notice that if $\mathfrak{n} \mid \mathfrak{m}$ then $I^\mathfrak{n}$ contains $I^\mathfrak{m}$. Thus we have an injection $I^\mathfrak{m} \to I^\mathfrak{n}$ which induces a surjection at the level of the ray class groups $\mathrm{Cl}_\mathfrak{m} \to \mathrm{Cl}_\mathfrak{n}$. In particular, every congruence subgroup modulo $\mathfrak{n}$ can be lifted to a congruence subgroup modulo $\mathfrak{m}$. This is why we introduce an equivalence relation on the set of congruence subgroups.

Definition 1.13. *Let U, V be congruence subgroups defined respectively modulo $\mathfrak{m}$ and $\mathfrak{n}$. Let $\mathfrak{f}$ be the least common multiple of $\mathfrak{m}$ and $\mathfrak{n}$. We say that U is equivalent to V if $U \cap I^\mathfrak{f} = V \cap I^\mathfrak{f}$. We call an equivalence class under this relation an ideal class.*

In particular, an ideal class has different representatives: if $\mathfrak{m}$ is a modulus for which there exists a representative for the ideal class $[U]$, we say that $\mathfrak{m}$ is an admissible modulus for $[U]$.

Definition 1.14. *Let $[U]$ be an ideal class. We define the conductor $\mathfrak{f}$ of $[U]$ as the greatest common divisor of all the admissible moduli for $[U]$, i.e. for each admissible modulus $\mathfrak{m}$ for $[U]$ holds $\mathfrak{f} \mid \mathfrak{m}$.*

The correspondence theorem gives a relation between the ideal classes and the abelian extensions of K, therefore giving a parametrization of the abelian extensions of K in terms of objects contained in K:

Theorem 1.15 (Correspondence Theorem). *Let K be a number field. There is a one to one, inclusion reversing, correspondence between ideal classes of K and abelian extensions of K. In particular, given an abelian extension L/K, the corresponding ideal group is generated by the norm of prime ideals of L that are unramified over K.*

As a consequence, we can define the conductor to abelian extensions as the conductor of the corresponding ideal class; it encodes information on the ramification:

Lemma 1.16. *Let L/K be an abelian extension with conductor $\mathfrak{f}$. Let $\mathfrak{p}$ be a prime ideal of K. Then:*

- *$\mathfrak{p}$ is unramified in L/K if and only if $v_{\mathfrak{p}}(\mathfrak{f}) = 0$;*
- *$\mathfrak{p}$ is at most tamely ramified in L/K if and only if $v_{\mathfrak{p}}(\mathfrak{f}) \leq 1$.*

In particular, the conductor has a strong relation with the discriminant, given by the so-called discriminant-conductor formula:

Theorem 1.17. *Let $A_{\mathfrak{m}}$ be a congruence subgroup modulo $\mathfrak{m}$. Let $\mathfrak{p}$ be a prime ideal of K and let δ be the discriminant of the abelian extension corresponding to $A_{\mathfrak{m}}$. Given a modulus $\mathfrak{f}$ dividing $\mathfrak{m}$, consider the projection $\pi_{\mathfrak{f}} \colon \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{f}}$ and denote by $h_{\mathfrak{f},A_{\mathfrak{m}}}$ the index $[\mathrm{Cl}_{\mathfrak{f}} \colon \pi_{\mathfrak{f}}(A_{\mathfrak{m}})]$. Then*

$$v_{\mathfrak{p}}(\delta) = v_{\mathfrak{p}}(\mathfrak{m}_0) h_{\mathfrak{m},A_{\mathfrak{m}}} - \sum_{i=1}^{v_{\mathfrak{p}}(\mathfrak{m}_0)} h_{\mathfrak{m}/\mathfrak{p}^i,A_{\mathfrak{m}}}$$

Proof. See [15, Theorem 3.5.11].

Example 1.18. The easiest examples of abelian extensions is given by the cyclotomic fields. In particular, the cyclotomic field $\mathbf{Q}(\zeta_n)$ corresponds to the trivial congruence subgroup modulo $\mathfrak{m} = (n\mathbf{Z}, \infty)$, where ∞ is the unique embedding of $\mathbf{Q}$ into $\mathbf{C}$. The conductor of $\mathbf{Q}(\zeta_{p^n})$ is (p^n, ∞) if p is an odd prime or $p = 2$ and $n \geq 2$.

This strong relation between the conductor and the ramification of L/K has influence also on the ramification groups.

Theorem 1.19. *Let L/K ba an abelian extension of number fields with conductor $\mathfrak{f}$. Let $\mathfrak{p}$ be a prime ideal of L and let $\mathfrak{p}_0$ be the prime ideal of K underneath $\mathfrak{p}$. If c is the largest integer such that the upper numbering ramification group $G_{\mathfrak{p}}^c$ of $\mathfrak{p}$ is non-zero, then $v_{\mathfrak{p}_0}(\mathfrak{f}) = c + 1$.*

Proof. See [59, Section 4.2, Proposition 1]

The Artin map

The proof of the correspondence theorem is based on the existence of a canonical isomorphism between the quotient of the ray class group modulo a congruence subgroup and the automorphism group of the corresponding abelian extension. This isomorphism is obtained via the Frobenius automorphisms:

Definition 1.20. *Let L/K be a normal extension and let $\mathfrak{p}$ be a prime ideal of L, unramified over K. Let q be the order of the residue field of $\mathfrak{p} \cap K$. The Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p},L/K}$ is the unique automorphism in the decomposition group of $\mathfrak{p}$ in L/K with the property that*

$$\mathrm{Frob}_{\mathfrak{p},L/K}(x) \equiv x^q \pmod{\mathfrak{q}}.$$

The Frobenius automorphism behaves well with respect to the conjugation; more precisely, for every prime ideal $\mathfrak{p}$ of L and $\sigma \in \mathrm{Gal}(L/K)$ it holds that $\mathrm{Frob}_{\sigma(\mathfrak{p}),L/K} = \sigma \circ \mathrm{Frob}_{\mathfrak{p},L/K} \circ \sigma^{-1}$. In particular, if $\mathrm{Gal}(L/K)$ is abelian, all conjugate primes share the same Frobenius automorphism; this allows us to define the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p},L/K}$ of a prime ideal $\mathfrak{p}$ of K as $\mathrm{Frob}_{\mathfrak{q},L/K}$, where $\mathfrak{q}$ is any prime ideal of L lying over $\mathfrak{p}$. As a consequence, we can define a map $\Phi_{L/K}$ on the prime ideals of K coprime to $\operatorname{disc} L/K$ sending $\mathfrak{p}$ to $\mathrm{Frob}_{\mathfrak{p},L/K}$. Let $\mathfrak{m}$ be the modulus having $\operatorname{disc} L/K$ as finite part and divisible by all the infinite places; then we can extend this map to $I^{\mathfrak{m}}$ by multiplicativity (the prime ideals coprime to $\operatorname{disc} L/K$ generate $I^{\mathfrak{m}}$):

Definition 1.21. *The following map*

$$\begin{aligned} \Phi_{L/K}\colon\ I^{\mathfrak{m}} &\longrightarrow \mathrm{Gal}(L/K) \\ \mathfrak{p} &\longmapsto \mathrm{Frob}_{\mathfrak{p},L/K} \end{aligned}$$

defined on the prime ideals of K coprime to $\mathfrak{m}$ and extended by multiplicativity to the whole $I^{\mathfrak{m}}$ is called the Artin map of the abelian extension L/K.

The Artin map is surjective [36, Chapter IV, Corollary 5.3] and the kernel contains the ray group $P_{\mathfrak{m}}$ [36, Chapter V, Theorem 5.7]. In particular, if U is the congruence subgroup corresponding to the kernel of $\Phi_{L/K}$, we have an induced isomorphism (which by abuse of notation we denote again by $\Phi_{L/K}$)

$$\begin{aligned} \Phi_{L/K}\colon\ \mathrm{Cl}_{\mathfrak{m}}/U &\longrightarrow \mathrm{Gal}(L/K) \\ \mathfrak{p} &\longmapsto \mathrm{Frob}_{\mathfrak{p},L/K}\,. \end{aligned}$$

Example 1.22. The Artin map is rather simple in the case of cyclotomic extensions. Given an odd prime number p, the modulus $\mathfrak{m} = (p^n, \infty)$ is the conductor of $\mathbf{Q}(\zeta_{p^n})$, which corresponds to the trivial congruence subgroup modulo $\mathfrak{m}$. We can identify naturally $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q})$ with $(\mathbf{Z}/p^n\mathbf{Z})^\times$; with this identification, the Artin map is just the map that sends a prime number q to the class $[q]$ in $(\mathbf{Z}/p^n\mathbf{Z})^\times$.

Translation The Artin map has nice properties with respect to the translation of extensions. Let L be an abelian extension of K and let E be any extension of K; then EL is an abelian extension of E. We can identify $\mathrm{Gal}(EL/E)$ with a subgroup of $\mathrm{Gal}(L/K)$ by the restriction map $\mathrm{res}_{EL/L}$. The map that makes the diagram commute is then the norm:

Lemma 1.23. *Let $\tilde{\mathfrak{m}}$ be the extension to E of the modulus $\mathfrak{m}$. The following diagram commutes:*

$$\begin{tikzcd}
\mathrm{Cl}_{\tilde{\mathfrak{m}}}^{E} \arrow[r, "\Phi_{EL/E}"] \arrow[d, "N_{E/K}"'] & \mathrm{Gal}(EL/E) \arrow[d, "\mathrm{res}_{EL/L}"] \\
\mathrm{Cl}_{\mathfrak{m}}^{K} \arrow[r, "\Phi_{L/K}"'] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

Proof. See [36, Chapter III, Proposition 3.1].

1.2 Computation of ray class groups

The correspondence theorem shows that every abelian extension corresponds to a subgroup of a suitable ray class group. In order to enumerate abelian extensions of a number field using class field theory, the first step is to construct ray class groups with respect to a set of moduli (depending on the requirements on the extensions). In this section we will illustrate the algorithm to compute them, discussing the main issues.

Let K be a number field and let $\mathfrak{m}$ be a modulus of K, with finite part $\mathfrak{m}_0$ and infinite part $\mathfrak{m}_\infty$. We aim at finding an abstract group A isomorphic to $\mathrm{Cl}_\mathfrak{m}$ together with an isomorphism between A and $\mathrm{Cl}_\mathfrak{m}$, meaning that we want to be able to produce an ideal representing each element of A and determine an element of A corresponding to the class to which an ideal belongs. The algorithm (see [17]) to compute ray class groups $\mathrm{Cl}_\mathfrak{m}$ relies on the exact sequence appearing in the following proposition:

Proposition 1.24. *Let K be a number field and let $\mathfrak{m}$ be a modulus of K. Denote by $\mathcal{U}_K$ the unit group of the maximal order $\mathcal{O}_K$ of K and by* Cl *the class group of K. Then the ray class group modulo $\mathfrak{m}$ fits in the following exact sequence*

$$\mathcal{U}_K \xrightarrow{\iota} (\mathcal{O}_K/\mathfrak{m})^\times \longrightarrow \mathrm{Cl}_\mathfrak{m} \longrightarrow \mathrm{Cl} \longrightarrow 1. \tag{1.1}$$

Proof. See [18, Proposition 3.2.3].

The exact sequence in the proposition can be replaced by the following short exact sequence

$$1 \to (\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{U}_K) \longrightarrow \mathrm{Cl}_\mathfrak{m} \longrightarrow \mathrm{Cl} \longrightarrow 1. \tag{1.2}$$

Example 1.25. In the case $K = \mathbf{Q}$, the class group is trivial and we have an isomorphism $\mathrm{Cl}_\mathfrak{m} \simeq (\mathcal{O}_K/\mathfrak{m})^\times/\langle -1\rangle$. In particular, given a modulus $\mathfrak{m} = (m\mathbf{Z}, \mathfrak{m}_\infty)$ with $\mathfrak{m}_\infty$ not empty, there is an isomorphism $\mathrm{Cl}_\mathfrak{m} \simeq (\mathbf{Z}/m\mathbf{Z})^\times$. If $\mathfrak{m}_\infty$ is empty, we get instead $\mathrm{Cl}_\mathfrak{m} \simeq (\mathbf{Z}/m\mathbf{Z})^\times/\langle -1\rangle$.

Computation of $(\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{U}_K)$

The first step is the construction of the factor group $(\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{U}_K)$: we first determine the group $(\mathcal{O}_K/\mathfrak{m})^\times$ and then factor out the image of $\mathcal{U}_K$. For what concerns the computation of $(\mathcal{O}_K/\mathfrak{m})^\times$, we refer to [15, Chapter 4, Section 2]. Thus, we only need to deal with the computation of the image of $\mathcal{U}_K$ into $(\mathcal{O}_K/\mathfrak{m})^\times$. We assume that the generators of $\mathcal{U}_K$ are given in factored form, i.e. for every element $u \in \mathcal{U}_K$ we have elements $a_1, \dots, a_s \in K$ and exponents $e_1, \dots, e_s \in \mathbf{Z}$ such that $u = \prod_{i=1}^s a_i^{e_i}$.

Image at infinite places The computation of the image of u in the components of $(\mathcal{O}_K/\mathfrak{m})^\times$ corresponding to the infinite places is straightforward. Indeed, we need to compute the sign of u at every real place in $\mathfrak{m}_\infty$. Let $\sigma_v \colon K \to \mathbf{R}$ be a real embedding. Then we compute the sign of $\sigma_\mathfrak{v}(a_i)$ for all the factors of u such that e_i is odd (a square is always positive): u will be positive at $\mathfrak{v}$ if the number of negative elements among these a_i is even, negative otherwise.

Image at finite places We now deal with the computation of the discrete logarithm of an element $u = \prod a_i^{e_i}$ in $(\mathcal{O}_K/\mathfrak{m})^\times$ at the components corresponding to the finite places. This requires in particular an efficient algorithm to determine the images of factored elements of K under the projection to the residue ring. We will work in the more general case of an element u whose support is disjoint from the support of $\mathfrak{m}_0$, as this operation is needed also for the discrete logarithm function and in that case we are not dealing with units. Of course, the naive algorithm would evaluate the product in K and then project it down to the residue ring. However, the evaluation in K is usually costly and this approach might lead to slow performance depending on the field.

We proceed as follows. Consider the factorization of $\mathfrak{m}_0$ into prime ideals, $\mathfrak{m}_0 = \prod \mathfrak{p}_i^{d_i}$ and let $\pi_i \colon \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}_i^{d_i}$ be the natural projection to the quotient. By means of the Chinese remainder theorem, we can reduce to the problem of computing the projection under π_i for all indices i. The algorithm is then made of three main steps:

1. write u as a product of elements in $\mathcal{O}_K$,
2. write u as a product of elements in $\mathcal{O}_K$ having valuation zero at $\mathfrak{p}$,
3. evaluate u in the residue ring.

We will now discuss every step.

1. We want to write $u = \prod b_i^{e_i}$ as a product of integral elements. We present here two different strategies:
   - assuming that the defining polynomial of $K = \mathbf{Q}(\alpha)$ is monic and integral, we can write every a_i as N_i/D_i with $N_i \in \mathbf{Z}[\alpha] \subseteq \mathcal{O}_K$ and $D_i \in \mathbf{Z}$;
   - for every a_i we can compute its denominator with respect to $\mathcal{O}_K$, i.e. the minimum $D_i \in \mathbf{N}$ such that $D_i \cdot a_i \in \mathcal{O}_K$.

Both decompositions yield a factorization of every a_i into a product of integral elements. Notice that the first decomposition can be obtained easily, while the second is more expensive. However, as at the end we want to obtain a product of integral elements having valuation zero at $\mathfrak{p}_i$, the second approach is (at the end) experimentally more performant, since the valuations of the elements tend to be smaller. After this step, we have a factorization $u = \prod b_i^{e_i}$ with $b_i \in \mathcal{O}_K$.

2. For the second step, we use a so-called anti-uniformizer, i.e. an element $x \in K$ such that $v_\mathfrak{p}(x) = -1$, $v_\mathfrak{q}(x) = 0$ for all the primes lying over p different from $\mathfrak{p}$ and $v_\mathfrak{q}(x) \geq 0$ for all the prime ideals $\mathfrak{q}$ not lying over p. Then, for every b_i we compute its valuation at $\mathfrak{p}$. If $v_\mathfrak{p}(b_i) = v > 0$, then we replace b_i by $b_i \cdot x^v$. By hypothesis, the element u has valuation 0 at $\mathfrak{p}$ and this operation does not change the product. Once we have done this, we finally get a factorization $u = \prod c_i^{e_i}$ with $c_i \in \mathcal{O}_K$ and $v_\mathfrak{p}(c_i) = 0$ for all i.
3. The last step consists in the evaluation of the element in the residue ring, i.e. computation of the product $\pi_i(u) = \prod \pi_i(c_i)^{e_i}$. This step is straightforward; the only remark is that we can reduce the exponents e_i modulo the exponent of the multiplicative group $(\mathcal{O}_K/\mathfrak{p}_i^{d_i})^\times$ to avoid inversions and reduce the size of the exponents.

Using this method, we can therefore compute the image $\iota(\mathcal{U}_K)$ in $(\mathcal{O}_K/\mathfrak{m})^\times$ and compute the quotient group.

Algorithm 2 Computation of $(\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{U}_K)$

```
Input: An abelian group $G$ together with a map $f_\mathfrak{m}$ that gives the isomorphism
    between $G$ and $(\mathcal{O}_K/\mathfrak{m})^\times$, generators for the unit group $u_1, \dots, u_l$ given
    in factored form.
Output: An abelian group $H$ together with an isomorphism $g_\mathfrak{m}$ between $H$
    and $(\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{U}_K)$.

1. Inizialize an empty list $L$.
2. For $i \in \{1, \dots, l\}$,
    • Write $u$ as a product of integral elements
    • Compute the projection $\pi(u)$ of $u$ into $(\mathcal{O}_K/\mathfrak{m})^\times$.
    • Add to $L$ the element of $G$ corresponding to $\pi(u)$ via $f_\mathfrak{m}$.
3. Compute the quotient group $H = G/\langle x \mid x \in L\rangle$ and the projection
    $q\colon G \to H$.
4. Define $g_\mathfrak{m}$ as the map such that $g_\mathfrak{m}(x) = f_\mathfrak{m}(y)$ for $x \in H$ and $y \in q^{-1}(x)$
    and $(g_\mathfrak{m})^{-1}(a) = q((f_\mathfrak{m})^{-1}(a))$.
5. Return $H, g_\mathfrak{m}$.
```

Computation of $\mathrm{Cl}_\mathfrak{m}$

We now focus on the computation of $\mathrm{Cl}_\mathfrak{m}$ using the sequence

$$1 \to (\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{U}_K) \longrightarrow \mathrm{Cl}_\mathfrak{m} \longrightarrow \mathrm{Cl} \longrightarrow 1 \tag{1.3}$$

For what concerns the computation of Cl, we refer to [7, 11].

Representatives of ideal classes By the exact sequence (1.3), given the lifts $g_1, \dots, g_t \in \mathcal{O}_K$ of generators of $(\mathcal{O}_K/\mathfrak{m})^\times/\iota(\mathcal{U}_K)$ and generators $I_1, \dots, I_s$ of Cl coprime to $\mathfrak{m}$, the products $g_i I_j$ for $i \in \{1, \dots, t\}$ and $j \in \{1, \dots, s\}$ generate Cl. In particular, we need to fix a set of representatives for the class group which behaves well with respect to multiplication and coprime to the modulus $\mathfrak{m}$. More precisely, assume that the class group Cl of $\mathcal{O}_K$ is given in Smith normal form, i.e. the relation matrix of the given set of generators $x_1, \dots, x_s$ of the group is diagonal with diagonal entries $d_1, \dots, d_s$ having the property that $d_i \mid d_{i+1}$ for $i = 1, \dots, s-1$. Then we pick representatives $I_1, \dots, I_s$ for the generators $x_1, \dots, x_s$ and extend them to a set of representatives for every class. At the same time, we need to compute a principal generator for the ideals $I_i^{d_i}$. As computing a generator for a principal ideal is in general expensive, we want to make sensible choices in order to achieve better performance. The class group can be identified as the cokernel of the map $\iota\colon \mathcal{U}_S \to \mathbf{Z}^{|S|}$ for a suitable set of prime ideals S, where every S-unit is sent to the vector corresponding to its valuation at the prime ideals in S. We denote the cokernel of this map by D. Let T be the isomorphism between Cl and D. Then the generators $x_1, \dots, x_s$ correspond via T to elements $y_1, \dots, y_s$ of D. This gives us a way of choosing a representative I_i for the classes of the x_i, just by taking the corresponding product of the prime ideals in S. To produce a generator for $I_i^{d_i}$, we notice that $d_i \cdot y_i$ is zero in D, which means that we can find via linear algebra a S-unit s_i such that $\iota(s_i) = d \cdot y_i$. This is the principal generator for the ideal $I_i^{d_i}$.

At this point, it only remains to ensure that these representatives are coprime to $\mathfrak{m}$. Given one of the representatives I_i, we compute the ideal $I_i + \mathfrak{m}_0$. If $I_i + \mathfrak{m}_0 = \mathcal{O}_K$, then I_i is coprime to $\mathfrak{m}$ and we can continue. Otherwise, let $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ be the prime ideals dividing $I_i + \mathfrak{m}_0$. Notice that this is a subset of the prime ideals dividing $\mathfrak{m}_0$, therefore we do not need any factoring algorithm but just to compute the valuation of I_i for each $\mathfrak{p}_j$. We search for an element z satisfying the following requirements:

- $v_{\mathfrak{p}_j}(z) = -v_{\mathfrak{p}_j}(I_i)$ for $j \in \{1, \dots, k\}$;
- $v_\mathfrak{p}(z) = 0$ for all prime ideals $\mathfrak{p}$ not dividing $\mathfrak{m}_0$;
- $v_\mathfrak{p}(z) \geq 0$ for any other prime ideal $\mathfrak{p}$.

Then the ideal zI_i will be coprime to $\mathfrak{m}_0$, as required. In order to find z, we suggest an approach via anti-uniformizers. Notice that we are assuming that the input is an integral ideal, so that $v_\mathfrak{p}(I_i) \geq 0$ for every prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. Let $p_1, \dots, p_h$ be the rational primes lying underneath the support of $\mathfrak{m}_0$.

- For every prime ideal $\mathfrak{p}_{k,j}$ lying over p_k, we consider the anti-uniformizer $z_{\mathfrak{p}_{k,j}}$ and take the element $s_{\mathfrak{p}_{k,j}} = z_{\mathfrak{p}_{k,j}}^{v_{\mathfrak{p}_{k,j}}(I_i)}$.

- For each index $k \in \{1, \dots, h\}$, we compute the product z_{p_k} of the elements $s_{\mathfrak{p}_{k,j}}$ for $\mathfrak{p}_{k,j}$ lying over p_k.
- Initialize $z = z_{p_1}$; then, for $i = 2, \dots, h$,
  - compute a Bézout's identity between $\prod_{s=1}^{i-1} p_s \in \mathbf{Z}$ and $p_i \in \mathbf{Z}$, so that $1 = \gamma + \delta$ with $p_i \mid \gamma$ and $p_s \mid \delta$ for $s \leq i-1$;
  - update $z = z_{p_i}\delta + z\gamma$.

It is easy to see that the final z satisfies the requirements. This method is deterministic and, compared to [15, Algorithm 1.3.14], it is often preferable as it does not involve linear algebra which could be expensive if the field degree is too large.

Example 1.26. We consider the number field $K = \mathbf{Q}(\sqrt{-5})$. The class group of K is isomorphic to C_2 and we find as a generator the ideal $I = (6, 3\sqrt{-5}+3)$. If we want to compute the ray class group $\mathrm{Cl}_\mathfrak{m}$ with $\mathfrak{m} = (6\mathcal{O}_K, \{\})$, we need to find a different representative for $[I]$. Following the algorithm, we consider the rational primes $p_1 = 2$ and $p_2 = 3$.

There is a unique prime ideal lying over 2, namely $\mathfrak{p}_{1,1} = (2, \sqrt{-5}+1)$. The valuation of I at $\mathfrak{p}_{1,1}$ is 1 and so we take $z_{p_1} = (3\sqrt{-5}+1)/2$.

There are 2 prime ideals lying over p_2, namely $\mathfrak{p}_{2,1} = (3, \sqrt{-5}+1)$ and $\mathfrak{p}_{2,2} = (3, \sqrt{-5}-1)$. The valuation of I at them is equal to 1, so we take $z_{p_2} = (4\sqrt{-5}+4)/3 \cdot (4\sqrt{-5}+5)/3 = 4\sqrt{-5} - 20/3$.

The last step is to combine the elements via a Bézout's identity between p_1 and p_2. Since $-p_1 + p_2 = 1$, we take $z = -p_1 z_{p_2} + p_2 z_{p_1}$, giving $z = (-21\sqrt{-5} + 89)/6$. The representative that we take as a generator for the class group is then the ideal zI.

Algorithm 3 Ray Class Group Modulo $\mathfrak{m}$

Input: The class group Cl of K with relation matrix $C = \mathrm{Diag}(d_1, \dots, d_s)$ in Smith normal form, the unit group $\mathcal{U}_K$ of K, the group $(\mathcal{O}_K/\mathfrak{m})^\times$.

Output: An abstract group A isomorphic to the the ray class group $\mathrm{Cl}_\mathfrak{m}$ together with representative for each generator of A.

1. Compute representatives $I_1, \dots, I_s$ for the generators of Cl that are coprime to m.
2. Compute principal generators $\alpha_1, \dots, \alpha_s$ for $I_1^{d_1}, \dots, I_s^{d_s}$.
3. Compute the quotient group $Q = (\mathcal{O}_K/\mathfrak{m})^\times/\mathcal{U}_K$ using Algorithm 2. Let M_Q be relation matrix of the quotient.
4. Compute the matrix D whose rows are the discrete logarithm of $\alpha_1, \dots, \alpha_s$ in Q.
5. Define A as the abelian group with relation matrix given by
$$\begin{pmatrix} C & -D \\ 0 & M_Q \end{pmatrix}$$
6. Set the representatives of the generators as $I_1, \dots, I_s, (w_1), \dots, (w_t)$.

7. Return A and the set of representatives.

The discrete logarithm map associating to each ideal the corresponding element of A is slightly more complicated. In the same notation of the pseudocode, given an ideal $\mathfrak{J} \in \mathrm{I}^{\mathfrak{m}}$, we do the following.

- Compute the discrete logarithm of $\mathfrak{J}$ in Cl as $(q_1, \dots, q_s)$.
- Using the chosen set of representatives $I_1, \dots, I_s$, compute the ideal $\mathcal{I} = I_1^{q_1} \dots I_s^{q_s}$ in the same class as $\mathfrak{J}$.
- Compute a principal generator y of $\mathfrak{J} \cdot \mathcal{I}^{-1}$.
- Compute the discrete logarithm of y in $(\mathcal{O}_K/\mathfrak{m})^\times/\mathcal{U}_K$, so that $y = \prod_{i=1}^t w_i^{r_i}$.
- Return the element of A with coordinates $(q_1, \dots, q_s, r_1, \dots, r_t)$.

Remark 1.27. The discrete logarithm is easier in the case the ideal $\mathfrak{J}$ is known to be principal with generator β. In this case, we can skip the first three steps and the algorithm reduces to the computation of the discrete logarithm of β in the factor group $(\mathcal{O}_K/\mathfrak{m})^\times/\mathcal{U}_K$.

Issues For the computation of the structure of the ray class group, the most expensive steps in the algorithm are the computation of the discrete logarithms in the residue rings and the computation of the principal ideal generators of the powers of $I_1, \dots, I_s$, assuming that the unit group and the class group are already at our disposal. The discrete logarithm function has several bottlenecks, as it requires a computation of a discrete logarithm in the class group, of a principal generator of a given ideal and a discrete logarithm in a residue ring of $\mathcal{O}_K$: these operations are costly.

1.2.1 Quotients of ray class groups

Abelian extensions of K with Galois group of exponent n correspond to congruence subgroups H of ray class groups $\mathrm{Cl}_{\mathfrak{m}}$ such that $\mathrm{Cl}_{\mathfrak{m}}/H$ is of exponent n, that is, to subgroups H with $\mathrm{Cl}_{\mathfrak{m}}^n \subseteq H \subseteq \mathrm{Cl}_{\mathfrak{m}}$. Thus, abelian extensions of exponent n can be identified with subgroups of the quotient $\mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^n$. We now show how to directly construct $\mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^n$, following the exposition of [26].

Reduction to the prime power case By means of the Chinese remainder theorem, we can assume that $n = p^s$ is a prime power. Indeed, if n factors as $n = \prod_{i=1}^r p_i^{e_i}$, we get

$$\mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^n \cong \prod_{i=1}^r \mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^{p_i^{e_i}}.$$

Thus, if we are able to construct the quotients for the different prime divisors of n, we can compute $\mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^n$ as the direct product.

Conditions on the modulus The first observation is that the hypotheses imply some restrictions on the primes appearing in the modulus and their exponents by Lemma 1.16. Indeed, let $\mathfrak{m}_0 = \prod \mathfrak{p}_i^{e_i}$ be the factorization of $\mathfrak{m}_0$ into prime ideals. Then the only primes appearing with exponent greater then one are the primes lying over a divisor of n. Moreover, we will see in Section 1.4 that we can also bound the exponent for these primes. For the others, we have that $N(\mathfrak{p}_i) - 1$ must be not coprime to n.

Sequence of factor groups While for finite abelian groups, the functor $A \mapsto A/p^s A$ is in general only right exact, we can use the exact sequence of Proposition 1.24 together with the following lemma to construct the quotient directly.

Lemma 1.28 ([26, Lemma 3]). *Let* $0 \to A \to B \to C \to 0$ *be an exact sequence of finite abelian groups. Let* $p \in \mathbf{Z}_{>0}$ *be a prime number and* $k \in \mathbf{Z}_{>0}$ *with* $k \geq v_p(|B|)$*. Then the following sequence is exact:*

$$1 \to A/p^k A \to B/p^k B \to C/p^k C \to 1.$$

Proof. The lemma follows from the following trivial observations:

- an abelian group M is the product of its p-Sylow subgroups P_i;
- if $M \simeq \prod P_i$ and $w \in \mathbf{Z}_{\geq 0}$, then $M/M^w \simeq \prod P_i/P_i^w$;
- if w is coprime to the order of M, then $\#M/M^w = 0$;
- if w is a multiple of the order of M, then $M^w = 0$ and $M/M^w \simeq M$.

In order to apply Lemma 1.28 to the exact sequence in Proposition 1.24, we need to bound the valuation at p of the exponent of $\mathrm{Cl}_\mathfrak{m}$. It is straightforward to see that $\tilde{s} = v_p(\#(\mathcal{O}_K/\mathfrak{m})^\times) + v_p(\#\mathrm{Cl})$ gives the desired bound.

Consequences for the algorithm According to Lemma 1.28, if $\tilde{n} = p^{\tilde{s}}$, we can construct $\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^{\tilde{n}}$ by working only with $\mathrm{Cl}/\mathrm{Cl}^{\tilde{n}}$ and $(\mathcal{O}_K/\mathfrak{m})^\times/(\mathcal{O}_K/\mathfrak{m})^{\times\tilde{n}}$. This is highly beneficial for the whole algorithm, because

- the number of generators of $\mathrm{Cl}_\mathfrak{m}/\mathrm{Cl}_\mathfrak{m}^{\tilde{n}}$ might be smaller than $\mathrm{Cl}_\mathfrak{m}$, so that we can avoid the computation of some principal ideal generators;
- we only need to construct $(\mathcal{O}_K/\mathfrak{m})^\times$ modulo $\tilde{n}$-th powers, whose structure can be obtained more easily.

The second point is crucial and it speeds up the discrete logarithm function too. Let $\mathfrak{q}$ be a prime ideal divisor of $\mathfrak{m}_0$ and $l = v_\mathfrak{q}(\mathfrak{m}_0)$. Recall that by [15, Proposition 4.2.4] we have

$$(\mathcal{O}_K/\mathfrak{q}^l)^\times \cong (\mathcal{O}_K/\mathfrak{q})^\times \times (1+\mathfrak{q})/(1+\mathfrak{q}^l).$$

We distinguish two cases, depending on the power of $\mathfrak{q}$ dividing the modulus.

$l = 1$ Under this assumption, we know that $p \mid N(\mathfrak{q})-1$. Let $e = v_p(N(\mathfrak{q})-1)$. and denote by G the group $(\mathcal{O}_K/\mathfrak{q})^\times$. Finding a generator of the group $G/\tilde{n}G$ is equivalent to finding an element of G of order divisible by p^e.

Such an element can be found by picking random elements with high probability: indeed, let g be an element of G and let $s = (N(\mathfrak{q}) - 1)/p^e$. Then g is a generator of $G/\tilde{n}G$ if $g^{sp^{e-1}}$ is not trivial. The probability of finding an element of order divisible by p^e is $\phi(p^e)/p^e = (p-1)/p$, which is always greater than 1/2: a few attempts will suffice. The discrete logarithm is simplified too, as it is reduced to a discrete logarithm problem in a cyclic group of order p^e. Since e is usually small, in our application the Baby Step-Giant Step algorithm is enough for this purpose.

$l > 1$ In this case, $p \nmid N(\mathfrak{q}) - 1$ and we can avoid computing the multiplicative group of the residue field altogether, since its order is not divisible by p.

Since in this way we have constructed the quotient $A = \mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^{\tilde{n}}$, as a final step we have to factor A by A^n.

Example 1.29. We consider the special case $K = \mathbf{Q}$. If we want to construct the quotient $\mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^2$ for $\mathfrak{m} = (101\mathbf{Z}, \{\})$, according to the discussion above, we do not need to construct the multiplicative group $(\mathbf{Z}/101\mathbf{Z})^\times$, but just its 2-Sylow subgroup, which has order 4. A generator for the 2-Sylow subgroup is $10 \in (\mathbf{Z}/101\mathbf{Z})^\times$.

1.3 Conductor and discriminant

The knowledge of the ideal class of an abelian extension allows to compute some of the invariants of the extension without the use a primitive element. This section is devoted to the discussion of the algorithms to compute the conductor and of the discriminant of an abelian extension, given as a congruence subgroup $A_{\mathfrak{m}}$ of a ray class group $\mathrm{Cl}_{\mathfrak{m}}$. The algorithms we present are an improvement on the methods presented in [18] as they avoid the computation of some ray class groups. In practice, most of the information that is needed has already been computed during the ray class group algorithm.

Conductor of an abelian extension

We now deal with the problem of computing the conductor $\mathfrak{f}$ of an abelian extension given as an ideal class $A_{\mathfrak{m}}$ in a suitable ray class group $\mathrm{Cl}_{\mathfrak{m}}$. We will use the following characterization of the conductor:

Lemma 1.30. *Let $A_{\mathfrak{m}}$ be a congruence subgroup in $\mathrm{Cl}_{\mathfrak{m}}$ and let $\mathfrak{f}$ be its conductor. Let $\mathfrak{n}$ be a modulus such that the kernel of projection $\pi\colon \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{n}}$ is contained in $A_{\mathfrak{m}}$, i.e. $[\mathrm{Cl}_{\mathfrak{m}} : A_{\mathfrak{m}}] = [\mathrm{Cl}_{\mathfrak{n}} : \pi(A_{\mathfrak{m}})]$. Then $\mathfrak{f} \mid \mathfrak{n}$.*

As $\mathfrak{f} \mid \mathfrak{m}$, we know that the places dividing the conductor $\mathfrak{f}$ are a subset of the places dividing $\mathfrak{m}$. Thus, for every prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}$, we want to determine the valuation of $\mathfrak{f}_0$ (the finite part of $\mathfrak{f}$) at $\mathfrak{p}$ and, for every infinite place $\mathfrak{v}$ appearing in $\mathfrak{m}_\infty$, we want to determine whether it divides $\mathfrak{f}_\infty$.

Finite places Let $\mathfrak{p}$ be a prime ideal dividing $\mathfrak{m}$ and let $e = v_{\mathfrak{p}}(\mathfrak{m}_0)$. The strategy is to compute the projections $\pi_{s-1}\colon \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{m}\mathfrak{p}^{1-s}}$ for $s \in \{2, \dots, e\}$ until we find a projection such that the kernel is not contained in $A_{\mathfrak{m}}$ or we determine that $\mathfrak{p}$ does not divide the conductor $\mathfrak{f}$. We proceed recursively: assume that we have already computed the kernel of the projection map $\pi_{s-1}\colon \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{m}\mathfrak{p}^{1-s}}$ for $s \in \{1, \dots, e\}$ and that $A_{\mathfrak{m}}$ contains it. Now, we want to compute the kernel of the projection map $\pi_s\colon \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{m}\mathfrak{p}^{-s}}$.

Proposition 1.31. *Let $\mathfrak{m}_0 = \prod_{j=1}^{r} \mathfrak{p}_j^{e_j}$ be the factorization into prime ideals of the finite part $\mathfrak{m}_0$ of $\mathfrak{m}$ and let $\mathfrak{v}_1, \dots, \mathfrak{v}_t$ be the infinite places in $\mathfrak{m}_\infty$. Given $i \in \{1, \dots, r\}$ and $s \in \{1, \dots, e_i\}$, let $y_1, \dots, y_l \in \mathcal{O}_K$ be elements such that the principal ideals $(y_1), \dots, (y_l)$ generate the kernel of π_{s-1}. Consider $x_1, \dots, x_k \in \mathcal{O}_K$ such that*

- *if $s < e_i$, $\bar{x}_1, \dots, \bar{x}_k$ generate the group $(1 + \mathfrak{p}^{e_i - s})/(1 + \mathfrak{p}^{e_i})$;*
- *if $s = e_i$, $\bar{x}_1, \dots, \bar{x}_k$ generate the group $(\mathcal{O}_K/\mathfrak{p}^e)^\times$;*
- *$x_j \equiv 1 \pmod{\mathfrak{p}_l^{e_l}}$ for $l \in \{1, \dots, r\} \setminus \{i\}$ and $j \in \{1, \dots, k\}$;*
- *$x_1, \dots, x_k$ are positive at $\mathfrak{v}_1, \dots, \mathfrak{v}_t$.*

Then the principal ideals $(y_1), \dots, (y_l), (x_1), \dots, (x_k)$ generate the kernel of the projection π_s.

Proof. Denote by $\mathfrak{n}_1, \mathfrak{n}_2$ the moduli $\mathfrak{m}\mathfrak{p}^{1-s}$ and $\mathfrak{m}\mathfrak{p}^{-s}$ respectively and consider the commutative diagram

$$\begin{tikzcd}
(\mathcal{O}_K/\mathfrak{n}_1)^\times \arrow[r] \arrow[d, "\pi"'] & \mathrm{Cl}_{\mathfrak{n}_1} \arrow[r] \arrow[d, "\tilde{\pi}"'] & \mathrm{Cl}_K \arrow[r] \arrow[d, "\mathrm{id}"'] & 1 \\
(\mathcal{O}_K/\mathfrak{n}_2)^\times \arrow[r] & \mathrm{Cl}_{\mathfrak{n}_2} \arrow[r] & \mathrm{Cl}_K \arrow[r] & 1
\end{tikzcd}$$

where $\pi\colon (\mathcal{O}_K/\mathfrak{n}_1)^\times \to (\mathcal{O}_K/\mathfrak{n}_2)^\times$ is the natural projection. The exactness of the horizontal sequences implies that the kernel of $\tilde{\pi}$ is contained in the image of $(\mathcal{O}_K/\mathfrak{n}_1)^\times$ in $\mathrm{Cl}_{\mathfrak{n}_1}$. The elements $x_1, \dots, x_s$ are chosen exactly to generate the kernel of π; since π_s is the composition of π_{s-1} and $\tilde{\pi}$, the claim follows.

By virtue of Proposition 1.31, we need to compute elements as in the statement in order to produce the kernel of the projection and check if they are contained in $A_{\mathfrak{m}}$. In particular, we do not need to compute the ray class groups $\mathrm{Cl}_{\mathfrak{m}\mathfrak{p}^{-s}}$, which would have been expensive.

Algorithm 4 Valuation of the conductor at a prime ideal $\mathfrak{p}$

```
Input: A norm group $A_{\mathfrak{m}} \subseteq \mathrm{Cl}_{\mathfrak{m}}$, a prime ideal $\mathfrak{p}$.
Output: The valuation of the conductor of $A_{\mathfrak{m}}$ at $\mathfrak{p}$.

1. Set $n = [\mathrm{Cl}_{\mathfrak{m}} \colon A_{\mathfrak{m}}]$.
2. Set $p = \min \mathfrak{p} \cap \mathbf{N}$
3. Compute the valuation $e$ of $\mathfrak{m}$ at $\mathfrak{p}$.
```

```
4. If $e = 0$, return 0.
5. If $e > 1$, $(p, n) = 1$ and $(N(\mathfrak{p}) - 1, n) = 1$, return 0.
6. Inizialize an empty list $L$ of elements of $\mathrm{Cl}_{\mathfrak{m}}$
7. For $i = e, \dots, 2$,
     • Compute generators $x_{i,1}, \dots, x_{i,s_i} \in \mathcal{O}_K$ of $1 + \mathfrak{p}^{i-1}/1 + \mathfrak{p}^i$.
     • Compute the discrete logarithms $y_{i,1}, \dots, y_{i,s_i}$ of $(x_{i,1}), \dots, (x_{i,s_i})$ in $\mathrm{Cl}_{\mathfrak{m}}$.
     • Add $y_{i,1}, \dots, y_{i,s_i}$ to $L$.
     • Compute the factor group $F$ of $\mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}}$ modulo the subgroup generated by the elements in $L$.
     • If $F$ doesn't have the same order as $\mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}}$, return $e$.
8. If $(N(\mathfrak{p}) - 1, n) = 1$, return 0.
9. Compute a generator $x$ of $(\mathcal{O}_K/\mathfrak{p})^\times$.
10. Compute the discrete logarithm $y$ of $(x)$ in $\mathrm{Cl}_{\mathfrak{m}}$.
11. Compute the factor group $F$ of $\mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}}$ modulo the subgroup generated by the elements in $L$.
12. If $F$ doesn't have the same order as $\mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}}$, return 1. Otherwise return 0.
```

The only part we miss is to find the elements $x_1, \dots, x_k$ of Proposition 1.31. In the same notation as in the proposition, assume that we already have generators for the kernel of π_{s-1}. Then, according to the proposition, we need to provide generators for either $(\mathcal{O}_K/\mathfrak{p})^\times$ if $s = e$ or $(1 + \mathfrak{p}^{e-s})/(1 + \mathfrak{p}^{e-s-1})$. We distinguish two cases.

$e \neq s$ If $y_1, \dots, y_s \in \mathcal{O}_K$ are generators for the additive group $\mathfrak{p}^{e-s-1}/\mathfrak{p}^{e-s}$, then $1 + y_1, \dots, 1 + y_s$ generate $(1 + \mathfrak{p}^{e-s-1})/(1 + \mathfrak{p}^{e-s})$ ([15, Proposition 4.2.14]). Computing generators of the additive groups is straightforward, as we could just take a $\mathbf{Z}$-basis for $\mathfrak{p}^{e-s-1}$. On the other hand, depending on the degree of K, it might be convenient to compute a basis for $\mathfrak{p}^{e-s-1}/\mathfrak{p}^{e-s}$ as a $\mathbf{Z}$-module, as in this way we get fewer generators. This can be done using linear algebra as in [15, Algorithm 4.2.15].

$e = s$ According to Proposition 1.31, we need a generator of $(\mathcal{O}_K/\mathfrak{p})^\times$. Notice that the kernel of the composition

$$(\mathcal{O}_K/\mathfrak{p})^\times \to \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}}$$

contains the subgroup of $(\mathcal{O}_K/\mathfrak{p})^\times$ generated by the n-th powers, where n is the exponent of $\mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}}$. This means for our purpose it suffices to have a generator of $(\mathcal{O}_K/\mathfrak{p})^\times/((\mathcal{O}_K/\mathfrak{p})^\times)^n$. Such an element can be found more easily than a generator of $(\mathcal{O}_K/\mathfrak{p})^\times$, as we have seen in Subsection 1.2.1.

We still need to change the generators we have so that they satisfy the third and the forth conditions of Proposition 1.31. Let z be one of the generators we have computed. If $u, v \in \mathcal{O}_K$ are idempotents for $\mathfrak{p}^e$ and $\mathfrak{m}_0\mathfrak{p}^{-e}$, i.e. elements such that $u \in \mathfrak{p}^e$, $v \in \mathfrak{m}_0\mathfrak{p}^{-e}$ and $u+v=1$, then $vz+u$ is an element satisfying the requirements at the finite primes. In order to make the element positive at all the infinite places, we add to it a sufficiently large multiple of $\min \mathfrak{m}_0 \cap \mathbf{N}$.

Infinite places Let $\mathfrak{v}_1, \dots, \mathfrak{v}_r$ be an infinite place dividing $\mathfrak{m}$. We follow the same strategy as before; in particular, the same proof as in Proposition 1.31 yields the following:

Proposition 1.32. *Let $\mathfrak{m}_0$ be the finite part of $\mathfrak{m}$ and let $\mathfrak{v}_1, \dots, \mathfrak{v}_t$ be the infinite places in $\mathfrak{m}_\infty$. Given $i \in \{1, \dots, t\}$, consider $x \in \mathcal{O}_K$ such that*

- *$x \equiv 1 \pmod{\mathfrak{m}_0}$,*
- *x is negative at $\mathfrak{v}_i$,*
- *x is positive at $\mathfrak{v}_j$ for $j \in \{1, \dots, t\} \setminus \{i\}$.*

Then the ideal (x) generates the kernel of the projection $\pi_{\mathfrak{v}_i} \colon \mathrm{Cl}_\mathfrak{m} \to \mathrm{Cl}_{\mathfrak{m}\mathfrak{v}_i^{-1}}$.

According to Proposition 1.32, for each $i \in \{1, \dots, t\}$, we need to find an elements $x_i \in \mathcal{O}_K$ such that $x_i \equiv 1 \pmod{\mathfrak{m}_0}$, $|x_i|_{\mathfrak{v}_i} < 0$ and $|x_i|_{\mathfrak{v}_j} > 0$ for $j \in \{1, \dots, r\} \setminus \{i\}$. This can be done in practice quite easily by taking random elements as in [15, Algorithm 4.2.20]. Then $\mathfrak{v}_i$ divides the conductor if and only if (x_i) is not contained in $A_\mathfrak{m}$.

Example 1.33. Let $K = \mathbf{Q}$ and let $\mathfrak{m} = (k\mathbf{Z}, \infty)$ be a modulus of K, with $k \in \mathbf{Z}$ a positive integer. Let $A_\mathfrak{m}$ be a congruence subgroup modulo $\mathfrak{m}$. In order to compute the conductor of $A_\mathfrak{m}$, we need to produce elements as in Proposition 1.32 and Proposition 1.31. For what concerns the infinite place, we need a negative integer $x \in \mathbf{Z}$ such that $x \equiv 1 \pmod{k}$. This is straightforward, as $1-k$ is an element satisfying the requirements. For the finite places, we need to factor $k = \prod_{i=1}^{r} p_i^{e_i}$ into prime numbers. For each prime number p_i, we have to compute the valuation of the conductor of $A_\mathfrak{m}$ at p_i. For $s \in \{2, \dots e_i\}$, we then need an element $x \in \mathbf{Z}$ that generates the group $1 + (p_i)^{s-1}/1 + (p_i)^s$ and such that $x \equiv 1 \pmod{k/p_i^{e_i}}$. First, we focus on finding a generator of $1 + (p_i)^{s-1}/1 + (p_i)^s$.

$p_i = 2$ We know that in this case the group $1 + (2)/1 + (2)^s$ is generated by 5. Thus a suitable power of 5 in $\mathbf{Z}/2^{e_i}\mathbf{Z}$ generates $1 + (2)^{s-1}/1 + (2)^s$.

$p_i \neq 2$ The group $1 + (p_i)/1 + (p_i)^s$ is generated by $1 + p_i$. Thus a suitable power of $1 + p_i$ generates $1 + (p_i)^{s-1}/1 + (p_i)^s$.

After having found such a generator x, we need to make it satisfy the second condition. This can be easily done by computing a Bézout identity between $k/p_i^{e_i}$ and $p_i^{e_i}$, so that we find elements $\delta, \gamma \in \mathbf{Z}$ such that $\delta + \gamma = 1$, $k/p_i^{e_i} \mid \gamma$ and $p_i^{e_i} \mid \delta$. Then the element $\gamma x + \delta$ is the desired one.

For $s = 1$, we need to produce an element $x \in \mathbf{Z}$ such that $x \equiv 1 \pmod{k/p_i^{e_i}}$ and x generates the multiplicative group of $\mathbf{Z}/p_i\mathbf{Z}$. In this case, we can assume that $p_i \neq 2$ (it is trivial). Let c be the largest divisor of $p_i - 1$ coprime to $[\mathrm{Cl}_\mathfrak{m} \colon A_\mathfrak{m}]$; then we compute an element $\bar{y}$ of $(\mathbf{Z}/p_i\mathbf{Z})^\times$ of order $p_i - 1/c$ by picking random elements. Let $y \in \mathbf{Z}$ be a lift of $\bar{y}$; then we need to change y so that it satisfies the condition $y \equiv 1 \pmod{k/p_i^{e_i}}$. As above, we can do it by computing a Bézout's identity.

Test whether a modulus is the conductor In most applications, it is relevant to decide whether the defining modulus $\mathfrak{m}$ is the conductor of a subgroup $A_\mathfrak{m} < \mathrm{Cl}_\mathfrak{m}$. This problem is slightly easier, as we could stop Algorithm 4 after the first iteration of Step (7) if the exponent is greater than one.

Discriminant of an abelian extension

The computation of the discriminant of an abelian extension follows the same approach as the computation of the conductor. Indeed, these invariants are related by the discriminant-conductor formula of Theorem 1.17. More specifically, we can compute the valuation of the discriminant at a prime ideal $\mathfrak{p}$ by computing the index of the projection of $A_\mathfrak{m}$ in the quotients $\mathrm{Cl}_{\mathfrak{m}/\mathfrak{p}^i}$ for $i = 0, \dots, v_\mathfrak{p}(\mathfrak{m})$. As we have seen in Proposition 1.31 how to compute the kernel of the projections, we can use the same strategy as the algorithm for the the conductor. Notice that in this way we can compute the relative discriminant $\operatorname{disc} L/K$; in order to compute the absolute discriminant of L, we use the formula $|\operatorname{disc} L| = |\operatorname{disc} K|^{[L:K]} N(\operatorname{disc} L/K)$. To determine the sign of the absolute discriminant, in general we need to determine the signature of L, which can be read off from the conductor of L as in [15, Proposition 3.5.8]. We now illustrate in pseudocode how to compute the valuation of the discriminant $\operatorname{disc} L/K$ at a prime ideal $\mathfrak{p}$:

Algorithm 5 Valuation of the discriminant at a prime ideal $\mathfrak{p}$

```
Input: A norm group $A_\mathfrak{m} \subseteq \mathrm{Cl}_\mathfrak{m}$, a prime ideal $\mathfrak{p}$.
Output: The valuation at $\mathfrak{p}$ of the discriminant of the abelian extension corresponding to $\mathfrak{A}_\mathfrak{m}$.

1. Set $n = [\mathrm{Cl}_\mathfrak{m} : A_\mathfrak{m}]$.
2. Set $p = \min \mathfrak{p} \cap \mathbf{N}$
3. Compute the valuation $e$ of $\mathfrak{m}$ at $\mathfrak{p}$.
4. Initialize an empty list $L$ of elements of $\mathrm{Cl}_\mathfrak{m}$.
5. $v = e \cdot n$.
6. For $i = e, \dots, 2$,
    • Compute generators $x_{i,1}, \dots, x_{i,s_i} \in \mathcal{O}_K$ of $1 + \mathfrak{p}^{i-1}/1 + \mathfrak{p}^i$.
    • Compute the discrete logarithms $y_{i,1}, \dots, y_{i,s_i}$ of $(x_{i,1}), \dots, (x_{i,s_i})$ in $\mathrm{Cl}_\mathfrak{m}$.
    • Add $y_{i,1}, \dots, y_{i,s_i}$ to $L$.
    • Compute the factor group $F$ of $\mathrm{Cl}_\mathfrak{m}/A_\mathfrak{m}$ modulo the subgroup generated by the elements in $L$.
    • $v = v - |F|$.
7. Compute a generator $x$ of $(\mathcal{O}_K/\mathfrak{p})^\times$.
8. Compute the discrete logarithm $y$ of $(x)$ in $\mathrm{Cl}_\mathfrak{m}$.
```

```
 9. Compute the factor group $F$ of $\mathrm{Cl}_\mathfrak{m}/A_\mathfrak{m}$ modulo the subgroup generated
    by the elements in $L$.
10. $v = v - |F|$.
11. Return $v$.
```

1.4 Bounds on the conductor

We have discussed in the previous sections the tools that are in practice necessary to parametrize abelian extensions of a number field K: each abelian extension of conductor $\mathfrak{m}$ can be represented via a subgroup of a ray class group. Moreover, we have seen an algorithm to compute the discriminant of an extension from the knowledge of its ideal class. However, we still need a characterization of the conductors depending on the requirements on the abelian extensions. In this section, we focus on bounds on the prime ideals dividing the conductor of an abelian extension of K with absolute discriminant lower than $B \in \mathbf{N}$.

Let L be an abelian extension of K such that $|\operatorname{disc} L| \leq B$. First of all, we notice that the prime ideals dividing the conductor of L/K are exactly the primes that ramify in L/K and they must satisfy the following bound:

Lemma 1.34. *Let $\mathfrak{p}$ be a prime ideal of K ramified in L. Assume that $|\operatorname{disc} L| \leq B$. Then $N(\mathfrak{p}) \leq B/|\operatorname{disc} K|^{[L:\,K]}$.*

Proof. It follows from the formula $|\operatorname{disc} L| = |\operatorname{disc} K|^{[L:\,K]} N(\operatorname{disc} L/K)$ and the multiplicativity of the norm.

This simple bound has as a consequence the fact that the prime ideals that can appear in the conductor of L are only finitely many. We now try to give stronger conditions on them and their exponents depending on their ramification behaviour.

1.4.1 Tamely ramified primes

Let $\mathfrak{p}$ be a prime ideal of K and let L be an abelian extensions of degree m. We now deal with the case in which the prime number p underneath $\mathfrak{p}$ is coprime to m. In this case, $\mathfrak{p}$ is either unramified in L (and so it does not divide the conductor of the extension) or it is tamely ramified in L and the following constraints hold:

Lemma 1.35. *Let L/K be an abelian extension of degree m and let $\mathfrak{p}$ be a prime ideal of K tamely ramified in L. Let $\mathfrak{m}_0$ be the finite part of the conductor of L/K. Then:*

- $\gcd(N(\mathfrak{p}) - 1, m) \neq 1$,
- $v_\mathfrak{p}(\mathfrak{m}_0) = 1$.

Proof. Follows immediately from Lemma 1.16.

Moreover, we can relate the valuation of the discriminant at $\mathfrak{p}$ and its ramification index in L/K by using Theorem 1.17, which implies that the valuation of $\operatorname{disc} L/K$ at $\mathfrak{p}$ is equal to $m - \frac{m}{e}$. In particular, let k be the smallest prime dividing $\gcd(m, N(\mathfrak{p}) - 1)$. Since k is a lower bound on e, the exponent of $\mathfrak{p}$ in $\operatorname{disc} L/K$ must be at least $m - \frac{m}{k}$. This improves upon Lemma 1.34:

Lemma 1.36. *Let $\mathfrak{p}$ be a prime ideal of K tamely ramified in L. Assume that $|\operatorname{disc} L| \leq B$ and denote by k the minimal prime divisor of $m = [L\colon K]$. Then*

$$N(\mathfrak{p})^{m-\frac{m}{k}} \leq \frac{B}{|\operatorname{disc} K|^{[L\colon K]}}.$$

1.4.2 Wildly ramified primes

Let $\mathfrak{p}$ be a prime ideal of K lying over a prime number p dividing the degree m of L/K. In this case, the bound of Lemma 1.34 does not give a constraint on the maximal exponent of $\mathfrak{p}$ dividing the conductor $\mathfrak{f}$ of L/K. We will now present different bounds depending both on the structure of the Galois group $\operatorname{Gal}(L/K)$ and the discriminant bound B.

Reduction to cyclic extensions First of all, we notice that for this purpose we can assume that L is cyclic.

Lemma 1.37. *Let $L_1, \ldots, L_k$ be abelian extensions of a number field K with conductors $\mathfrak{f}_1, \ldots, \mathfrak{f}_k$ respectively. Let L be the composite of $L_1, \ldots, L_k$. Then:*

- *the conductor of L/K is the least common multiple of $\mathfrak{f}_1, \ldots, \mathfrak{f}_k$;*
- $\operatorname{disc} L_i/K \leq \sqrt[[L:L_i]]{\operatorname{disc} L/K}$.

From now on, we assume that L is cyclic of degree $m = p^s$ and it satisfies the discriminant bound of the lemma.

From discriminant to conductor

The first bound that we present does not really depend on the structure of the field but it comes directly from the bound of the discriminant of L. More specifically, we show that if we have a bound on the discriminant of L/K, we can get a bound on the exponent of $\mathfrak{p}$ in the conductor by means of Theorem 1.17. Let $\mathfrak{f}$ be the conductor of L/K and let p^s be the degree of L; then

$$v_{\mathfrak{p}}(\operatorname{disc} L/K) \geq p^s v_{\mathfrak{p}}(\mathfrak{f}) - p^{s-1} v_{\mathfrak{p}}(\mathfrak{f}) = v_{\mathfrak{p}}(\mathfrak{f})(p^s - p^{s-1})$$

We now isolate $v_{\mathfrak{p}}(\mathfrak{f})$ to get the following:

Lemma 1.38. *Let L be an abelian extension of a number field K of degree p^s, where p is a prime number. Let $\mathfrak{p}$ be a prime ideal of K and $\mathfrak{f}$ be the conductor of L/K. Then*

$$v_{\mathfrak{p}}(\mathfrak{f}) \leq \frac{v_{\mathfrak{p}}(\operatorname{disc} L/K)}{p^s - p^{s-1}}.$$

The bound that we present here on $v_{\mathfrak{p}}(\operatorname{disc} L/K)$ is quite simple and uses the same formula as Lemma 1.34.

Lemma 1.39. *Let L/K be an abelian extension and let $\mathfrak{p}$ be a prime ideal in K. If $|\operatorname{disc} L| \leq B$, then*

$$v_{\mathfrak{p}}(\operatorname{disc} L/K) \leq \log_{N(\mathfrak{p})} B - [L\colon K] \log_{N(\mathfrak{p})} |\operatorname{disc} K|$$

Proof. As $|\operatorname{disc} L| = |\operatorname{disc} K|^{[L\colon K]} N(\operatorname{disc} L/K)$, we have that $N(\operatorname{disc}(L/K)) \leq B/|\operatorname{disc} K|^{[L\colon K]}$. Isolating the contribution of $\mathfrak{p}$, we get $N(\mathfrak{p})^{v_{\mathfrak{p}}(\operatorname{disc} L/K)} \leq B/|\operatorname{disc} K|^{[L\colon K]}$. Thus, if we take the logarithm with base $N(\mathfrak{p})$, we get the desired formula.

This bound is quite important for small examples, as it gives a relation between the maximal exponent and the discriminant bound B; however, if the bound B is large, it becomes quite useless, and we need to combine it with other bounds.

We present now a bound on the valuation of the discriminant of L at a prime ideal $\mathfrak{p}$, coming from the study of the local different.

Proposition 1.40. *Let L/K be a cyclic extension of degree p^s and let $\mathfrak{p}$ be a prime ideal of K. Denote by e the ramification index of $\mathfrak{p}$ in L/K and by e_0 the ramification index of $\mathfrak{p}$ in K. Then*

$$v_{\mathfrak{p}}(\operatorname{disc} L/K) \leq \frac{p^s}{e}(e - 1 + e \cdot e_0 \cdot s).$$

Proof. Let $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ be a prime ideal of L lying over $\mathfrak{p}$ and let $\mathcal{D}_{L/K}$ the different of L/K. Since the extension L/K is normal, the valuation of $\mathcal{D}_{L/K}$ at $\mathfrak{q}_i$ is the same for all for all $i = 1, \dots, r$; we denote it by d. We write $\mathcal{D}_{L/K} = J \prod_{i=1}^r \mathfrak{q}_i^d$ with J coprime to $\mathfrak{q}_i$ for all $i = 1, \dots, r$. Then $\operatorname{disc} L/K = N_{L/K}(\mathcal{D}_{L/K}) = N_{L/K}(J) \prod_{i=1}^r N_{L/K}(\mathfrak{q}_i)^d$. Let f be the inertia degree of any of the $\mathfrak{q}_i$ over $\mathfrak{p}$. Then the norm $N_{L/K}(\mathfrak{q}_i)$ is equal to $\mathfrak{p}^f$ and therefore $v_{\mathfrak{p}}(\operatorname{disc} L/K) = frd$. To get the result, it is enough to use [60, Chapter III, Proposition 13], that gives the bound $d \leq e - 1 + e \cdot e_0 \cdot s$ and notice that $fr = \frac{p^s}{e}$.

Using the fact that $e \leq p^s$, we get the following bound from Lemma 1.38:

Theorem 1.41. *Let L/K be a cyclic extension of degree p^s with conductor $\mathfrak{f}$. Let $\mathfrak{p}$ be a prime ideal of K lying over p and let e_0 be the ramification index of $\mathfrak{p}$ over $\mathbf{Q}$. Then*

$$v_{\mathfrak{p}}(\mathfrak{f}) \leq \frac{p}{p-1}(1 + se_0). \tag{1.4}$$

Ramification groups and conductor

Apart from the constraints coming from the analysis of the discriminant, the structure of the Galois group of L/K yields more directly a bound on the valuation of the conductor of L/K at $\mathfrak{p}$, exploiting the relation between ramification groups and class field theory given by Theorem 1.19. In particular, any bound on the largest index for which the upper numbering ramification group is non-zero will immediately translate into a bound on the valuation of the conductor. Let $\mathfrak{q}$ be a prime ideal of K and let $\mathfrak{p}$ be a prime ideal of L lying over $\mathfrak{q}$. Let $G_{\mathfrak{p}}$ be the decomposition group of $\mathfrak{p}$ in L/K and let $G_{\mathfrak{p}} = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{e\}$ be the filtration of $G_{\mathfrak{p}}$ given by the lower index ramification groups. The first step is to give a bound on the last non-zero G_i. In the following, π will always be a uniformizer of $\mathfrak{p}$ and e will be the absolute ramification index of $\mathfrak{p}$, i.e. $e = v_{\mathfrak{p}}(p)$ where p is the prime number underneath $\mathfrak{p}$. The statements of the following lemmas are taken from the exercises of [60, Chapter IV, §2].

Lemma 1.42. *Let $\sigma \in G_i$ be an element of the i-th ramification group with $i \geq 1$ and let $a \in \mathfrak{p}^i$ be the element such that $\sigma(\pi) = \pi(1+a)$. If $x \in \mathfrak{p}^j$ and $i > \frac{e}{p-1}$, then $\sigma^p(x) - x \equiv pjax \pmod{\mathfrak{p}^{i+j+e+1}}$.*

Proof. First, we show that $\sigma(x) - x = jax \pmod{\mathfrak{p}^{i+j+1}}$. Write $x = \pi^j u$ for some u; then $\sigma(x) = \sigma(\pi)^j \sigma(u) = \pi^j (1+a)^j \sigma(u)$. Reducing this modulo $\mathfrak{p}^{i+j+1}$, we get

$$\sigma(x) \equiv x(1+a)^j \frac{\sigma(u)}{u} \pmod{\mathfrak{p}^{i+j+1}}$$

The claim is then equivalent to show that $(1+a)^j \frac{\sigma(u)}{u} \equiv 1 + ja \pmod{\mathfrak{p}^{i+1}}$ Since $\sigma \in G_i$, $\frac{\sigma(u)}{u} \equiv 1 \pmod{\mathfrak{p}^{i+1}}$ and, by the binomial formula, $(1+a)^j \equiv 1 + ja \pmod{\mathfrak{p}^{i+1}}$. Therefore we proved that $\sigma(x) - x = jax \pmod{\mathfrak{p}^{i+j+1}}$.

Now, we prove that $\sigma^p(x) - x \equiv pjax \pmod{\mathfrak{p}^{i+j+e+1}}$. First, we prove the following polynomial identity:

$$y^p - 1 = p(y-1) + pq(y)(y-1)^2 + (y-1)^p$$

In order to prove this, we use the binomial formula:

$$\begin{aligned} y^p - 1 &= ((y-1)+1)^p - 1 \\ &= -1 + \sum_{i=0}^{p} \binom{p}{i} (y-1)^i \\ &= p(y-1) + (y-1)^p + pq(y)(y-1)^2 \end{aligned}$$

for some polynomial $q(y) \in \mathbf{Z}[y]$. Since σ and the identity homomorphism commute, the same identity holds for σ:

$$(\sigma^p - \mathrm{id})(x) = p(\sigma - \mathrm{id})(x) + (\sigma - \mathrm{id})^p(x) + pq(\sigma)(\sigma - \mathrm{id})^2(x)$$

Notice that, if b is an element of valuation l, then $(\sigma - \mathrm{id})(b)$ has valuation at least $i + l$ by what we proved before. This means that the valuation of $(\sigma - \mathrm{id})^p(x)$ is at least $pi + j$. As $i > \frac{e}{p-1}$ by hypothesis, $pi + j \geq i + j + e + 1$, proving that $(\sigma - \mathrm{id})^p(x) \equiv 0 \pmod{\mathfrak{p}^{i+j+e+1}}$. The same holds for $pq(\sigma)(\sigma - \mathrm{id})^2(x)$, as the valuation of $(\sigma - \mathrm{id})^2(x)$ is at least $2i + j$ and therefore the valuation of $pq(\sigma)(\sigma - \mathrm{id})^2(x)$ is lower bounded by $2i + j + e > i + j + e + 1$. Summarizing, we have

$$(\sigma^p - \mathrm{id})(x) \equiv p(\sigma - \mathrm{id})(x) \pmod{\mathfrak{p}^{i+j+e+1}}$$

which proves the lemma.

Lemma 1.43. *Let p be the prime number underneath $\mathfrak{p}$. If $i > \frac{e}{p-1}$, then G_i is trivial.*

Proof. Assume by contradiction that G_i is not trivial. Then there exists an index $s \geq i$ such that G_s is non trivial and G_{s+1} is trivial. Let $\sigma \in G_s \setminus G_{s+1}$ and let π be a uniformizer of $\mathfrak{p}$. Write $\sigma(\pi) = \pi(1 + a)$ for some $a \in \mathfrak{p}^s \setminus \mathfrak{p}^{s+1}$. We show that $\sigma^p \in G_{s+e} \setminus G_{s+e+1}$. By Lemma 1.42, we know that $\sigma^p(\pi) = \pi(1 + pa) \pmod{\mathfrak{p}^{s+e+2}}$. As $v(pa) = e + s$, $\sigma^p \notin G_{s+e+1}$. However, by hypothesis s was the index of the last non trivial group and $s + e + 1 > s$, giving a contradition. This means that G_i must be trivial, as claimed.

Now that we have a bound for the last non-zero lower numbering ramification group G_i, we translate it into a bound on the exponent v of the last non-zero upper numbering ramification group G^v. Recall that the upper ramification groups and the lower ramification groups are related by definition via the function

$$\varphi(u) = \int_0^u \frac{1}{[G_0 \colon G_t]} dt$$

and, precisely, $G^{\varphi(u)} = G_u$.

Theorem 1.44. *Let L/K be a cyclic extension of degree $m = p^s$ and let $\mathfrak{p}$ be a prime ideal of K lying over p. Denote by e_0 the ramification index of $\mathfrak{p}$. Then $v_{\mathfrak{p}}(\mathfrak{f}(L/K)) \leq \lfloor \frac{e_0 p^s}{p-1} \rfloor - \sum_{i=2}^s p^{i-1} + s$.*

Proof. First, we aim at upper bounding the last non-zero upper numbering ramification group G^v. By means of Lemma 1.43 and by definition of the upper numbering ramification groups, it is bounded by

$$\varphi\Big(\Big\lfloor \frac{e}{p-1} \Big\rfloor\Big) = \int_0^{\lfloor \frac{e}{p-1} \rfloor} \frac{1}{[G_0 \colon G_t]} dt \tag{1.5}$$

where e is the absolute ramification index of $\mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal of L lying over $\mathfrak{p}$. As φ is piecewise constant, we can rewrite the integral in (1.5) as

$$\varphi\Big(\Big\lfloor\frac{e}{p-1}\Big\rfloor\Big) = \sum_{i=1}^{\lfloor\frac{e}{p-1}\rfloor}\frac{|G_i|}{|G_0|}$$

Let $w_1, \dots, w_t \in \mathbf{N}$ be the indices such that $G_i \neq G_{i+1}$. Defining $w_0 = 0$, we can rewrite the sum as

$$\sum_{i=1}^{\lfloor\frac{e}{p-1}\rfloor}\frac{|G_i|}{|G_0|} = \sum_{i=1}^{t}(w_i - w_{i-1})\frac{|G_{w_i}|}{|G_0|}$$

As the extension is cyclic and we selected the jumps in the filtration, we know that $\frac{|G_{w_i}|}{|G_0|} = \frac{1}{p^{i-1}}$ and so

$$\varphi\Big(\Big\lfloor\frac{e}{p-1}\Big\rfloor\Big) = \sum_{i=0}^{t}\frac{1}{p^{i-1}}(w_i - w_{i-1})$$

In order to have information on the differences $w_{i+1} - w_i$ we use the Hasse-Arf Theorem 1.9 to deduce that $w_{i+1} - w_i$ must be divisible by p^{i-1}. Denoting by $q_i \in \mathbf{N}$ the quotient of $w_{i+1} - w_i$ and p^i, we get

$$\varphi\Big(\Big\lfloor\frac{e}{p-1}\Big\rfloor\Big) = \sum_{i=1}^{t} q_i$$

Summarizing, we want an upper bound for this sum, with the constraints $t \leq s$, $q_i > 0$ for all i, $\sum_{i=1}^{t} p^{i-1}q_i \leq \frac{e}{p-1}$. The maximum of the expression is clearly attained when $t = s$, $q_i = 1$ for $i = 2, \dots, s$ and $q_1 = \lfloor\frac{e}{p-1}\rfloor - \sum_{i=2}^{s} p^{i-1}$. The result follows by summing the solutions $q_1, \dots, q_s$ and by Theorem 1.19.

Example 1.45. Let K be the biquadratic field generated by $\sqrt{2}$ and $\sqrt{3}$ and suppose we want to bound the valuation of the conductor of a cyclic extension of degree 2^n at the prime ideal lying over 2 (2 is totally ramified).

Theorem 1.44 tells us that the valuation is bounded by $2^{n+2} - \sum_{i=2}^{n} 2^{i-1} + n$, while Theorem 1.41 gives us $2(1+4n)$ as a bound. Since $\sum_{i=2}^{n} 2^{i-1} = 2^n - 2$, we can rewrite the first bound as $3 \cdot 2^n + n + 2$ (for $n \geq 2$). It is then clear that asymptotically the bound provided by Theorem 1.41 is better. However, for small values of n this is not the case.

n	Theorem 1.44	Theorem 1.41
1	9	10
2	16	18
3	29	26

This example shows that we need both bounds for our computation: depending on the structure of the extension we are searching for and the ramification index of the prime ideals, one of the two bounds might be unpredictably better than the other.

1.5 Computation of a defining polynomial

In this section, we deal with the problem of computing defining polynomials for an abelian extension L/K given as a congruence subgroup $A_{\mathfrak{f}}$ of a ray class group $\mathrm{Cl}_{\mathfrak{f}}$, following the exposition of [26]. More precisely, we aim at finding polynomials $f_1(x_1), \dots, f_s(x_s) \in K[x_1, \dots, x_s]$ such that $L = K[x_1, \dots, x_s]/(f_1(x_1), \dots, f_s(x_s))$. In the literature there are mainly two methods, based on either Hecke's theorem or the Artin map. The algorithm based on Hecke's theorem can be found in [15, Section 5.5.5], while here we follow the Artin map approach. We will split the discussion into three parts:

- computation of a Kummer generator over a cyclotomic extension;
- reduction of the size of the Kummer generator;
- descent to K.

Reduction to the prime power case Using the elementary divisor theorem, we may decompose $\mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \cong \mathrm{Gal}(L/K)$ into a product of cyclic groups of prime power order. Accordingly, L/K is the compositum of linearly disjoint cyclic extensions of K of prime power degree. Thus, from now on we assume that $\mathrm{Gal}(L/K) \cong \mathbf{Z}/p^m\mathbf{Z}$ is a cyclic extension of prime power degree $n = p^m$ for some prime p.

1.5.1 Computation of a Kummer generator

The algorithm relies heavily on the properties of Kummer extensions: the first step of the algorithm is to reduce to the case of a field containing the roots of unity. Thus, we study the translation F of L over $K(\zeta_n)$; more precisely, we consider the fields $E = K(\zeta_n)$ and $F = LE = L(\zeta_n)$ and F/E is again an abelian extension.

$$\begin{tikzcd}
& L(\zeta_n) = F \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & K(\zeta_n) = E \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

Since $N_{E/K}(P_{\mathfrak{f}\mathcal{O}_E}) \subseteq P_{\mathfrak{f}}$, we know that the lift $\mathfrak{f}_E = \mathfrak{f}\mathcal{O}_E$ is an admissible modulus for the abelian extension F/E by [36, Chapter III, Section 3]. The aim of this part of the algorithm is to find a defining equation for the field extension F/E, which is now a Kummer extension.

Computation of the S-units The first step is to compute a Kummer extension of E which contains the target field F.

Lemma 1.46. *Let E be a field containing the n-th roots of unity and let F/E be a cyclic extension of degree n with admissible modulus $\mathfrak{f}_E$. Let S be a finite set of places of E containing*

1. *all places dividing $\mathfrak{f}_E$,*
2. *primes generating $\mathrm{Cl}_E/\mathrm{Cl}_E^n$,*
3. *the infinite primes.*

Consider the group U_S of S-units of E. Then $F \subseteq N = E(\sqrt[n]{U_S})$.

Proof. See [15, Propositon 5.4.4].

Let S be the set of places as in the lemma. By Dirichlet's unit theorem [36, Chapter V, Theorem 8.2], the group of S-units is isomorphic to $\mu_E \times \mathbf{Z}^{\#S-1}$. Let $\zeta \in U_E$ be a torsion unit with $\langle\zeta\rangle = \mu_E$. Denoting $r = \#S$, we can compute r elements such that $\zeta = \varepsilon_1, \dots, \varepsilon_r$ generates U_S as in [15, Algorithm 7.4.8] or using other techniques coming from the analysis of the Galois group of E as in [8]. Since F/E is a cyclic subextension of $N/E = E(\sqrt[n]{U_S})/E$, Kummer theory asserts that there exists an element $\alpha = \varepsilon_1^{n_1}\varepsilon_2^{n_2}\cdots\varepsilon_r^{n_r}$ such that $F = E(\sqrt[n]{\alpha})$. Our aim is to determine such an element $\alpha \in U_S$ or, equivalently, suitable exponents $n_1, \dots, n_r \in \mathbf{Z}$.

Computation of a generator The method to find a suitable α relies on the restriction homomorphism between normal extensions. Precisely, in order to identify F as a subextension of N/E, we aim at describing $\mathrm{Gal}(N/F)$ as a subgroup of $\mathrm{Gal}(N/E)$, and for this purpose we realize $\mathrm{Gal}(N/F)$ as the kernel of the composition of the restriction maps $\mathrm{res}\colon \mathrm{Gal}(N/E) \to \mathrm{Gal}(F/E)$ and $\mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K)$. Lemma 1.23 tells us that the latter can be seen as the composition of the inverse of Artin map of N/E, the norm and the Artin map for L/K. Thus, we aim at constructing this composition effectively in order to retrieve F.

Explicitly, given an element $\sigma \in \mathrm{Gal}(N/E)$, we can find a prime ideal $\mathfrak{p}$ of E such that $\mathrm{Frob}_{\mathfrak{p},N/E} = \sigma$. The restriction res maps then $\mathrm{Frob}_{\mathfrak{p},N/E}$ to $\mathrm{Frob}_{\mathfrak{p},F/E}$ ([36, Chapter III, Property 2.4]). The application of the norm map to $\mathrm{Frob}_{\mathfrak{p},F/E}$ gives the Frobenius automorphism $\mathrm{Frob}_{N_{E/K}(\mathfrak{p}),L/K}$ (as $N_{E/K}(\mathfrak{p})$ might not be prime, we are considering the extension of the Frobenius automorphism to non-prime ideals by multiplicativity), which corresponds to the element $[N_{E/K}(\mathfrak{p})] \in \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}}$. In total, the map sends the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p},N/E}$ of a prime ideal $\mathfrak{p}$ of E to the class $[N_{E/K}(\mathfrak{p})] \in \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}}$. The situation is illustrated by the following diagram, where $\mathfrak{f}_N$ is an admissible modulus for N/E and $A_{\mathfrak{f}_N} < \mathrm{Cl}_{\mathfrak{f}_N}$ is the ideal class corresponding to F/E and we use Φ to denote the Artin map (the subscript clarifies the extension we are considering).

$$\begin{tikzcd}
\mathrm{Gal}(L/K) & \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \arrow[l, "\Phi_{L/K}"'] & \mathrm{Cl}_{\mathfrak{f}_N}/A_{\mathfrak{f}_N} \arrow[l, "N_{E/K}"'] \arrow[r, "\Phi_{F/E}"] & \mathrm{Gal}(F/E) & \mathrm{Gal}(N/E) \arrow[l, "\mathrm{res}"']
\end{tikzcd}$$

Since $N = E(\sqrt[n]{U_S}) = E(\sqrt[n]{\varepsilon_1}, \dots, \sqrt[n]{\varepsilon_r})$, we realize the Galois group $\mathrm{Gal}(N/E)$ as $(\mathbf{Z}/n\mathbf{Z})^r$ via

$$\begin{aligned}\Psi\colon\ \mathrm{Gal}(N/E) &\longrightarrow \quad (\mathbf{Z}/n\mathbf{Z})^r\\ \sigma \quad &\longmapsto (\overline{m}_1,\dots,\overline{m}_r)\end{aligned}$$

where $\sigma(\sqrt[n]{\varepsilon_i}) = \zeta_n^{m_i}\cdot\sqrt[n]{\varepsilon_i}$ for $1\le i\le r$. As our aim is to compute F, we can only aim at realizing this map via computing the Frobenius automorphism of prime ideals of E. Notice that computing a prime $\mathfrak{p}$ such that $\mathrm{Frob}_{\mathfrak{p},N/E} = \sigma$ is difficult; this is the reason why we do not consider the generators of $\mathrm{Gal}(N/E)$ corresponding to the canonical basis of $(\mathbf{Z}/n\mathbf{Z})^r$. Thus we set up the map between $(\mathbf{Z}/n\mathbf{Z})^r \simeq \mathrm{Gal}(N/E)$ and $\mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}}$ by computing a set of prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ such that $\mathrm{Frob}_{\mathfrak{p}_1,N/E},\dots,\mathrm{Frob}_{\mathfrak{p}_r,N/E}$ generate $\mathrm{Gal}(N/E)$ and mapping them to $\mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}}$. We can then compute the kernel of the map which corresponds to $\mathrm{Gal}(N/F)$ and compute F as the fixed field. In particular, if M is the matrix whose columns are a basis of the kernel in $(\mathbf{Z}/n\mathbf{Z})^r$, the exponents $n_1,\dots,n_r$ can be found by computing the left kernel of M.

Algorithm 6 Computation of a Kummer generator

```
Input: A cyclic extension $L/K$ of prime power degree $n$ given by an ideal
    class $A_{\mathfrak{f}} < \mathrm{Cl}_{\mathfrak{f}}$.
Output: An element $\alpha \in K(\zeta_n) = E$ such that $L(\zeta_n) = E(\sqrt[n]{\alpha})$.

 1. Compute a suitable set of places $S$ of $E$ as in Lemma 1.46.
 2. Compute generators $\varepsilon_1,\dots,\varepsilon_r$ for the $S$-units.
 3. Set $N = K(\zeta_n)(\sqrt[n]{\varepsilon_1},\dots,\sqrt[n]{\varepsilon_r})$.
 4. Find prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ of $K(\zeta_n)$ such that $\mathrm{Frob}_{\mathfrak{p}_1,N/E},\dots,\mathrm{Frob}_{\mathfrak{p}_r,N/E}$
    generate $\mathrm{Gal}(N/E)$.
 5. Compute the ideals $\mathfrak{I}_1 = N(\mathfrak{p}_1),\dots,\mathfrak{I}_r = N(\mathfrak{p}_r)$.
 6. Compute the classes $[I_1],\dots,[I_r]$ in $\mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}}$.
 7. Define the map $\vartheta\colon\ \mathrm{Gal}(N/E)\to\mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}}$ by sending $\mathrm{Frob}_{\mathfrak{p}_i,N/E}$ to $[I_i]$.
 8. Compute the kernel $\mathrm{Gal}(N/F)$ of $\vartheta$ as a subspace of $(\mathbf{Z}/n\mathbf{Z})^r$.
 9. Let $M$ be the matrix over $\mathbf{Z}/n\mathbf{Z}$ whose rows correspond to a set of gen-
    erators of $\mathrm{Gal}(N/F)$.
10. Compute the generator $(n_1,\dots,n_r)\in(\mathbf{Z}/n\mathbf{Z})^r$ of the kernel of $M$ over
    $\mathbf{Z}/n\mathbf{Z}$.
11. Return $\prod_{i=1}^r \varepsilon_i^{n_i}$.
```

Remark 1.47. As in [24, Section 3], given a Kummer extension $E(\sqrt[n]{\alpha})$ and a prime ideal $\mathfrak{p}$ of E, we can efficiently find $k\in\mathbf{Z}$ with $\mathrm{Frob}_{\mathfrak{p},E(\sqrt[n]{\alpha})/E}(\sqrt[n]{\alpha}) = \zeta_n^k\sqrt[n]{\alpha}$ doing only computations in K. This is crucial for Step (4): we do not explicitly need to compute N.

1.5.2 Reduction of the generator

The Kummer generator we find in the first step of the algorithm might be larger than necessary. Depending on the situation, it is either the final result or this computation is followed by the descent: this causes the defining polynomial that we compute to be far from optimal. In particular, any further computation on the resulting field might be infeasible. To improve the overall performance, it is beneficial to find a "small" generator for the Kummer extension. Thus, we will now deal with the following task: given a non-zero element α in a number field K, we want to find a "small" representative for $\alpha \cdot K^{\times n}$, that is, we want to find $\beta \in K^\times$ such that $\beta^n \cdot \alpha$ is "small". To this end, we will describe how to compute a so called compact representation

$$\alpha = \prod_{i=0}^{l} \alpha_i^{n^i}$$

with small elements $\alpha_i \in \mathcal{O}_K$. Once we have found this, α_0 will be a small representative in the coset of α modulo $K^{\times n}$. Note that the notion of compact representations was used in [64] in connection with the computation of units and principal ideal generators. As the value of the presented algorithms comes from the practicality, we will refrain from giving precise statements about the size of the objects.

The first step of a compact representation is a reduction at the finite places. We let $(\alpha) = \prod_{i=1}^{l} \mathfrak{p}_i^{n_i}$ be the prime ideal factorization of (α) and set $N = \max_i n_i$. Given two numbers $a \in \mathbf{Z}$, $b \in \mathbf{N}$, we write $a \bmod b$ for the unique positive remainder of the division of a by b.

Remark 1.48. In our application, we already know a small set of primes containing the support of α: the set S we used in the construction of the primitive element for the Kummer extension. Thus computing the factorization reduces to the problem of finding the valuation of α at some prime ideals. In general, finding the factorization of (α) might be expensive: we can relax the hypothesis and consider a partial factorization $\alpha\mathcal{O}_K = \prod_{i=1}^{l} I_i^{n_i}$ where the I_i are pairwise coprime.

Algorithm 7 Reduction at finite places

```
Input: An element $\alpha \in \mathcal{O}_K$ with a factorization $\alpha\mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{p}_i^{n_i}$, $k = \lfloor \log_n(N) \rfloor$
Output: Returns small elements $\alpha_0, \dots, \alpha_k$ and $\mathfrak{a}_0$ of small norm with
    $$(\alpha) = \left( \prod_{i=1}^{k} (\alpha_i)^{n^i} \right) \cdot \mathfrak{a}_0.$$
1. Define $\mathfrak{a}_{k+1} = 1$
2. For $j = k, \dots, 0$,
    a) Define $\mathfrak{b}_j = \prod_{i=1}^{l} \mathfrak{p}_i^{\left\lfloor \frac{n_i \bmod n^{j+1}}{n^j} \right\rfloor}$.
    b) Find $\alpha_j \in (\mathfrak{a}_{j+1}^n \mathfrak{b}_j)^{-1}$ such that the ideal $\mathfrak{a}_j := \alpha_j^{-1} \mathfrak{a}_{j+1}^n \mathfrak{b}_j$ has small norm.
3. Return $\alpha_0, \ldots, \alpha_k$ and $\mathfrak{a}_0$.
```

Remark 1.49. The ideal $\mathfrak{b}_j$ of Step ($2a$) is not computed explicitly but handled as a power product of ideals, as it is in general too large.

Proposition 1.50 ([26]). *Algorithm 7 is correct.*

Proof. Since $\mathfrak{b}_k = \alpha_k \mathfrak{a}_k$ we have $\mathfrak{b}_k^n = \alpha_k^n \mathfrak{a}_k^n$ and therefore $\mathfrak{b}_k^n \mathfrak{b}_{k-1} = \alpha_k^n \mathfrak{a}_k^n \mathfrak{b}_{k-1} = \alpha_k^n \alpha_{k-1} \mathfrak{a}_{k-1}$. Inductively this yields the result since

$$\sum_{j=0}^{k} \left\lfloor \frac{n_i \bmod n^{j+1}}{n^j} \right\rfloor \cdot n^j = n_i$$

and hence

$$\mathfrak{a} = \prod_{i=0}^{k} \mathfrak{b}_i^{n^i}.$$

Remark 1.51. Finding α_j in Step (2b) is the well known problem of finding small representative in ideal classes. The solution involves computing a small basis of the inverse ideal using a lattice reduction. In case one uses LLL reduction, the ideals $\mathfrak{a}_j$ will have a small norm bounded by $O(2^{d^2}\sqrt{|\operatorname{disc} K|})$.

We now assume that we have an element $\alpha \in \mathcal{O}_K$ such that $|N(\alpha)|$ is small and for which we want to compute a compact representation. To do so, we need the following notion. Let $\mathfrak{b}$ be a non-zero integral ideal of $\mathcal{O}_K$. We define

$$\lfloor \sqrt[n]{\mathfrak{b}} \rfloor = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(\mathfrak{b})}{n} \rfloor},$$

to be the n-th root of $\mathfrak{b}$. Here the product runs over all non-zero prime ideals of $\mathcal{O}_K$. Note that $\lfloor \sqrt[n]{\mathfrak{b}} \rfloor$ is an integral ideal such that $(\sqrt[n]{\mathfrak{b}})^n$ divides $\mathfrak{b}$.

Let $\sigma_1, \ldots, \sigma_d \colon K \to \mathbf{C}$ be the complex embeddings of K.

Algorithm 8 Compact representation for elements of small norm

```
Input: $\alpha \in \mathcal{O}_K$ with $|N(\alpha)|$ small.
Output: Small elements $\alpha_0, \ldots, \alpha_l$ such that $\alpha = \prod_{i=1}^k \alpha_i^{n^i}$.

1. Set $v = (v_j)_{1 \le j \le d} = (\log(|\sigma_j(\alpha)|))_{1 \le j \le d} \in \mathbf{R}^d$
2. Set $k = \lfloor \log_n(\|v\|_\infty) \rfloor$ so that $n^k \le \|v\|_\infty \le n^{k+1}$.
3. Set $\tilde{\alpha}_{k+1} = \alpha$.
4. For $i = k, \ldots, 1$,
    • Set $w = (\exp(n^{-i} v_j))_{1 \le j \le d}$
    • Compute $\mathfrak{b}_i = \lfloor \sqrt[n^i]{\tilde{\alpha}_{i+1} \mathcal{O}_K} \rfloor$.
```

- Compute a $T_{2,w}$-small element $\gamma_i \in \mathfrak{b}_i^{-1}$.
- Set $\alpha_i = \gamma_i^{-n^i}$ and $\tilde{\alpha}_i = \tilde{\alpha}_{i+1} \cdot \gamma_i^{n^i}$.

5. Define $\alpha_0 = \tilde{\alpha}_1$ and return $\alpha_0, \dots, \alpha_k$.

Proposition 1.52 ([26]). *Algorithm 8 is correct.*

Proof. Note that by construction we have $\tilde{\alpha}_{k-1} = \tilde{\alpha}_k \gamma_{k-1}^{n^{k-1}} = \alpha\gamma_k^{n^k}\gamma_{k-1}^{n^{k-1}}$ and inductively

$$\tilde{\alpha}_1 = \alpha \prod_{i=1}^{k} \gamma_i^{n^i}.$$

Remark 1.53. The size of the output $\gamma_1, \dots, \gamma_k$ of the algorithm is bounded in T_2-norm in terms of n and $\sqrt{|\operatorname{disc} K|}$. Assume that we are in the i-th iteration of the algorithm; in the same notations as above, the element $\gamma_i \in \mathfrak{b}_i^{-1}$ obtained by the LLL-algorithm has small $T_{2,w}$-norm:

$$T_{2,w}(\gamma_i) \leq C\big(|\operatorname{disc} K|^{\frac{1}{2}} N(\mathfrak{b}_i)^{-1} \prod_j w_j\big)^{\frac{2}{d}} \leq C\big(|\operatorname{disc} K|^{\frac{1}{2}} N(\alpha)^{\frac{1}{n^i}}\big)^{\frac{2}{d}}$$

where C is the explicit constant for the reduction algorithm and the last inequality comes from the fact that $(N(\mathfrak{b}_i)^{-1}\prod_j w_j)^{n^i} = N(\alpha)N(\mathfrak{b}_i)^{-n^i}$ is integral, hence bounded by $N(\alpha)$. Clearly, $\alpha\gamma_i^{n^i} \in \mathcal{O}_K$ and we have the following bound on its size:

$$\begin{aligned} T_2(\alpha\gamma_i^{n^i}) &= \sum_s \Big(w_s^{-2n^i}|\sigma_s(\alpha)|^2\Big)\Big(w_s^{2n^i}|\sigma_s(\gamma_i^{n^i})|^2\Big) \\ &= \sum_s w_s^{2n^i}|\sigma_s(\gamma_i^{n^i})^2| \leq \Big(\sum_s w_s^2|\sigma_s(\gamma_i)|^2\Big)^{n^i} \\ &= T_{2,w}(\gamma_i)^{n^i} \leq C^{n^i} N(\alpha)^{\frac{2}{d}} |\operatorname{disc} K|^{\frac{n^i}{d}} \end{aligned}$$

Thus

$$\|v\|_\infty = \log\|\alpha\gamma_i^{n^i}\|_\infty \leq \log T_2(\alpha\gamma_i^{n^i}) \leq n^i \log\big(CN(\alpha)^{2/d}|\operatorname{disc} K|^{1/d}\big)$$

Now, $w_i^{-1} = \exp(-n^{-i}v_i) \leq \exp(n^{-i}\|v\|_\infty) \leq CN(\alpha)^{2/l}|\operatorname{disc} K|^{1/d}$ and

$$\begin{aligned} T_2(\gamma_i) &= \sum_s w_s^{-2} w_s^2 |\sigma_s(\gamma_i)|^2 \leq \|w^{-1}\|_2^2 T_{2,w}(\gamma_k) \\ &\leq dC^3|\operatorname{disc} K|^{3/d} N(\alpha)^{\frac{4}{d}+\frac{2}{dn^i}} \end{aligned}$$

is bounded as well.

We now summarize the algorithm to compute a compact presentation of an element:

Algorithm 9 Compact presentation

```
Input: An element $\alpha \in K$, $n \in \mathbf{N}$.
Output: A small element $\beta \in K$ such that $\alpha K^n = \beta K^n$.

1. Compute the support $\alpha \mathcal{O}_K = \prod_{i=1}^{l} \mathfrak{p}_i^{n_i}$.
2. Set $N = \max n_i$.
3. Apply Algorithm 7 to obtain $\alpha_0, \dots \alpha_k \in K$ such that
       $\tilde{\alpha} = \alpha \left( \prod_{i=0}^{k} \alpha_i^{-n^i} \right)$
4. Apply Algorithm 8 to $\tilde{\alpha}$, which yields $\tilde{\alpha}_0, \dots, \tilde{\alpha}_l$ with
       $\tilde{\alpha} = \prod_{i=0}^{k} \tilde{\alpha}_i^{n^i}.$
5. Return $\alpha_0 \tilde{\alpha}_0$.
```

1.5.3 Descent to L/K

The last step of the algorithm is the descent: given $\alpha \in E$ such that $F = E(\sqrt[n]{\alpha})$, we aim at finding a defining equation for L/K. In practice, we want to construct L as a subfield of F. In order to accomplish this, we find the subgroup $\mathrm{Gal}(F/L)$ of $\mathrm{Gal}(F/K)$, so that L will be the fixed field of this set of automorphisms.

First of all, we need a primitive element for F/K: the abelianity of F/K implies that the Kummer generator of F/E is a primitive element for F/K.

Lemma 1.54. *Let $F = E(\sqrt[n]{\alpha})$ be a cyclic Kummer extension of degree n of $K(\zeta_n)$. Assume that F/K is abelian. Let $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$ be the automorphism such that $\sigma(\zeta_n) = \zeta_n^i$. Then σ extends to an element $\tilde{\sigma} \in \mathrm{Gal}(F/K)$ such that $\tilde{\sigma}(\sqrt[n]{\alpha}) = c \sqrt[n]{\alpha}^i$ for an element $c \in E = K(\zeta_n)$.*

Proof. Denote by $\tau \in \mathrm{Gal}(F/K)$ the automorphism such that $\tau(\zeta_n) = \zeta_n$ and $\tau(\sqrt[n]{\alpha}) = \zeta_n \sqrt[n]{(\alpha)}$. Since F is a Kummer extension of E which is normal over K, there exist $c \in E$ and j coprime to n such that $\tilde{\sigma}(\sqrt[n]{\alpha}) = c \sqrt[n]{\alpha}^j$. As $\mathrm{Gal}(F/K)$ is abelian, τ and σ must commute:

$$\sigma(\tau(\sqrt[n]{\alpha})) = \sigma(\zeta_n \sqrt[n]{(\alpha)}) = \zeta_n^i c \sqrt[n]{\alpha}^j \tag{1.6}$$

$$\tau(\sigma(\sqrt[n]{\alpha})) = \tau(c \sqrt[n]{\alpha}^j) = c \zeta_n^j \sqrt[n]{\alpha}^j \tag{1.7}$$

and we must have $i = j$, as claimed.

Lemma 1.55. *Let $F = E(\sqrt[n]{\alpha})$ be a cyclic Kummer extension of degree n of $K(\zeta_n)$. If F/K is abelian, then $F = K(\sqrt[n]{\alpha})$.*

Proof. We want to show that the only automorphism of F/K fixing $\sqrt[n]{\alpha}$ is the identity. By the previous lemma, for every element $\sigma \in \mathrm{Gal}(F/K)$ there exist an element $c_\sigma \in E$ and an integer i_σ coprime to n such that $\sigma(\zeta_n) = \zeta_n^{i_\sigma}$ and $\sigma(\sqrt[n]{\alpha}) = c_\sigma \sqrt[n]{\alpha}^{i_\sigma}$. If $\sigma(\sqrt[n]{\alpha}) = \sqrt[n]{\alpha}$, then i_σ must be equal to 1, meaning that $\sigma(\zeta_n) = \zeta_n$, i.e. $\sigma \in \mathrm{Gal}(F/E)$. However, the only automorphism of F/E fixing $\sqrt[n]{\alpha}$ is the identity, as claimed.

Remark 1.56. Lemma 1.55 does not apply in the case the target extension L and $K(\zeta_n)$ are not disjoint over K. In this case, we need to test small linear combinations of $\sqrt[n]{\alpha}$ and ζ_n in order to get a primitive element.

We now focus on the computation of an explicit description of $\mathrm{Gal}(F/L)$ on $\sqrt[n]{\alpha}$ and ζ_n. Since F/K is the compositum of E and L, it is abelian with admissible modulus $\mathfrak{f}_F = n\mathcal{O}_K \cap \mathfrak{f}_N$. We have the following commutative diagram induced by the restriction homomorphism:

$$\begin{tikzcd}
\mathrm{Cl}_{\mathfrak{f}_F} \arrow[r, "\Phi_{F/K}"] \arrow[d] & \mathrm{Gal}(F/K) \arrow[d, "\mathrm{res}"] \\
\mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}} \arrow[r, "\Phi_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

Firstly, we compute generators for $\mathrm{Gal}(F/K)$. As $\mathrm{Gal}(E/K) = \mathrm{Gal}(K(\zeta_n)/K)$ is a subgroup of $(\mathbf{Z}/n\mathbf{Z})^\times$ and n is a prime power, we can find $r, s \in \mathbf{Z}$ such that $\mathrm{Gal}(E/K)$ is generated by $\zeta_n \mapsto \zeta_n^r$ and $\zeta_n \mapsto \zeta_n^s$ (if n is not a power of 2, the group is even cyclic). Using the characterization of Lemma 1.54, we determine extensions $f, g \colon F \to F$ of both morphisms by computing a n-th root, which together with $F \to F$, $\sqrt[n]{\alpha} \mapsto \zeta_n \sqrt[n]{\alpha}$ generate $\mathrm{Gal}(F/K)$.

The second step is to find $\mathrm{Gal}(F/L)$ as a subgroup of $\mathrm{Gal}(F/K)$. The idea is to create the map taking advantage of the properties of the Frobenius automorphisms. Specifically, if T is a set of prime ideals of K coprime to $\mathfrak{f}_F$ such that $(\mathrm{Frob}_{\mathfrak{q},F/K})_{\mathfrak{q}\in T}$ generate $\mathrm{Gal}(F/K)$, then we can establish a map $\mathrm{Gal}(F/K) \to \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}}$ by sending $\mathrm{Frob}_{\mathfrak{q},F/K}$ to $[\mathfrak{q}] \in \mathrm{Cl}_{\mathfrak{f}}/A_{\mathfrak{f}}$, whose kernel is $\mathrm{Gal}(F/L)$ by the diagram above. Thus, it only remains to show how to identify the automorphism of $\mathrm{Gal}(F/K)$ corresponding to the Frobenius automorphism of a given prime ideal $\mathfrak{q}$ of K. Let $\mathfrak{p}$ be a prime ideal of F lying over $\mathfrak{q}$. Then we can find $\mathrm{Frob}_{\mathfrak{p}}$ as the unique $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma(\zeta_n) \equiv \zeta_n^{N(\mathfrak{p})} \pmod{\mathfrak{p}}$ and $\sigma(\sqrt[n]{\alpha}) \equiv (\sqrt[n]{\alpha})^{N(\mathfrak{p})} \pmod{\mathfrak{p}}$.

Remark 1.57. If $n = \ell$ is prime, even less steps are necessary. Since $[K(\zeta_n) : K]$ is a divisor of $\ell - 1$, it is coprime to ℓ and thus $\mathrm{Gal}(F/L)$ is the unique subgroup of $\mathrm{Gal}(F/K)$ of order ℓ. If f is the lift of a generator of $\mathrm{Gal}(K(\zeta_n)/K)$ to $\mathrm{Gal}(F/K)$, then f^ℓ will be a generator of $\mathrm{Gal}(F/L)$.

Finally, we compute a primitive element for L. For simplicity, we now denote $\sqrt[n]{\alpha}$ by μ. We take advantage of the following lemma:

Lemma 1.58. *Let μ be the primitive element for an extension F/K and let L/K be a subextension. Let $f_{\mu,L}$ be the minimal polynomial of μ over L. If L/K is cyclic of prime power degree, then one of the coefficients of $f_{\mu,L}$ is a primitive element for L over K.*

Proof. See [15, Lemma 5.5.4].

We can easily compute the coefficients of $f_{\mu,L}$ by knowing the action of the elements of $\mathrm{Gal}(F/L)$ on μ, as

$$f_{\mu,L} = \prod_{\sigma\in\mathrm{Gal}(F/L)} (x - \sigma(\mu)) = \sum_{i=0}^{[F:L]} b_i x^i$$

Now, starting from $b_{[F:L]-1}$, we compute the minimal polynomials of the b_i (using again the automorphisms to compute the conjugates) until we find one which is has degree $[L : K]$.

Algorithm 10 Descent to K

```
Input: An abelian extension $L/K$ given by an ideal class $A_\mathfrak{f} < \mathrm{Cl}_\mathfrak{f}$, a Kummer
    generator $\mu$ for the extension $LK(\zeta_n)/K(\zeta_n) = F/K(\zeta_n)$.
Output: A polynomial $f \in K[x]$ such that $L = K[x]/(f)$.

1. Compute a set of generators for $\mathrm{Gal}(F/K)$.
2. Compute a set of primes $T$ of $K$ such that $(\mathrm{Frob}_{\mathfrak{q},F/K})_{\mathfrak{q}\in T}$ generate
   $\mathrm{Gal}(F/K)$.
3. Define the map $\pi\colon \mathrm{Gal}(F/K) \to \mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f}$ sending $\mathrm{Frob}_{\mathfrak{q},F/K}$ to $[\mathfrak{q}] \in$
   $\mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f}$.
4. Compute the kernel $\mathrm{Gal}(F/L)$ of $\pi$.
5. For $i = t-1, \dots, 0$,
    a) Compute the $i$-th coefficient $a$ of the minimal polynomial of $\mu$ over $L$.
    b) Compute the minimal polynomial $f_a \in K[x]$ of $a$.
    c) If $\deg f_a = [L : K]$, return $f_a$.
```

Remark 1.59. Experimentally, the bottleneck of the algorithm is the computation of the automorphisms of $\mathrm{Gal}(F/K)$, in particular the n-th roots necessary for the extension of the automorphisms of $\mathrm{Gal}(K(\zeta_n)/K)$.

CHAPTER 2

Normal abelian extensions

In this chapter, we deal with the task of computing abelian extensions of a field that are normal over a subfield: in other words, we focus on Step (5) of Algorithm 1.

Let K be a Galois extension of $\mathbf{Q}$ with Galois group G and suppose that we are searching for abelian extensions of K with Galois group over K isomorphic to A and absolute Galois group isomorphic to E up to an absolute discriminant bound B. We proceed as follows:

1. find a set F containing all possible conductors $\mathfrak{f}$;
2. for every conductor $\mathfrak{f} \in F$, compute the ray class group $\mathrm{Cl}_{\mathfrak{f}}$ and all subgroups $U \subseteq \mathrm{Cl}_{\mathfrak{f}}$ of conductor $\mathfrak{f}$ with $\mathrm{Cl}_{\mathfrak{f}}/U \cong A$;
3. given L an abelian extension of K corresponding to a pair $(\mathfrak{f}, U)$ of Step (2), if $\operatorname{disc} L \leq B$ and $\mathrm{Gal}(L/\mathbf{Q}) \simeq E$, compute a defining polynomial for L.

This strategy can be dramatically improved by using the additional hypothesis at our disposal, in particular the normality of the extension over $\mathbf{Q}$.

2.1 Galois action on ideal classes

The first task we want to solve is to characterise the ideal classes corresponding to abelian extensions of a given normal field that are themselves normal. Let K be a number field which is normal over some base field K_0 with Galois group $G = \mathrm{Gal}(K/K_0)$. The natural action of G on K extends to an action on the places of K. Precisely, given a place P and an element $\sigma \in G$, $\sigma(P)$ is the composition $P \circ \sigma^{-1}$. The action on the places of K extends naturally on the set of moduli of K. Let $\mathfrak{m}$ be a modulus which is stable under the action of G, that is, $\sigma(\mathfrak{m}) = \mathfrak{m}$ for every $\sigma \in G$. In this case G acts on the ray class group $\mathrm{Cl}_{\mathfrak{m}}$: given an ideal I coprime to $\mathfrak{m}$ and an element $\sigma \in G$, the image $\sigma([I])$ of the class $[I]$ under σ is $[\sigma(I)]$.

Lemma 2.1. *Let L be an abelian extension of K with conductor $\mathfrak{m}$ and let $\sigma\colon L \to \overline{\mathbf{Q}}$ be an embedding into the algebraic closure. Then $\sigma(\mathfrak{m})$ is the conductor of $\sigma(L)$ over $\sigma(K)$.*

Proof. Let $A_{\mathfrak{m}}$ be the congruence subgroup modulo $\mathfrak{m}$ corresponding to L. Then the Artin map $\Phi_{L/K}\colon \mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is an isomorphism. We now study the action of σ on the domain and the codomain of $\Phi_{L/K}$. Consider the map $\iota_\sigma\colon\ \mathrm{Gal}(L/K) \to \mathrm{Gal}(\sigma(L)/K)$ sending an element τ to $\sigma \circ \tau \circ \sigma^{-1}$. ι_σ is clearly an isomorphism. At the level of the ray class groups, σ induces the isomorphism $\tilde{\chi}_\sigma\colon \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_{\sigma(\mathfrak{m})}$ by sending $[I]$ to $[\sigma(I)]$. In particular, this induces an isomorphism $\chi_\sigma\colon \mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}} \to \mathrm{Cl}_{\sigma(\mathfrak{m})}/\tilde{\chi}_\sigma(A_{\mathfrak{m}})$. By the properties of the Frobenius automorphisms, it is easy to see that the composition $\iota_\sigma \circ \Phi_{L/K} \circ \chi_\sigma$ coincides with the Artin map $\Phi_{\sigma(L)/K}$. This proves that $\sigma(\mathfrak{m})$ is an admissible modulus for $\sigma(L)$. However, the same argument shows that if $\mathfrak{n}$ is an admissible modulus for $\sigma(L)$, then $\sigma^{-1}(\mathfrak{n})$ is an admissible modulus for L.

Proposition 2.2 ([26, Proposition 15]).

- *Let $\mathfrak{m}$ be modulus of K which is stable under the action of G. Every congruence subgroup H of $\mathrm{Cl}_{\mathfrak{m}}$ which is stable under the action of G corresponds to an abelian extension L/K such that L/K_0 is normal.*
- *Let L be an abelian extension of K which is normal over K_0. Then the conductor $\mathfrak{f}$ of L/K as well as the corresponding congruence subgroup are stable under the action of G.*

Proof. Firstly, we prove that if $\mathfrak{m}$ is a stable modulus, the statement is true for $H = \{e\}$ and the corresponding extension L. Let σ be an embedding of L into $\overline{\mathbf{Q}}$ such that $\sigma|_{K_0} = \mathrm{id}$. Then $\sigma(K) = K$ since K is normal over K_0 and $\sigma(L)$ is an abelian extension of K with admissible modulus $\sigma(\mathfrak{m})$. As $\sigma(\mathfrak{m}) = \mathfrak{m}$, we get $\sigma(L) \subseteq L$ and thus L/K_0 is normal.

Now, let H be a stable subgroup of $\mathrm{Cl}_{\mathfrak{m}}$ corresponding to an extension L and let F be the ray class field corresponding to $\{e\} < \mathrm{Cl}_{\mathfrak{m}}$. We want to show that L is normal over K_0, or, equivalently, that $\mathrm{Gal}(F/L)$ is normal in $\mathrm{Gal}(F/K_0)$. In this setting, we have the exact sequence

$$1 \to \mathrm{Gal}(F/K) \longrightarrow \mathrm{Gal}(F/K_0) \longrightarrow \mathrm{Gal}(K/K_0) \to 1$$

In particular, $\mathrm{Gal}(F/K_0)$ is generated by a set of generators of $\mathrm{Gal}(F/K)$ and preimages of generators of $\mathrm{Gal}(K/K_0)$. Obviously, $\mathrm{Gal}(F/L)$ is invariant under conjugation by elements of $\mathrm{Gal}(F/K)$ in $\mathrm{Gal}(F/K_0)$ since F/K is abelian. By the properties of the Artin map, $\mathrm{Cl}_{\mathfrak{m}} \simeq \mathrm{Gal}(F/K)$ and the action of G on $\mathrm{Cl}_{\mathfrak{m}}$ corresponds to conjugation in the group $\mathrm{Gal}(F/K_0)$. Since H is stable, this means that $\mathrm{Gal}(F/L)$ is invariant under conjugation by generators of $\mathrm{Gal}(K/K_0)$ and therefore it is a normal subgroup.

Conversely, let L be an abelian extension of K which is normal over K_0. The invariance of the conductor follows from the observation above. Furthermore, we know that the field L corresponding to $\{e\} < \mathrm{Cl}_{\mathfrak{f}}$ is normal over

K_0. Since L is normal, it correspond to a normal subgroup of $\mathrm{Gal}(F/K_0)$, so it is invariant under conjugation by elements of this group. By the properties of the Artin map, the action of $\mathrm{Gal}(K/K_0)$ on $\mathrm{Gal}(F/K)$ is given by the the conjugation in $\mathrm{Gal}(F/K_0)$. Since L is normal, the corresponding subgroup is stable.

Consequently, if we are searching for abelian extensions of K which are also normal over K_0, we can restrict to congruence subgroups that are invariant under the Galois action.

Conductor and discriminant of an ideal class

The first consequence of this characterization that we want to highlight is that we can compute the discriminant and the conductor of an abelian extension more efficiently. Indeed, by Proposition 2.2, the conductor of an abelian extension which is normal over K_0 is stable under the Galois action. This means that, if $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of $\mathcal{O}_K$ lying over the same prime ideal of $\mathcal{O}_{K_0}$, then the valuation of the finite part of the conductor $\mathfrak{f}$ of the congruence subgroup $A_\mathfrak{m} < \mathrm{Cl}_\mathfrak{m}$ at $\mathfrak{p}$ is the same as the one at $\mathfrak{q}$. Consequently, in order to compute the conductor of $A_\mathfrak{m}$, we just need to compute its valuation at one of the prime ideals lying over a prime of K_0, simplifying the algorithm. The same property holds for the infinite places and for the discriminant:

Lemma 2.3. *Let L/K be an abelian extension such that L/K_0 is normal. Then the discriminant of L/K is invariant under the action of* $\mathrm{Gal}(K/K_0)$*.*

Proof. Follows from [52, Chapter III, Theorem 2.5, Theorem 2.9].

Listing the conductors

Let K_0 be a number field and K be a normal extension of K_0 with Galois group G. Assume that we want to construct abelian extensions of K that are normal over K_0 up to an absolute discriminant bound B. In order to list the possible conductors, we follow the same strategy as in Section 1.4. However, by Proposition 2.2, we know that the conductor of such an extension must be invariant under the action of G. Consequently, if $\mathfrak{p}_0$ is a prime of K_0 and $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ are the prime ideals of K lying over $\mathfrak{p}_0$, their exponent in the factorization of the conductor must be the same.

2.2 Computing invariant subgroups

Let $\mathfrak{m}$ be a modulus of K invariant under the action of $\mathrm{Gal}(K/K_0)$ and let $\mathrm{Cl}_\mathfrak{m}$ be the ray class group modulo $\mathfrak{m}$. By Proposition 2.2, the abelian extensions of K that are normal over K_0 correspond to the subgroups that are stable under the action of $\mathrm{Gal}(K/K_0)$. We now illustrate an algorithm to find these subgroups. The problem of computing all the subgroups of an abelian group has been extensively studied. In particular, we could compute the set of all subgroups of M using a theorem of Butler [13]. However, it is important to find directly the invariant subgroups, as the following example shows.

Example 2.4. We consider the abelian group $M = (\mathbf{Z}/25\mathbf{Z})^{11}$ with the symmetric group $G = S_{11}$ acting via $\sigma(a_1, \dots, a_{11}) = (a_{\sigma(1)}, \dots, a_{\sigma(11)})$ for $\sigma \in S_{11}$ and $(a_1, \dots, a_{11}) \in (\mathbf{Z}/25\mathbf{Z})^{11}$. Then the number of subgroups of M with quotient isomorphic to $H = \mathbf{Z}/25\mathbf{Z}$ is 119209287109375, while only one of these subgroups is stable.

Denote by G the Galois group $\mathrm{Gal}(K/K_0)$. The action of G on $\mathrm{Cl}_{\mathfrak{m}}$ determines a structure of $\mathbf{Z}[G]$-module on $\mathrm{Cl}_{\mathfrak{m}}$. Denoted by n the exponent of $\mathrm{Cl}_{\mathfrak{m}}$ as an abelian group, $n\mathbf{Z}$ acts trivially on $\mathrm{Cl}_{\mathfrak{m}}$. Therefore, our task reduces to the problem of finding the $(\mathbf{Z}/n\mathbf{Z})[G]$-submodules of $\mathrm{Cl}_{\mathfrak{m}}$.

Computing the Galois action on ray class groups

We now explain how to compute efficiently the action of $\mathrm{Gal}(K/K_0)$ on $\mathrm{Cl}_{\mathfrak{m}}$, i.e. given $g \in G$ an automorphism of K, we want to compute the automorphism of the abelian group $\mathrm{Cl}_{\mathfrak{m}}$ induced by g.

The idea of the algorithm is straightforward: we take generators of $\mathrm{Cl}_{\mathfrak{m}}$, apply g on them and then write the images in terms of the generators.

Algorithm 11 Action of Galois group on ray class group

```
Input: A ray class group $\mathrm{Cl}_{\mathfrak{m}}$, an automorphism $g$ of $K$.
Output: An endomorphism of $\mathrm{Cl}_{\mathfrak{m}}$ representing the action of $g$.

1. Choose a set of generators $v_1, \dots, v_s$ of $\mathrm{Cl}_{\mathfrak{m}}$.
2. Compute ideals $I_1, \dots, I_s$ representing the classes $v_1, \dots, v_s$.
3. Compute $g(I_1), \dots, g(I_s)$.
4. Compute the classes $w_1, \dots, w_s$ of $g(I_1), \dots, g(I_s)$ in $\mathrm{Cl}_{\mathfrak{m}}$.
5. Return the homomorphism $\tilde{g}\colon \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{m}}$ sending $v_i$ to $w_i$ for $i = 1, \dots, s$.
```

The most expensive steps are the computation of $g(I_i)$ and of its class w_i in $\mathrm{Cl}_{\mathfrak{m}}$. The cost of these operations can be reduced if the generators are chosen wisely. Indeed, by Remark 1.27, the discrete logarithm is faster if it involves ideals that are known to be principal. This suggests that, if we can generate the ray class group with principal ideals, we could avoid the computation of the discrete logarithm of the ideals in the class group. Moreover, computing the image under g of a principal ideal I_i requires only the computation of the image of the principal generator. Unfortunately, this is possible only if the class group of the field is trivial:

Lemma 2.5. *Let K be a number field and let $\mathrm{Cl}_{\mathfrak{m}}$ be a ray class group over K. There exists principal ideals $I_1, \dots, I_s$ generating $\mathrm{Cl}_{\mathfrak{m}}$ if and only if the class number of K is 1.*

Proof. By Proposition 1.24, the natural map $\mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}$ is surjective. Therefore the image of any set of generators of $\mathrm{Cl}_{\mathfrak{m}}$ must generate the class group. The result follows from the observation that the kernel is generated by the principal ideals.

The idea is therefore to take as many principal ideals as possible and complete them to a set of generators of $\mathrm{Cl}_{\mathfrak{m}}$ with some small ideals generating the class group:

Lemma 2.6. *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_a$ be ideals generating the class group Cl and let $x_1, \dots, x_b \in \mathcal{O}_K$ be elements of the maximal order of K whose images generate the unit group of $\mathcal{O}_K/\mathfrak{m}$. Then the ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_a, (x_1), \dots, (x_b)$ generate the ray class group $\mathrm{Cl}_{\mathfrak{m}}$.*

Proof. Follows from Proposition 1.24.

Therefore, the strategy that we follow for the generators is the following:

- we pick lift of the generators for the multiplicative group for the x_i of the lemma;
- as generators for the class group, we take prime ideals lying over small prime numbers coprime to $\mathfrak{m}$ that generate the class group.

Remark 2.7. These elements have already been computed during Algorithm 3 and are needed in the conductor computation. Thus, they are essentially known and easy to use.

Example 2.8. Consider the number field $K = \mathbf{Q}(\sqrt{2})$ and the modulus $\mathfrak{m} = (5)\cdot(13)$ (notice that the prime numbers 13 and 5 are inert in K). The elements $\alpha = -150\sqrt{2}+1$ and $\beta = 78\sqrt{2}+79$ generate $(\mathcal{O}_K/\mathfrak{m})^\times$. Thus, since the class group of K is trivial, the ideals (α) and (β) span the whole ray class group $\mathrm{Cl}_{\mathfrak{m}}$, which is isomorphic to $C_2 \times C_{24}$. In particular, choosing these elements as generators, the corresponding relation matrix is

$$\begin{pmatrix} 6 & 6 \\ 0 & 8 \end{pmatrix}$$

The action of the generator σ of $\mathrm{Gal}(K/\mathbf{Q})$ on K sends the chosen generators to $\sigma(\alpha) = 150\sqrt{2} + 1$ and $\sigma(\beta) = -78\sqrt{2} + 79$. Computing their discrete logarithm in the unit group of $\mathcal{O}_K/\mathfrak{m}$ modulo the units, we can see that $[\sigma(\alpha)]$ corresponds to the element with coordinates $(1, 4)$ and $[\sigma(\beta)]$ to $(0, 5)$.

Enumerate the submodules

We now deal with the problem of finding the submodules of a $\mathbf{Z}/n\mathbf{Z}[G]$-module M. This task can be solved when n is a prime number using the Meataxe (see [55] and [34, Section 7.4]). We focus here on the non-prime case. We follow mainly the exposition of [26, Section 5].

The idea of the algorithm relies on the fact that every submodule of M is either irreducible or it contains an irreducible submodule. Thus, if we are able to find the irreducible submodules of M, we can find all the submodules by induction on the quotient.

Reduction to prime power order We can assume that the exponent n is a prime power: indeed, for every prime number q dividing the order of M, the q-Sylow subgroup M_q of M is invariant under the action of G and the decomposition as an abelian group $M = \sum M_q$ agrees with the structure of $\mathbf{Z}/n\mathbf{Z}[G]$-module. In particular, every irreducible $(\mathbf{Z}/n\mathbf{Z})[G]$-submodule of M must be contained in one of the Sylow subgroups of M. As the q-Sylow subgroup of M is naturally a $(\mathbf{Z}/q^{v_q(n)}\mathbf{Z})[G]$-module, we may assume that $n = p^s$ is a prime power.

Characterization of irreducible submodules Consider the subgroup N of M given by all the elements of order p, i.e. $N = \{m \in M \mid pm = 0\}$. This subgroup is invariant under the action of G and therefore it is a submodule; as all the elements have order p, it is a $\mathbf{F}_p[G]$-module. As we said before, we can compute the irreducible submodules of N by using the Meataxe algorithm. The following proposition shows that all the irreducible submodules of M are contained in N:

Proposition 2.9 ([26, Proposition 17]). *If M is an irreducible $(\mathbf{Z}/p^s\mathbf{Z})[G]$-module, then its exponent as an abelian group is p.*

Proof. Assume by contradiction that the exponent of M is a proper power of p, say p^l with $l \geq 2$. Then the subgroup $pM = \{pm \mid m \in M\}$ is a proper $(\mathbf{Z}/p^s\mathbf{Z})[G]$-submodule. Indeed, if $m \in pM$ and $g \in G$, we have $gm = gpn = pgn$ and so $gm \in pM$. This means that N is not irreducible, a contradiction.

Thus, to find the $(\mathbf{Z}/p^s\mathbf{Z})[G]$-submodules, we apply the method for the prime case and iterate. In particular, we have an algorithm to determine the G-invariant subgroups of an abelian group M.

The efficiency of the algorithm relies on the fact that we expect that the submodules of M will be only a few. In particular, one of the most critical part is the natural redundancy that this approach presents. Indeed, every submodule S_1 containing two different irreducible submodules S_2, S_3 is found during the algorithm at least twice, as a submodule of M/S_2 and of M/S_1.

Algorithm 12 Submodule of a finite $\mathbf{Z}[G]$-module

Input: A finite $\mathbf{Z}[G]$-module M of prime power order.
Output: All the submodules of M.

```
1. If $M$ is trivial, return the trivial submodule.
2. Compute the submodule $N = \{m \in M \mid pm = 0\}$.
3. Compute the set $S$ of irreducible submodules of $N$ using the Meataxe algorithm.
4. Initialize an empty list of submodules $L$.
5. For each submodule $Q \in S$,
   a) Compute the quotient $M/Q$.
   b) Recursively, compute the set $\tilde{S}_{M/Q}$ of submodules of $M/Q$.
   c) Compute the lift of the submodules in $\tilde{S}_{M/Q}$ to $M$ and add them in $L$.
6. Remove all the multiple occurrences of a submodule in $L$.
7. Return $L$.
```

Remark 2.10. Assume we want to compute only submodules N of M such that the quotient M/N has exponent m. As mM itself is G-invariant, these correspond to submodules of M/mM. In the situation where $M = \mathrm{Cl}_{\mathfrak{m}}$ is the ray class group, this implies that again it is sufficient to only compute the quotient $\mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^m$ instead of the whole ray class group.

Example 2.11. We consider the action of $G = C_2 = \langle\sigma\rangle$ on the abelian group $M = C_4 \times C_4$ given by $\sigma(1,0) = (0,1)$ and $\sigma(0,1) = (1,0)$. We want to find the $(\mathbf{Z}/4\mathbf{Z})[G]$-submodules of M. The first step is to find the irreducible submodules of the submodule of elements of order 2: there is only one, generated by the element $(2,2)$. Denote it by N. Thus, we need to find the irreducible $(\mathbf{Z}/4\mathbf{Z})[G]$-submodules of M/N. The quotient is isomorphic to the group $C_2 \times C_4$ with the action $\sigma(1,0) = (1,0)$ and $\sigma(0,1) = (1,1)$. Again, we need to compute the irreducible submodules of exponent 2: this time the action on the submodule of elements of order 2 is trivial, so every subgroup is a submodule. Taking preimages, we have found the submodules $\langle(2,2)\rangle$, $\langle(2,0),(0,2)\rangle$, $\langle(1,3),(2,2)\rangle$ and $\langle(1,1)\rangle$. The algorithm continues then by computing the irreducible submodules in the quotients by the last 3 submodules.

Submodules with given structure Algorithm 12 can be modified so that it finds submodules of M with a given structure, i.e. isomorphic to an abelian group A. The idea is to construct the submodules with the desired structure layer by layer. Denote by p^iA the subgroup of A given by the elements of the form p^ix for $x \in A$ and for $i \in \{0,\dots,k\}$ and assume we have already all the submodules $S_1,\dots,S_l$ isomorphic to p^iA for a given $0 < i < k$. For every submodule S_i, we consider the quotient M/S_i and search in the quotient for a submodule isomorphic to $p^{i-1}A/p^iA$. Then, we compute the lift of every submodule obtained this way and discard all the lifts that are not isomorphic to $p^{i-1}A$. This approach presents some desirable features, that we highlight in the following remarks.

Remark 2.12. The method presented above completely avoids the redundancy. Indeed, assume that we compute the same submodule $\tilde{M}$ twice at the i-th step, coming from two submodules N_1, N_2 of the $(i-1)$-st step. Then $p\tilde{M}$ is by construction a submodule isomorphic to $p^{k-i}A$ contained in both N_1 and N_2. Since $N_1 \simeq N_2 \simeq p^{k-i}A$, we must have $N_1 = N_2$. This means that the situation described above can not happen, so that we can skip the final check for multiple occurrences of submodules that we did in Step (6) of Algorithm 12.

Remark 2.13. A more subtle observation is a consequence of Nakayama's lemma [43, Chapter X, Section 4]. At the i-th step, we search for submodules of M/Q, where Q is a submodule isomorphic to $p^{k-i+1}A$, such that their lifts are isomorphic to $p^{k-i}A$. Given a submodule $\tilde{N}$ of M/Q, we compute first its lift N to M and then check if it has the desired structure. By means of Nakayama's lemma, if N has the correct structure, then it is generated by any set of preimages of the generators of $\tilde{N}$. This allows us to work with a smaller set of generators of N, improving the performance.

Algorithm 13 Submodule of a finite $\mathbf{Z}[G]$-module with a given structure

```
Input: A finite $\mathbf{Z}[G]$-module $M$ of prime power order, an abelian $p$-group $A$
    of exponent $p^k$.
Output: All the submodules of $M$ isomorphic to $A$.

1. Compute the submodule $N = \{p^{k-1}m \mid m \in M\}$.
2. Compute the set $L_{k-1}$ of submodules of $N$ isomorphic to $p^{k-1}A$.
3. If $k = 1$, return $S$.
4. For $i = k-2, \ldots, 0$,
    a) Initialize an empty list $L_i$.
    b) Compute the quotient $B_i = p^iA/p^{i+1}A$.
    c) For each submodule $Q \in L_{i+1}$,
        • Compute the quotient $M_Q = M/Q$.
        • Compute the submodule $N_Q = \{p^im \mid m \in M_Q\}$.
        • Compute the set $S_Q$ of submodules of $N_Q$ isomorphic to $B_i$.
        • Append to $L_i$ the lifts of the elements of $S_Q$ to $M$.
    d) Remove from $L_i$ the submodules that are not isomorphic to $A$.
5. Return $L_0$.
```

Duality

Algorithm 13 is inefficient if we are looking for submodules with small index in M, because of the multiple recursive calls. In this case, we can use duality to translate the problem of finding submodules of small index into the one of finding submodules of small order.

Definition 2.14. *Let M be a finite abelian group of exponent n. We define the dual group M^* of M as* $\mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Z}/n\mathbf{Z})$

The dual group M^* is isomorphic to M, even if this isomorphism is not canonical and depends on the choice of a basis. In our case, we assume that M has exponent p^s and is given in Smith normal form, that is, $M = \mathbf{Z}/p^{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{n_w}\mathbf{Z}$ with $1 \leq n_1 \leq \cdots \leq n_w = s$. Let $e_1, \dots, e_w$ be the canonical generators of M. Then we define elements of the dual

$$\begin{array}{rrcl} e_i^*\colon & M & \longrightarrow & \mathbf{Z}/p^s\mathbf{Z} \\ & e_j & \longmapsto & \delta_{ij} p^{s-n_j} \end{array}$$

where δ_{ij} is the Kronecker delta and $\operatorname{ord}(e_i)$ denotes the order of e_i. The dual is again in Smith normal form with respect to this generating set. In any case, we have that $(M^*)^*$ is canonically isomorphic to M.
Now, we want to endow the dual group of a structure of $\mathbf{Z}/p^s\mathbf{Z}[G]$-module.

Definition 2.15. *Let M be a finite abelian group and let φ be an endomorphism of M. We define the dual endomorphism as the map*

$$\begin{array}{rrcl} \varphi^*\colon & M^* & \longrightarrow & M^*, \\ & f & \longmapsto & f \circ \varphi, \end{array}$$

In particular every element $g \in G$ acts on M^*, giving M^* the structure of a $(\mathbf{Z}/p^s\mathbf{Z})[G]$-module. The action of G on the dual group just defined preserves the inclusion-reversing correspondence existing between subgroups of M and subgroups of M^*.

Definition 2.16. *Let M be a finite abelian group. Given a subgroup H of M, define the orthogonal $H^\top$ as*

$$H^\perp = \{\varphi \in M^* \mid H \subseteq \ker(\varphi)\}.$$

Lemma 2.17. *Let H be a submodule of M. Then the orthogonal $H^\perp$ is a submodule of M^*.*

Proof. Let $g \in G$ and let φ_g be the induced map on M. It is enough to show that φ_g^* leaves $H^\perp$ invariant. Let $x \in H^\perp$; then $\varphi_g^*(x) = x \circ \varphi_g$. As H is a submodule of M, for every $y \in H$ it holds $\varphi_g(y) \in H$ and $H \subseteq \ker(x)$. Thus the kernel of $x \circ \varphi_g$ contains H, proving that it is in $H^\perp$.

Proposition 2.18. *There is an inclusion-reversing bijection between submodules of M and M^*:*

$$\begin{array}{rccc} \psi_M\colon & \{(\mathbf{Z}/p^s\mathbf{Z})[G]\text{-submodules of } M\} & \longrightarrow & \{(\mathbf{Z}/p^s\mathbf{Z})[G]\text{-submodules of } M^*\} \\ & H & \longmapsto & H^\perp. \end{array}$$

For every submodule H of M, it holds $H^\perp \simeq G/H$. Furthermore, the composition of ψ_M with ψ_{M^*} is the identity on the set of submodules of M.

Proof. Follows from Lemma 2.17 and [43, Chapter I, §9].

Thus submodules of M of small index correspond to submodules of the dual module of small order. In order to make this computationally effective, we need to understand how to get the structure of G-module on the dual group M^*. As above, we assume that M is given in Smith normal form with generators e_i and we consider the corresponding element of the dual e_i^*. Let $\varphi \in \mathrm{Aut}(M)$ be the automorphism of M induced by $g \in G$; we want compute the matrix $A = (a_{ij})$ associated to φ^* with respect to the basis e_i^*. By definition, $\varphi^*(e_i^*) = e_i^* \circ \varphi$. Let B be the matrix representing φ with respect to the elements e_i. Then

$$\varphi^*(e_i^*)(e_j) = e_i^*(\varphi(e_j)) = e_i^*\Big(\sum_s b_{js} e_s\Big) = b_{ji} e_i^*(e_i) = b_{ji} p^{s-n_i}$$

On the other hand,

$$\varphi^*(e_i^*)(e_j) = \Big(\sum_k a_{ik} e_k^*\Big)(e_j) = a_{ij} e_j^*(e_j) = a_{ij} p^{s-n_j}$$

Therefore, it is enough to choose a_{ij} satisfying the relation $a_{ij} p^{s-n_j} = b_{ji} p^{s-n_i}$.

Algorithm 14 Submodules with a given structure of the quotient

Input: A finite $\mathbf{Z}[G]$-module M of prime power order, an abelian p-group A.
Output: All the submodules of M with quotient isomorphic to A.

1. Compute the dual module M^*.
2. Compute the set S of submodules of M^* isomorphic to A using Algorithm 13.
3. Compute the set $S^\perp$ of the orthogonal submodules of the elements in S.
4. Return $S^\perp$.

Example 2.19. Let us consider the $G = C_2 = \langle\sigma\rangle$-module $M = C_2 \times C_4$ with the action $\sigma(1,0) = (1,0)$ and $\sigma(0,1) = (1,1)$. Thus we can represent the action via the matrix

$$M_\sigma = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

The dual module M^* is then isomorphic to $C_2 \times C_4$; in order to determine the action, we need to transpose the matrix and multiply the entries by a suitable power of 2. We thus obtain

$$M_\sigma^* = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

The submodule N of M generated by $(1,0)$ correspond in this way to the submodule $N^\perp$ of M^* generated by $(0,1)$. Notice that, as expected, as an abelian group, since $N \simeq C_2$, we have that $M/N^\perp \simeq C_2$ and, vice versa, since $N^\perp \simeq C_4$, we have $M/N \simeq C_4$.

2.3 Computation of automorphisms

We have seen in the previous section that the knowledge of the automorphisms of the field is crucial for the algorithm, as they are essential to compute the Galois action on the ideals of K. In this section, we develop an algorithm to compute the automorphisms of the fields appearing in our construction. In particular, we consider a normal extension K of a number field K_0 and an abelian extension L of K which is normal over K_0 too. Under these assumptions, we have the following exact sequence:

$$1 \to \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/K_0) \longrightarrow \mathrm{Gal}(K/K_0) \to 1$$

Thus, we can find a set of generators for $\mathrm{Gal}(L/K_0)$ by computing generators for $\mathrm{Gal}(L/K)$ and lifts of generators of $\mathrm{Gal}(K/K_0)$ to $\mathrm{Gal}(L/K_0)$.

We assume that we have computed defining polynomials for L/K using the algorithm of Section 1.5.

Elements of $\mathrm{Gal}(L/K)$ The computation of $\mathrm{Gal}(L/K)$ can be split into different parts by considering the subfields corresponding to the cyclic components of $\mathrm{Gal}(L/K)$, as they are linearly disjoint extensions of K. Thus, we can assume that L is a cyclic extension of K of degree n, where n is a prime power. Recall that, from the computation of a defining polynomial for L, we know an element $\beta \in K(\zeta_n)$ such that $F = L(\zeta_n) = K(\zeta_n)(\sqrt[n]{\beta})$. Denote by E the cyclotomic extension $K(\zeta_n)$. By Galois theory, the restriction $\mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K)$ is an isomorphism. Moreover, since F/E is a Kummer extension with generator $\sqrt[n]{\beta}$, we have that $\mathrm{Gal}(F/E)$ is generated by

$$\begin{aligned} \sigma\colon\ & F \longrightarrow F \\ & \sqrt[n]{\beta} \longmapsto \zeta_n \sqrt[n]{\beta}. \end{aligned}$$

In particular, $\sigma|_L$ is a generator of $\mathrm{Gal}(L/K)$. Let γ be the primitive element of L. In order to compute the restriction, we first map γ to F and then find using linear algebra $a_0, \ldots, a_{n-1} \in K$ such that

$$\sigma|_L(\gamma) = \sigma(\gamma) = \sum_{i=0}^{n-1} a_i \gamma^i.$$

2.3.1 Containment of Kummer extensions

Before dealing with the extension of the automorphisms, we consider a more general problem that we will use for that purpose. Let K be a number field containing the n-th roots of unity and let L_1, L_2 be Kummer extensions of K of exponent n, so that there exists $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t \in K$ and $n_1, \ldots n_s, m_1, \ldots, m_t \in \mathbf{N}$ dividing n such that $L_1 = K(\sqrt[n_1]{\alpha_1}, \ldots, \sqrt[n_s]{\alpha_s})$ and $L_2 = K(\sqrt[m_1]{\beta_1}, \ldots, \sqrt[m_t]{\beta_t})$. We want to decide whether L_1 is a subfield of L_2 and, in that case, find an embedding. For simplicity, we assume $s = 1$:

if we have an algorithm to embed $K(\sqrt[n]{\alpha})$ into L_2, we can apply it to every cyclic component $K(\sqrt[n_i]{\alpha_i})$ of L_1.

The idea of the algorithm is to take advantage of the properties of Kummer extensions: as they are abelian extensions of K, the Frobenius automorphism of a prime ideal of the Kummer extension depends only on the underlying prime ideal of K and we can easily identify Frobenius automorphisms by a modular computation.

Suppose that $L_1 = K(\sqrt[n]{\alpha})$ embeds into L_2. Then, by the properties of Kummer extensions, we have a relation

$$\sqrt[n]{\alpha} = c\prod_{i=1}^{t} \sqrt[m_i]{\beta_i^{q_i}} \tag{2.1}$$

with $c \in K$ and the exponents $q_1, \dots, q_t$ with $0 \leq q_i \leq m_i - 1$ for every $i \in \{1, \dots, t\}$: under this assumption, $q_1, \dots, q_t$ are unique. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be prime ideals of K such that the corresponding Frobenius automorphisms generate $\mathrm{Gal}(L_2/K)$. Applying the Frobenius automorphism of a prime $\mathfrak{p}_i$ to the relation 2.1, we get

$$\mathrm{Frob}_{\mathfrak{p}_i,L_1}(\sqrt[n]{\alpha}) = c\prod_{i=1}^{t} \mathrm{Frob}_{\mathfrak{p}_i,L_2}\left(\sqrt[m_i]{\beta_i^{q_i}}\right)$$

As we know how the Frobenius automorphism acts on $\sqrt[m_i]{\beta_i}$ and $\sqrt[n]{\alpha}$, there exist $r_{\mathfrak{p}_i}, r_{\mathfrak{p}_i,1}, \dots, r_{\mathfrak{p}_i,t}$ such that

$$\zeta_n^{r_{\mathfrak{p}_i}}\sqrt[n]{\alpha} = c\prod_{j=1}^{t} \zeta_n^{r_{\mathfrak{p}_i,j}q_j}\sqrt[m_i]{\beta_j^{q_j}}$$

which gives us a relation between the exponents $r_{\mathfrak{p}_i} = \sum_{j=1}^{t} r_{\mathfrak{p}_i,j}q_j \pmod{n}$. Thus, we get the following linear system of equations over $\mathbf{Z}/n\mathbf{Z}$ with variables $x_1, \dots, x_t$

$$\begin{cases} r_{\mathfrak{p}_1} = \sum_{j=1}^{t} r_{\mathfrak{p}_1,j}x_j \\ \qquad\vdots \\ r_{\mathfrak{p}_t} = \sum_{j=1}^{t} r_{\mathfrak{p}_t,j}x_j \end{cases} \tag{2.2}$$

of which $q_1, \dots, q_t$ is a solution.

Proposition 2.20. *Let L_1, L_2 be Kummer extensions of K of exponent n with generators $\sqrt[n]{\alpha}$ and $\sqrt[m_1]{\beta_1}, \dots, \sqrt[m_t]{\beta_t}$ respectively. Let $q_1, \dots, q_t \in \mathbf{Z}/n\mathbf{Z}$ and $c \in K$ be elements such that $\sqrt[n]{\alpha} = c\prod_{j=1}^{t} \sqrt[m_j]{\beta_j}^{q_j}$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ be prime ideals of K such that $\mathrm{Frob}_{\mathfrak{p}_1,L_2}, \dots, \mathrm{Frob}_{\mathfrak{p}_t,L_2}$ generate $\mathrm{Gal}(L_2/K)$. Then $q_1, \dots, q_t$ is the unique solution to (2.2) satysfying $0 \leq q_i \leq m_i - 1$.*

Proof. We have already proven that $n_1, \dots, n_t$ is a solution to (2.2). The uniqueness comes from the fact that every solution $z_1, \dots, z_t$ with $0 \leq z_i \leq m_i - 1$ corresponds to a relation

$$\sqrt[n]{\alpha} = c_z \prod_{i=1}^{t} \sqrt[m_i]{\beta_i^{z_i}}$$

and such a relation is unique by the properties of Kummer extension.

Under the assumption that $L_1 \subseteq L_2$, this gives us a method to compute the embedding: we solve the linear system (2.2) in order to find $q_1, \dots, q_t$. Once this is done, we can recover the element c of (2.1) by extracting an n-th root of

$$\frac{\alpha}{\beta_1^{n_1} \cdots \beta_t^{n_t}} = c^n.$$

Notice that there exists n different roots of c^n: the different solutions correspond to the different embeddings that exist.

The algorithm may fail in one of the following steps:

- the Frobenius automorphisms of $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ in L_1 do not generate the Galois group $\mathrm{Gal}(L_1/K)$;
- the linear system (2.2) has either multiple solutions or none;
- the final n-root computation fails.

If this happens, then L_1 is not embeddable into L_2: otherwise, we get the desired embedding.

Algorithm 15 Embedding between Kummer extensions

```
Input: A cyclic Kummer extension $L_1 = K(\sqrt[n]{\alpha})$ and a Kummer extension
    $L_2 = K(\sqrt[m_1]{\beta_1}, \dots, \sqrt[m_t]{\beta_t})$.
Output: Either an embedding $L_1 \to L_2$ or an error in the case an embedding
    does not exist.

1. Compute $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ prime ideals of $K$ such that $\mathrm{Frob}_{\mathfrak{p}_1, L_2}, \dots, \mathrm{Frob}_{\mathfrak{p}_t, L_2}$
   generate $\mathrm{Gal}(L_2/K)$.
2. If $\mathrm{Frob}_{\mathfrak{p}_1, L_1}, \dots, \mathrm{Frob}_{\mathfrak{p}_t, L_1}$ do not generate $\mathrm{Gal}(L_1/K)$, return an error.
3. For each prime $\mathfrak{p}_i$,
     • Compute the elements $q_{\mathfrak{p}_i, j}$ such that $\mathrm{Frob}_{\mathfrak{p}_i, L_2}(\sqrt[m_i]{\beta_j}) = \zeta_n^{q_{\mathfrak{p}_i, j}} \sqrt[m_i]{\beta_j}$.
     • Compute the element $n_{\mathfrak{p}_i}$ such that $\mathrm{Frob}_{\mathfrak{p}_i, L_1}(\sqrt[n]{\alpha}) = \zeta_n^{q_{\mathfrak{p}_i}} \sqrt[n]{\alpha}$.
4. Solve the linear system

   $$\begin{cases} q_{\mathfrak{p}_1} &= \sum_{j=1}^{t} q_{\mathfrak{p}_1, j} x_j \\ & \vdots \\ q_{\mathfrak{p}_t} &= \sum_{j=1}^{t} q_{\mathfrak{p}_t, j} x_j \end{cases}$$

   over $\mathbf{Z}/n\mathbf{Z}$. If the system doesn't admit a solution, return an error. Otherwise, let $q_1, \dots, q_t$ be lifts of the components of the solution with the
   constraints $0 \le q_i \le m_i - 1$.
```

5. Compute a n-th root c of $\alpha\beta_1^{-q_1}\cdots\beta_t^{-q_t}$ in K. If such a root c does not exist, return an error. Otherwise, return the embedding

$$\begin{array}{rccc} \iota\colon & L_1 & \longrightarrow & L_2 \\ & \sqrt[n]{\alpha} & \longmapsto & c\prod_{j=1}^{t} \sqrt[m_i]{\beta_j^{q_j}} \end{array}$$

2.3.2 Extension of automorphisms

We now deal with the computation of lifts of the generators of $\mathrm{Gal}(K/K_0)$ to $\mathrm{Gal}(L/K)$. The naive way of computing $\mathrm{Gal}(L/K_0)$ would be to write L/K_0 as a simple extension and to find the roots of the defining polynomial. While this works well for small degrees, it quickly becomes infeasible. We show a method to extend the automorphisms that takes advantage of the information obtained during the computation of a defining equation and the properties of Kummer extensions.

Reduction to prime power degree. Firstly, we reduce to the case of an extension of prime power degree.

Lemma 2.21. *Let L/K be an abelian extension and assume that both L and K are normal over a subfield K_0. Let p be a prime divisor of $[L : K]$ and let L_p be the maximal subextension of L/K of degree a power of p. Then L_p is normal over K_0.*

Proof. Via Galois correspondence, L_p correspond to the subgroup $G_{(p)}$ of $\mathrm{Gal}(L/K)$ given by the product of the Sylow subgroups of $\mathrm{Gal}(L/K)$ for all the prime divisors of its order except for p. The lemma follows from a simple group theoretic argument: given a group G and subgroups $S \subseteq H$, if H is normal in G and S is characteristic in H, then S is normal in G. It is enough to apply this simple observation to $\mathrm{Gal}(L/K_0)$ as G, $\mathrm{Gal}(L/K)$ as H and G_p as S.

Let $p_1, \dots, p_s$ be the prime divisors of $[L : K]$. As the fields $L_{p_1}, \dots, L_{p_s}$ are linearly disjoint over K, we can compute generators for $\mathrm{Gal}(L/K_0)$ from the lifts of a given set of generators of $\mathrm{Gal}(K/K_0)$ to $\mathrm{Gal}(L_p/K_0)$. For this reason, in the following we will assume that $\mathrm{Gal}(L/K)$ is a p-group. In particular, we write L as the composite of linearly disjoint cyclic extensions $L_i = K(\gamma_i)$ of prime power degree p^{m_i}.

Extension of the automorphisms to the Kummer extension

Let m be the maximum of the m_i, set $n = p^m$ and denote by E the cyclotomic extension $K(\zeta_n)$ of K. We make the additional assumption that we have an embedding of L into a Kummer extension $E(\sqrt[n]{\beta_1}, \dots, \sqrt[n]{\beta_t})$ normal over K_0, so that we have the following lattice of number fields:

$$\begin{tikzcd}
 & E(\sqrt[m]{\beta_1},\ldots,\sqrt[m]{\beta_t}) & & \\
L \arrow[ur] & & E \arrow[ul] & \\
 & K \arrow[ul] \arrow[ur] & & K_0(\zeta_n) \arrow[ul] \\
 & & K \cap K_0(\zeta_n) \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

We aim at extending $\sigma \in \mathrm{Gal}(K/K_0)$ to an automorphism of $E(\sqrt[n]{\beta_1},\ldots,\sqrt[n]{\beta_t})$ and then restricting it to L. As the first step, we extend σ to $K(\zeta_n)$: denoted by the K_1 intersection $K_0(\zeta_n) \cap K$, $K(\zeta_n)/K_1$ is the compositum of the linearly disjoint extensions K/K_1 and $K(\zeta_n)/K_1$. It is then straightforward to extend σ to an automorphism of $K(\zeta_n)$, which we also denote by σ.

$$\begin{tikzcd}
 & K(\zeta_n) = E & \\
K \arrow[ur, dash] & & K_0(\zeta_n) \arrow[ul, dash] \\
 & K_1 \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

In the next step, we extend σ to an automorphism $\hat{\sigma}$ of $E(\sqrt[n]{\beta_1},\ldots,\sqrt[n]{\beta_t})$ by determining $\hat{\sigma}(\sqrt[n]{\beta_i})$ for all $i = 1,\ldots,r$. We apply Algorithm 15 to the extensions $E(\sqrt[n]{\sigma(\beta_i)})$ and $E(\sqrt[n]{\beta_1},\ldots,\sqrt[n]{\beta_t})$ in order to get the image of $\sqrt[n]{\beta_i}$ under σ. Doing this for every cyclic component $\sqrt[n]{\sigma(\beta_i)}$ gives us the image of $\sqrt[n]{\beta_i}$ under σ for all $i \in \{1,\ldots,r\}$ and thus the extension of the automorphism $\hat{\sigma}$.

$$\begin{tikzcd}
 & E(\sqrt[m]{\beta_1},\ldots,\sqrt[m]{\beta_t}) & \\
L \arrow[ur, dash] & & E \arrow[ul, dash] \\
 & K \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

As the final step, we restrict the automorphism to L by using linear algebra.

Reduction to a Kummer extension over the same cyclotomic field

Now we show how to compute a suitable Kummer extension and an embedding of L into it in order to reduce to the setting of the previous paragraph.

Let $L_1/K, \dots, L_s/K$ be the cyclic extensions of K of degree $p^{m_1}, \dots, p^{m_s}$ respectively that we have constructed when computing a defining polynomial for L. In particular, for every $i \in \{1, \dots, s\}$, we have constructed a generator $\beta_i \in K(\zeta_{p^{m_i}})$ for the Kummer extension $L_i(\zeta_{p^{m_i}})$. Given $m = \max_i m_i$ and $n = p^m$, we want to construct the smallest Kummer extension of $E = K(\zeta_{p^m})$ containing L. Generically, L and $K(\zeta_n)$ are linearly disjoint. In these case, we can easily embed L into $K(\zeta_{p^m}, \sqrt[p^{m_1}]{\beta_1}, \dots, \sqrt[p^{m_s}]{\beta_s})$ by taking the composition of the embedding of L_i into $L_i(\zeta_{p^{m_i}})$ and the embedding of $L_i(\zeta_{p^{m_i}})$ into $K(\zeta_{p^m}, \sqrt[p^{m_i}]{\beta_i})$. Sufficient conditions to test whether we are in this situation are provided by the following lemma:

Lemma 2.22. *Assume that one of the following holds:*

- $\operatorname{disc} L$ *is coprime to* p*;*
- *the maximal abelian subextension of* L *over* $\mathbf{Q}$ *is contained in* K*.*

Then L *and* $K(\zeta_n)$ *are linearly disjoint.*

Proof. The first condition implies that none of the primes that ramify in L is ramified in $\mathbf{Q}(\zeta_n)$ and vice versa. Thus L and $\mathbf{Q}(\zeta_n)$ are linearly disjoint and the same must be true for L and $K(\zeta_n)$ over K. Assume now that the second condition holds. Then $[K \cap \mathbf{Q}(\zeta_n) : \mathbf{Q}] = [L \cap \mathbf{Q}(\zeta_n) : \mathbf{Q}]$. Then

$$[K(\zeta_n) : K] = [\mathbf{Q}(\zeta_n) : K \cap \mathbf{Q}(\zeta_n)] = [\mathbf{Q}(\zeta_n) : L \cap \mathbf{Q}(\zeta_n)] = [L(\zeta_n) : L],$$

proving that L and $K(\zeta_n)$ are linearly disjoint over K.

Assume now that none of the conditions of the lemma holds. The first step is to determine whether L and $K(\zeta_n)$ are linearly disjoint. Let $A \subseteq \mathrm{Cl}_{\mathfrak{m}}$ be the congruence subgroup of K corresponding to L. We decide the disjointness by computing the norm group B of $K(\zeta_n)$ in $\mathrm{Cl}_{\mathfrak{m}}$. If the subgroup AB coincides with the whole $\mathrm{Cl}_{\mathfrak{m}}$, then the extensions are disjoint and we can apply the same strategy as above. Suppose now that $AB \subsetneq \mathrm{Cl}_{\mathfrak{m}}$. Then the restriction map $\operatorname{res}\colon \operatorname{Gal}(L(\zeta_n)/K(\zeta_n)) \to \operatorname{Gal}(L/K)$ composed with the inverse of the Artin map $\Phi_{L/K}^{-1}\colon \operatorname{Gal}(L/K) \to \mathrm{Cl}_{\mathfrak{m}}/A$ has the subgroup $AB/A \subseteq \mathrm{Cl}_{\mathfrak{m}}/A$ as image. In particular, we can establish this map by means of the Frobenius automorphisms. The Galois group $\operatorname{Gal}(L(\zeta_n)/K(\zeta_n))$ is a quotient of the product $\prod_{i=1}^{s} \operatorname{Gal}(K(\zeta_n)(\sqrt[p^{m_i}]{\beta_i})/K(\zeta_n))$ (by the universal property of the direct product). In order to decide the kernel of the projection, we compute the Frobenius automorphisms of primes of $K(\zeta_n)$ in the product of the Kummer extensions and compute their images in $\mathrm{Cl}_{\mathfrak{m}}/A$, until we generate the whole subgroup AB/A. In this way, we establish a surjective map $\psi\colon \prod_{i=1}^{s} \operatorname{Gal}(K(\zeta_n)(\sqrt[p^{m_i}]{\beta_i})/K(\zeta_n)) \to AB/A$ whose kernel corresponds to the kernel of the projection $\prod_{i=1}^{s} \operatorname{Gal}(K(\zeta_n)(\sqrt[p^{m_i}]{\beta_i})/K(\zeta_n)) \to \operatorname{Gal}(L(\zeta_n)/K(\zeta_n))$. Thus, we can represent $\operatorname{Gal}(L(\zeta_n)/K(\zeta_n))$ as a quotient of $G = \prod_{i=1}^{s} C_{p^{m_i}}$. Denote by H the kernel of the projection. We compute then the Smith normal form of G/H together with the change of basis. Let

$M = (m_{ij})_{i,j}$ be the matrix representing the projection from G to the Smith normal form of G/H. Let $g_1, \ldots, g_t$ be the generators of G/H (in Smith normal form). Since the map is surjective, every generator g_i has a preimage $\tilde{g}_i = (\tilde{g}_{i,1}, \ldots, \tilde{g}_{i,s}) \in G$. Then we take as generators of the Kummer extension $L(\zeta_n)/K(\zeta_n)$ the elements

$$\gamma_j = \prod_{i=1}^{s} \sqrt[p^{m_i}]{\beta_i^{\tilde{g}_{j,i}}}$$

for $j \in \{1, \ldots, t\}$. In order to get the embedding, some of the images of the elements $\sqrt[p^{m_i}]{\beta_i}$ can be recovered via linear algebra from the definition of the γ_j. If this is not possible, we apply Algorithm 15 to the cyclic component $K(\zeta_n)(\sqrt[p^{m_i}]{\beta_i})$.

Example 2.23. Consider the field $K = \mathbf{Q}(\sqrt{3})$ and its abelian extension $L = K(\zeta_{16})$. L corresponds to a congruence subgroup A of the ray class group $\mathrm{Cl}_{\mathfrak{m}}$, with $\mathfrak{m} = (16\mathcal{O}_K, \mathfrak{m}_\infty)$ and $\mathfrak{m}_\infty$ contains the two real places of K. Notice that $\mathrm{Gal}(L/K) \simeq C_2 \times C_4$, thus following the algorithm of Section 1.5, we compute L as the composite of a quadratic extension and a cyclic extension of degree 4. The corresponding Kummer extensions are the quadratic extension of K defined by the polynomial $x^2 + 1$ and the degree 4 extension of $K(i)$ given by the polynomial $x^4 + 1$. We denote by α and β the corresponding Kummer generators.

To extend the generator σ of $\mathrm{Gal}(K/\mathbf{Q})$, we need to write $L(i)$ as a Kummer extension of $K(i)$. By computing the norm group of $K(i)$ in $\mathrm{Cl}_{\mathfrak{m}}$, we see that $K(i) \cap L$ has degree 2 over K. We then establish a map φ between $C_2 \times C_4$ and the image of $\mathrm{Gal}(L(i)/K(i))$ in $\mathrm{Cl}_{\mathfrak{m}}/A$ by computing Frobenius automorphisms. The kernel of φ is the subgroup H generated by $(1, 0)$. By computing the Smith normal form of $C_2 \times C_4/H$, we see that $L(i)/K(i)$ is the Kummer extension defined by the polynomial $x^4 + 1$. To get the embedding, it is easy to compute the image of β via linear algebra, as it coincides with the chosen Kummer generator for $L(i)/K(i)$. In order to compute the image of α, we need instead to apply Algorithm 15. As a result, we get i (or $-i$) as the image of α.

2.4 From the relative extension to the absolute field

The last part of the algorithm consists in the computation of a primitive element of the field, as well as the automorphisms and the maximal order of the field, in order to prepare the data for the next layer.

Let L be an abelian extension of K and assume that we have already computed a representation of L as an extension $K(\alpha_1, \ldots, \alpha_k)$, where $\alpha_1, \ldots, \alpha_k$ are integral elements, and generators for the Galois group $\mathrm{Gal}(L/\mathbf{Q})$ in this representation. In order to translate the data from the relative setting to the absolute one, we perform the following operations:

- find a primitive element α;
- compute the maximal order of $\mathbf{Q}(\alpha)$;
- find a "small" primitive element β;
- compute the automorphisms of $\mathbf{Q}(\beta)$.

Find a primitive element The computation of a primitive element for L is based on the following classical result:

Lemma 2.24. *Let $L = K(\alpha_1, \dots, \alpha_k)$ be a number field and let γ be a primitive element for K. Then there exists a linear combination $\alpha = a\gamma + \sum_{i=1}^{k} a_i\alpha_i$ such that $K = \mathbf{Q}(\alpha)$.*

Proof. See [43, Chapter V, Theorem 4.6].

Thus, finding a primitive element for L is straightforward. Together with a primitive element, we also compute an isomorphism between the representation of K as $\mathbf{Q}(\alpha)$ and $K(\alpha_1, \dots, \alpha_k)$.

2.4.1 Maximal order

The second step is then the computation of the maximal order of L, assuming that we already have a maximal order for K. In order to exploit the knowledge of this additional information, we adjust the algorithm to compute the maximal order to our hypotheses. Indeed, the maximal order computation starts usually with the order $\mathbf{Z}[\alpha]$ and enlarge it until we reach the maximal order. However, we have at our disposal the order $\mathcal{O} = \mathcal{O}_K[\alpha_1, \dots, \alpha_k]$ and its basis

$$\left\{ \gamma_j \prod_{i=1}^{k} \alpha_i^{s_i} \mid j \in \{1, \dots, \deg(K)\}, s_i \in \{0, \dots, \deg_K(\alpha_i) - 1\} \right\},$$

where $\gamma_1, \dots, \gamma_{\deg(K)}$ is a basis for the maximal order of K and $\deg_K(\alpha_i)$ denotes the degree of the minimal polynomial of α_i over K.

Remark 2.25. We could compute directly the maximal order of the relative extension L/K. In practice, this computation seems more expensive than the strategy we are going to describe. Further experiments would be needed in this direction, even if the implementation we are going to describe seems to be good enough for our purposes.

Prefactorization of the discriminant

The first step of the algorithm is a prefactorization of the discriminant. Let d be the discriminant of the starting order $\mathcal{O}$ and let $f \in \mathbf{Z}[x]$ be the monic defining polynomial of the field L. Then we try to apply the Euclidean algorithm to f and f' over $\mathbf{Z}/d\mathbf{Z}$. Whenever we encounter a non invertible leading coefficient c in the sequence of remainders, we stop the algorithm: we have found a factor of d. In this case, we compute a coprime base $\{b_1, \dots, b_s\}$ of the set $\{c, d\}$ (see [4]) and iterate the computation over $\mathbf{Z}/b_i\mathbf{Z}$ for $i = \{1, \dots, s\}$, until we don't find any new divisor of d. At the end of this process, we get some factors $s_1, \dots, s_l$ of d with the property that $\gcd(s_i, s_j) = 1$ and every prime divisor of d divides one of the s_i. Moreover, we also check if the s_i are powers of a smaller integer (see [5]) and, in that case, we substitute them with their roots. Finally, we compute a factorization of every s_i as $s_i = \tilde{s}_i \prod p_i^{e_i}$ where $p_1, \dots, p_t$ are the prime divisors of s_i smaller than a suitably chosen bound B; in our implementation we check the first 10^5 primes, but more sensible choices can be made depending on the size of d. As a result, we have found some small prime factors of the discriminant and some large divisors.

Computation of the p-maximal order at small primes

Let p be a prime divisor of the discriminant of $\mathcal{O}$. We want to compute then the p-maximal overorder of $\mathcal{O}$. If p does not divide $[\mathcal{O} : \mathbf{Z}[\alpha]]$, then we compute the p-maximal overorder $\mathcal{O}_p$ of $\mathbf{Z}[\alpha]$ and then sum $\mathcal{O}$ with $\mathcal{O}_p$. For this purpose, we have implemented the method developed in [23], which is sufficient for most cases. This strategy is not optimal, as a full implementation of Montes algorithm as in [32] or [62] would be faster. However, our implementation is fast enough for our purpose and we decided not to investigate further.

Assume that p divides $[\mathcal{O} : \mathbf{Z}[\alpha]]$. In this case, we use the Round Two algorithm [14, Section 6.1] to extend the order. The Round Two algorithm iterates the following two steps:

- computation of a test ideal J for p;
- computation of the ring of multipliers $(J :_L J)$.

We illustrate our implementation since it seems to perform quite well in practice.

Computation of a test ideal for p Let A be an order between $\mathcal{O}$ and the maximal order $\mathcal{O}_L$. The first step of the Round Two algorithm consists in computing a test ideal at p.

Definition 2.26. *Let A be an order in a number field L and let p be a prime number. A test ideal for p is a radical ideal $J \subseteq A$ contained in every prime ideal $\mathfrak{p}$ lying over p such that $A_\mathfrak{p}$ is not integrally closed.*

The knowledge of a test ideal is enough to enlarge the order or to test its maximality by [31, Proposition 3.6.5]. Usually, the test ideal J is chosen as the radical of the ideal generated by p. However, this might be in general too much, as some of the localizations at prime ideals lying over p might already be invertible. Indeed, in the case of the equation order $\mathbf{Z}[\alpha]$, we can find a better test ideal.

Lemma 2.27. *Let $L = \mathbf{Q}(\alpha)$ be a number field generated by an integral element α and let $f \in \mathbf{Z}[x]$ be its minimal polynomial. Let p be a prime number* *and let $g \in \mathbf{Z}[x]$ be a lift of the squarefree part of (f, f') (mod p). Then the ideal $(p, g(\alpha))$ is a test ideal.*

Proof. It follows immediately from the fact that $f'(\alpha)$ is contained in every prime ideal $\mathfrak{p}$ such that $A_{\mathfrak{p}}$ is not integrally closed ($f'(\alpha)$ is contained in the conductor of $\mathbf{Z}[\alpha]$ in $\mathcal{O}_L$) and that $(p, g(\alpha))$ is the radical of $(p, f'(\alpha))$.

Remark 2.28. Lemma 2.27 improves over Dedekind criterion [14, Theorem 6.1.4], as it provides the test ideal $(p, h(\alpha))$ where $h \in \mathbf{Z}[x]$ is a lift of the squarefree part of f modulo p.

Lemma 2.29. *Let J be the test ideal for p in A. Then the radical of JA' is a test ideal for p in A'.*

Proof. If $\mathfrak{p}$ is a prime ideal of A' such that $A'_{\mathfrak{p}}$ is not integrally closed, then $A_{\mathfrak{p}\cap A}$ is not integrally closed.

Corollary 2.30. *Let A, A' be orders of L such that $\mathbf{Z}[\alpha] \subseteq A \subseteq A'$ and let J be the test ideal for p in $\mathbf{Z}[\alpha]$ as in Lemma 2.27. Then the radical J' of JA is a test ideal for p in A and the radical of $J'A'$ is a test ideal for p in A'.*

Thus we can use always information coming from a suborder to compute a large (in terms of containment) test ideal. The advantage of this approach is that, given the test ideal J for p in A, the dimension of the $\mathbf{F}_p$-algebra A'/J is lower than the dimension of A'/pA', meaning that the linear algebra involved in the computation of the radical deals with matrices of smaller dimension.

In order to compute the radical of a $\mathbf{F}_p$-algebra B, there are mainly two methods: if $p \le k = \dim B$, then the radical is the kernel of the Frobenius $\Phi_n(x) = x^{p^n}$ as a $\mathbf{F}_p$-linear map, where $n > \log_p k$. Notice that this map is the composition of n standard Frobenius $\Phi(x) = x^p$. Thus, instead of computing the matrix representing Φ_n, it is better to compute the kernel iteratively: in order to find the kernel of Φ_i, we compute the kernel K_{i-1} of Φ_{i-1} and then the kernel of Φ restricted to K_{i-1}. In the case $p > k$, then the radical is just the kernel of the trace matrix, i.e. the matrix M such that $M_{i,j} = \mathrm{tr}(x_i x_j)$, where $x_1, \dots, x_k$ is a basis of B.

Ring of multipliers Let now J be a test ideal for p in A; we want to compute the ring of multipliers

$$(J\colon {}_L J) = \{x \in L \mid xJ \subseteq J\}.$$

Given generators $g_1, \dots, g_s$ of the ideal J, we consider their representation matrices $M_{g_1}, \dots, M_{g_s}$ with respect to the basis of A. Let M_J the matrix whose rows represent a basis of J with respect to the basis of A. Notice that $p(J\colon {}_L J)$ is an ideal of A. The characteristic property of $p(J\colon {}_L J)$ is that, given the row matrix $v \in \mathbf{Z}^n$ representing an element $x \in p(J\colon {}_L J)$, there exists $y \in \mathbf{Z}^n$ such that $xM_{g_i} = yM_J$ for all $i \in \{1, \dots, s\}$. Thus, inverting the matrix M_J, the problem reduces to find the Hermite normal form of the matrix

$$M = \begin{pmatrix} M_{g_1} \\ M_{g_2} \\ \vdots \\ M_{g_s} \end{pmatrix} \cdot M_J^{-1}$$

The only observations that are crucial in this step are the following:

- the computation of the Hermite normal form can be done modularly, since the largest elementary divisor of M is p;
- the number of the generators involved makes a difference in the runtime; in particular, it is unwise to use the basis of J as a set of generators. A smaller set can be obtained directly from the computation of the test ideal. Otherwise, we can compute at every step the ideal I_i generated by $g_1, \dots, g_i$ and consider the representation matrix of g_{i+1} only if it is not contained in I_i.

Large factors of the discriminant

Let q be one of the large factors of the discriminant that we found in the first step. Basically, we follow the approach explained in [12]. However, we propose the following improvement that applies whenever q is coprime to $[\mathcal{O}\colon \mathbf{Z}[\alpha]]$. In this case, we try to mimic the Dedekind criterion. Let f be the minimal polynomial of α: by the choice of q, we already know that the Euclidean algorithm on f and f' modulo q succeeds and the result can't be trivial, otherwise the ideal $(q, f'(\alpha))$ would be trivial meaning that q is not a factor of the discriminant. Thus, it yields a polynomial $g \in \mathbf{Z}[x]$ and a factorization $f = gh \pmod q$, with $h \in \mathbf{Z}[x]$. In particular, there exists a polynomial $t \in \mathbf{Z}[x]$ such that $f = gh + qt$ over $\mathbf{Z}$. We then try to compute via the Euclidean algorithm the greatest common divisor of g, h and t modulo q. If we find a divisor of q, we can split q and restart. Suppose instead that the algorithm finishes and the result is non trivial, yielding a polynomial $u \in \mathbf{Z}[x]$. Then we can write $f = u^2\tilde{f}\tilde{g} + qu\tilde{t}$ for suitable polynomials $\tilde{f}, \tilde{g}, \tilde{t}$.

Lemma 2.31. *Let $K = \mathbf{Q}(\alpha)$ be a number field and let $f \in \mathbf{Z}[x]$ be the minimal polynomial of α. Let q be a positive integer and assume we can write f as*

$$f = u^2\tilde{f}\tilde{g} + qu\tilde{t}$$

for monic polynomials $u, \tilde{f}, \tilde{g} \in \mathbf{Z}[x]$ and $\tilde{t} \in \mathbf{Z}[x]$. Let $r \in Z[x]$ be a lift of the quotient f/u modulo q. Then $r(\alpha)/q$ is an integral element in K.

Proof. It is enough to show that $r(\alpha)/q$ is contained in the ring of multipliers of $J = (q, \tilde{g}(\alpha)) \subseteq \mathbf{Z}[\alpha]$. The product $(r(\alpha)/q) \cdot q = r(\alpha)$ is clearly contained in J, since for the polynomials it holds $r \equiv f/u \equiv u\tilde{f}\tilde{g} \pmod q$. For $(r(\alpha)/q) \cdot \tilde{g}(\alpha)$, we notice that $r \equiv u\tilde{f}\tilde{g} + q\tilde{t} \pmod{q^2}$, so there exists $w \in \mathbf{Z}[x]$ such that $r = u\tilde{f}\tilde{g} + q\tilde{t} + q^2 w$. This means that

$$\frac{r(\alpha)\tilde{g}(\alpha)}{q} = \frac{u(\alpha)\tilde{f}(\alpha)\tilde{g}(\alpha)^2}{q} + \underbrace{\tilde{t}(\alpha)\tilde{g}(\alpha)}_{\in J} + \underbrace{q\tilde{g}(\alpha)w(\alpha)}_{\in J}.$$

Thus we only need to show that the first term is in J. Notice that it follows immediately from the definition of r that there exists a polynomial $s \in \mathbf{Z}[x]$ such that $u(\alpha)\tilde{f}(\alpha)\tilde{g}(\alpha) = -q\tilde{t}(\alpha) + q^2 s(\alpha)$. Hence,

$$\frac{u(\alpha)\tilde{f}(\alpha)\tilde{g}(\alpha)^2}{q} = -\tilde{t}(\alpha) + qs(\alpha)$$

and the right hand side is clearly in J, as claimed.

If this doesn't work, then we use the algorithm of [12] in order to get the maximal order. Experiments show that in most cases the factorization of q is not needed, even if counterexamples can be easily produced.

2.4.2 Reduction of the primitive element

The primitive element α that we found in the first step of the process might be quite large, in two different ways:

- the coefficients of its minimal polynomials are large;
- its T_2-norm is large.

Here we discuss a method to find a primitive element for L with a (hopefully) smaller T_2-norm. We follow a similar approach to the one explained in [16]. A reduction of the primitive element in the sense of the size of the coefficients of the minimal polynomial is instead presented in [33].

Let L be a number field given by a primitive element α with a monic minimal polynomial $f \in \mathbf{Z}[x]$.

Find the candidate primitive elements First of all, we want to collect a set of short elements of L that might be primitive. In order to do this, we compute a LLL basis $b_1, \dots, b_n$ of the maximal order $\mathcal{O}_L$ and we consider the elements of the basis as well as all the small combinations $b_i \pm b_j$ of them.

Test for primitiveness The second step is to discard all the elements that lie in a subfield: given a candidate $\gamma \in L$, we want to test whether γ is a primitive element for the field or, equivalently, whether γ has n different conjugates. Thus we want to know the cardinality of the orbit of γ under the action of the Galois group of L. We perform this computation modularly.

Lemma 2.32. *Let p be a prime number that doesn't divide the discriminant of f. The projection map $\mathcal{O}_L \to \mathcal{O}_L/p\mathcal{O}_L$ induces an embedding of $\mathrm{Gal}(L/\mathbf{Q})$ in $\mathrm{Aut}_{\mathbf{F}_p}(\mathbf{F}_p[x]/f)$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be the roots of f in $\mathcal{O}_L$ and let $\bar{\alpha}_1, \dots \bar{\alpha}_n$ be their projection in $\mathcal{O}_L/p\mathcal{O}_L$. As p does not divide the discriminant of f, then $\mathcal{O}_L/p\mathcal{O}_L \simeq \mathbf{F}_p[x]/f$. Then the projection map induces a map between $\mathrm{Gal}(L/\mathbf{Q})$ and $\mathrm{Aut}(\mathbf{F}_p[x]/f)$: given $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$ sending α_1 to α_i, the images of σ is an automorphism $\tilde{\sigma}$ sending $\bar{\alpha}_1$ to $\bar{\alpha}_i$. The injectivity of the map follows from the fact that p does not divide the discriminant of f, meaning that the elements $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ are all distinct.

Remark 2.33. The normality of the field doesn't really play a role here. Suppose that L is not normal and let $\tilde{L}$ its normal closure. Let p be a prime number that doesn't divide the discriminant of f. Then $\mathcal{O}_L/p\mathcal{O}_L$ injects into $\mathcal{O}_{\tilde{L}}/p\mathcal{O}_{\tilde{L}}$, and f splits completely over the latter. By the hypothesis on p, $\mathcal{O}_L/p\mathcal{O}_L$ is isomorphic to $\mathbf{F}_p[x]/(f)$ and the fact that f splits completely over $\mathcal{O}_{\tilde{L}}/p\mathcal{O}_{\tilde{L}}$ means that we have an injection of $\mathbf{F}_q[x]/(f)$ into $\mathcal{O}_{\tilde{L}}/p\mathcal{O}_{\tilde{L}}$, where $\mathbf{F}_q$ is the splitting field of f over $\mathbf{F}_p$. As $\gamma \in L$, the image of γ under an automorphism of $\tilde{L}$ is determined by the image of a root α of f. The orbit of α under the action of $\mathrm{Gal}(\tilde{L}/\mathbf{Q})$ is given by the roots of f in $\tilde{L}$, that we denote by $\alpha_1 = \alpha, \dots, \alpha_n$. The projection of those roots in $\mathcal{O}_{\tilde{L}}/p\mathcal{O}_{\tilde{L}}$ is contained in $\mathbf{F}_q[x]/(f)$: this means that we can study the orbit of γ just by looking at the orbit of its projection in $\mathbf{F}_q[x]/(f)$ under the action of the group of automorphisms given by the map sending the projection of α to a root of f in $\mathbf{F}_q[x]/(f)$.

As a consequence, we can determine whether a γ is primitive by a modular computation. Suppose that $\operatorname{disc} \mathbf{Z}[\gamma]$ is not divisible by p; then, in order to understand if γ is primitive, we compute the orbit of the image of γ in $\mathcal{O}_L/p\mathcal{O}_L \simeq \mathbf{F}_p[x]/(f)$. More precisely, we compute the roots $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ of f in $\mathbf{F}_p[x]/(f)$ and compute $\bar{\gamma}(\bar{\alpha}_i)$ for $i \in \{1, \dots, n\}$. If the cardinality of the orbit of $\bar{\gamma}$ is n, then γ is primitive; otherwise, γ is not primitive. Since testing whether p divides $\operatorname{disc} \mathbf{Z}[\gamma]$ is expensive, we do not check that the condition holds for the input element: the algorithm will return false if γ is not primitive or if p divides $\operatorname{disc} \mathbf{Z}[\gamma]$.

Algorithm 16 Test for primitiveness

```
Input: A number field $L$ with defining polynomial $f$, an element $\gamma \in L$, a
    prime number $p$ not dividing the discriminant of $f$.
Output: Returns false if $\gamma$ is not primitive or if $p$ divides the discriminant of
    $\gamma$, true otherwise

1. Compute the splitting field $\mathbf{F}_q$ of $f$ over $\mathbf{F}_p$.
2. Compute the roots $\delta_1, \dots, \delta_n$ of $f$ over $\mathbf{F}_q$.
3. Compute the image $\bar{\gamma}$ of $\gamma$ in $\mathbf{F}_q[x]/(f)$.
4. Initialize an empty set $o$ which will consist of the orbit of $\bar{\gamma}$.
5. For $i \in \{1, \dots, n\}$,
     • Compute the image $\bar{\gamma}_i$ of $\bar{\gamma}$ under the automorphism sending $x$ to $\delta_i$.
    • If $\bar{\gamma}_i \in o$, return false. Otherwise, add $\bar{\gamma}_i$ to $o$.
6. Return true.
```

In order to determine whether an element γ is primitive, we need apply the algorithm for different primes and produce a bound on the primes that we need to test. Let $\sigma_1, \dots, \sigma_n$ the embeddings of L into $\mathbf{C}$. Then

$$|\operatorname{disc} \mathbf{Z}[\gamma]| = \prod_{i<j} |(\sigma_i(\alpha) - \sigma_j(\alpha))| \leq 2^{n^2} \max |\sigma_i(\alpha)|^{n^2}$$

Notice that we already know that $\operatorname{disc} L$ is a divisor of $\operatorname{disc} \mathbf{Z}[\gamma]$ and that if a prime number p divides $\operatorname{disc} \mathbf{Z}[\gamma]$ but $p \nmid \operatorname{disc} L$, then $p^2 \mid \operatorname{disc} \mathbf{Z}[\gamma]$. Thus, we can apply Algorithm 16 for a set of primes $p_1, \dots, p_n$ such that

$$|\operatorname{disc} K| \prod p_i^2 \geq 2^{n^2} \max |\sigma_i(\alpha)|^{n^2}$$

in order to be sure that the element is not primitive. This method is quite efficient in our case, since we take as input elements coming from a LLL basis of $\mathcal{O}_L$, thus having a rather small T_2-norm.

Choose the primitive element At this point, we have a set of primitive elements $x_1, \dots, x_s \in \mathcal{O}_L$ and we pick the smallest in terms of their T_2-norms. We denote the chosen element by β. We need to compute the minimal polynomial of β: in order to do so, the best strategy is to compute the minimal polynomial of the representation matrix of β in terms of the basis of the maximal order.

CHAPTER 3

Embedding problems

Algorithm 1 to construct fields with a given Galois group E follows the natural idea that a chain of subgroups of G corresponds to a tower of subfields of the target fields. By means of Shafarevich's theorem, we know that a field with Galois group G exists. However, in our construction we need to solve a more specific problem: given a number field K with Galois group G, where G is a quotient of E, we would like to embed K into a field with Galois group E. As we have shown in Example 2 in the introduction this might fail, motivating this chapter, which is devoted to the analysis of the solvability of embedding problems under an algorithmic perspective.

3.1 Second cohomology group and Brauer group

In this section we recall some basic facts on the second cohomology group and the Brauer group. The reader can find an extensive introduction to the subject in [45, 58].

Second cohomology group Let G be a group and let A be a $\mathbf{Z}[G]$-module. We define the group of (two)-cocycles $\mathrm{Z}^2(G, A)$ as the abelian group consisting of all the maps $c\colon G \times G \to A$ satisfying for all $\sigma, \tau, \delta \in G$ the relation

$$\sigma(c(\tau, \delta)) \cdot c(\sigma, \tau\delta) = c(\sigma, \tau) \cdot c(\sigma\tau, \delta)$$

where A is denoted multiplicatively. The group of (two)-coboundaries $\mathrm{B}^2(G, A)$ is the subgroup of $\mathrm{Z}^2(G, A)$ consisting of the cocycles $c \in \mathrm{Z}^2(G, A)$ for which there exists a map $a_c\colon G \to A$ such that for all $\sigma, \tau \in G$

$$c(\sigma, \tau) = \sigma(a_c(\tau)) \cdot a_c(\sigma\tau)^{-1} \cdot a_c(\sigma).$$

Definition 3.1. *Given a group G and a $\mathbf{Z}[G]$-module A, the second cohomology group $\mathrm{H}^2(G, A)$ is defined as the factor group $\mathrm{Z}^2(G, A)/\mathrm{B}^2(G, A)$.*

It follows immediately from the definition that, if G and A are finite, $\mathrm{H}^2(G, A)$ is a finite abelian group. In particular, if A is finite of exponent n, the exponent of $\mathrm{H}^2(G, A)$ divides n. Not surprisingly, the structure of the group plays a role too:

Proposition 3.2. *Let G be a finite group of order m and A be a $\mathbf{Z}[G]$-module. Then $\mathrm{H}^2(G, A)$ is annihilated by m.*

Proof. See [60, Chapter VIII, Corollary 1].

Corollary 3.3. *Assume that G and A are finite and $\gcd(|G|, |A|) = 1$. Then $\mathrm{H}^2(G, A)$ is trivial.*

Proof. Let $x \in \mathrm{H}^2(G, A)$. By the previous proposition, the order of x must divide the order of G. Moreover, we said previously that the order of x divides the exponent of A. As the orders are coprime by hypothesis, we must have that the order of x is one, i.e. $\mathrm{H}^2(G, A) = \{e\}$.

Cohomology and extensions

The elements of $\mathrm{H}^2(G, A)$ are in correspondence with the extensions of G by A, as we are going to see. Given a short exact sequence $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$, we can endow A with a structure of $\mathbf{Z}[G]$-module. Let $s\colon G \to E$ be a set theoretic map such that $\pi \circ s = \mathrm{id}_G$. Given $g \in G$ and $a \in A$, g acts on a by $g(a) = \iota^{-1}(s(g) \cdot \iota(a) \cdot s(g)^{-1})$. It is well defined as the image of ι is a normal subgroup of E and ι is injective.

Definition 3.4. *Let G be a group and A a $\mathbf{Z}[G]$-module. An extension of G by A is an exact sequence*

$$1 \to A \longrightarrow E \longrightarrow G \to 1$$

such that the structure of $\mathbf{Z}[G]$-module on A coincides with the structure induced by the exact sequence.

Definition 3.5. *Let G be a group and A be a $\mathbf{Z}[G]$-module. Let $1 \to A \xrightarrow{\iota_1} E \xrightarrow{\pi_1} G \to 1$ and $1 \to A \xrightarrow{\iota_2} E \xrightarrow{\pi_2} G \to 1$ be extensions of G by A. We say that the two extensions are equivalent if there exists an automorphism φ of E such that the following diagram commutes:*

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\iota_1"] \arrow[d, "\mathrm{id}"'] & E \arrow[r, "\pi_1"] \arrow[d, "\varphi"'] & G \arrow[r] \arrow[d, "\mathrm{id}"'] & 1 \\
1 \arrow[r] & A \arrow[r, "\iota_2"'] & E \arrow[r, "\pi_2"'] & G \arrow[r] & 1
\end{tikzcd}$$

Proposition 3.6. *Let G be a group and let A be a G-module. There is a correspondence between the extensions of G by A up to equivalence and the elements of $\mathrm{H}^2(G, A)$.*

Proof. The full proof can be found in [10, Chapter IV, Theorem 3.12]. Here we give a sketch of the proof as it shows from an algorithmic point of view how to determine a cocycle corresponding to an extension. Let $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ be an extension and let $s\colon G \to E$ be a section of π, i.e. a map (not necessarily a homomorphism) such that $\pi \circ s = \mathrm{id}$. Given $\sigma, \tau \in G$, we consider the element $\tilde{c}(\sigma,\tau) = s(\sigma)s(\tau)s(\sigma\tau)^{-1} \in E$. Notice that $\pi(\tilde{c}(\sigma,\tau))$ is the identity of G, thus there is an element $c(\sigma,\tau) \in A$ such that $\iota(c(\sigma,\tau)) = \tilde{c}(\sigma,\tau)$. By the associativity of the operation in E, c is a cocycle. One could verify that a different section would have produced a cocycle that differs from the one we got before by a coboundary. This means that we can associate to every extension a class in $\mathrm{H}^2(G,A)$.

Among the possible extensions of G by A, we obviously have the semi-direct product $A \rtimes G$, which plays a special role in the theory.

Definition 3.7. *Let G be a group and A be a $\mathbf{Z}[G]$-module. The split extension of G by A is the extension given by $1 \to A \to A \rtimes G \to G \to 1$.*

Remark 3.8. If $\gcd(|A|,|G|) = 1$, the split extension is the only extension of G by A by Corollary 3.3. However, the action of G on A plays a key role if we want to study the isomorphism class of groups that arising as extensions of G by A. Consider the case of $G = C_2$ and $A = C_3$: if G acts trivially on A the resulting split extension is isomorphic to C_6, otherwise it is isomorphic to S_3.

Proposition 3.9. *Let $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ be an extension and let $c \in \mathrm{H}^2(G,A)$ be the corresponding class. The following are equivalent:*

1. *the extension is split;*
2. *$c = 0$;*
3. *there exists a homomorphism $s\colon G \to E$ such that $\pi \circ s = \mathrm{id}$.*

Proof. The equivalence of (1) and (3) follows from [10, Chapter IV, Proposition 2.1]. To prove that (2) and (3) are equivalent, we use the correspondence between cocycles and extensions that we introduced in the proof of Proposition 3.6. If (2) holds, then there is a choice of the section $s\colon G \to E$ that makes the corresponding cocycle trivial. In particular, s is an homomorphism, proving (3). Conversely, if (3) holds, then the cocycle corresponding to s is trivial.

Functorial properties of the cohomology

We now recall the properties of the cohomology group with respect to homomorphisms of G-modules and homomorphisms of groups.

Maps between modules Let G be a finite group and let A, B be $\mathbf{Z}[G]$-module. Let $\varphi\colon A \to B$ be an homomorphisms of $\mathbf{Z}[G]$-modules. Then φ induces a map $\tilde{\varphi}$ between the cohomology groups

$$\tilde{\varphi}\colon \mathrm{H}^2(G, A) \to \mathrm{H}^2(G, B)$$

sending $c \in \mathrm{Z}^2(G, A)$ to $\tilde{\varphi}(c)(\sigma, \tau) = \varphi(c(\sigma, \tau))$. The map is well defined because it sends coboundaries to coboundaries.

Assume now that A is finite. In particular, A is a finite abelian group and we have a decomposition of A into the direct sum of its Sylow subgroups. The action of G on A leaves the Sylow subgroups invariant, yielding a decomposition of A as a $\mathbf{Z}[G]$-module. This results in a decomposition for the cohomology group:

Proposition 3.10. *Let A be a $\mathbf{Z}[G]$-module of order n. Let $n = \prod_{i=1}^{r} p_i^{e_i}$ be the factorization of n into prime numbers. For p a prime divisor of n, denote by A_p the p-Sylow subgroup of A. Then $\mathrm{H}^2(G, A) \simeq \oplus_{i=1}^{r} \mathrm{H}^2(G, A_{p_i})$. Moreover, this coincides with the decomposition of $\mathrm{H}^2(G, A)$ induced by its Sylow subgroups.*

Subgroups The cohomology groups behave nicely with respect to subgroups of G too. Indeed, given a subgroup H of G, we define the restriction map $\mathrm{res}_{G,H}\colon \mathrm{H}^2(G, A) \to \mathrm{H}^2(H, A)$ as the map taking a cocycle and restricting its domain to H. In terms of the extensions, given $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ corresponding to an element $c \in \mathrm{H}^2(G, A)$, the extension $1 \to A \to \pi^{-1}(H) \to H \to 1$ is in the class of $\mathrm{res}_{G,H}(c)$. The map is in general neither injective nor surjective, but it has nice properties when it involves a Sylow subgroup of G:

Lemma 3.11. *Let G be a finite group, let A be a $\mathbf{Z}[G]$-module and let G_p be a p-Sylow subgroup of G. Let H_p be the p-Sylow subgroup of $\mathrm{H}^2(G, A)$. Then the restriction map*

$$\mathrm{res}_{G,G_p}\colon \mathrm{H}^2(G, A) \to \mathrm{H}^2(G_p, A)$$

is injective on H_p.

Proof. See [60, Chapter IX, Theorem 4].

Inflation map Finally, we will show the behaviour of the cohomology group with respect to quotients by a normal subgroup.

Let H be a normal subgroup of G and let A be a $\mathbf{Z}[G]$-module. Then the submodule A^H of A given by the elements that are fixed by the action of H can be considered as a $\mathbf{Z}[G/H]$-module: given the projection $p_H\colon G \to G/H$, for every $a \in A^H$ and $g \in G/H$, we consider an element $\tilde{g} \in p_H^{-1}(g)$ and define $g(a)$ as $(\tilde{g})(a)$. This is well-defined and does not depend on the choice of the preimage since a is fixed by H. Now, if c is a cocycle in $\mathrm{Z}^2(G/H, A^H)$, we define a cocycle $\tilde{c} \in \mathrm{Z}^2(G, A)$ by $\tilde{c}(\sigma, \tau) = c(p_H(\sigma), p_H(\tau))$. This induces a map between the cohomology groups

$$\inf_{G,H}\colon \mathrm{H}^2(G/H, A^H) \to \mathrm{H}^2(G, A)$$

which is usually called inflation map. This map has a direct interpretation in terms of extensions by means of the pull-back of groups.

Definition 3.12. *Let G_1, G_2, H be groups and let $f_1\colon G_1 \to H$, $f_2\colon G_2 \to H$ be homomorphisms of groups. The pull-back of f_1, f_2 is a triple (P, g_1, g_2), where P is a group and $g_1\colon P \to G_1$, $g_2\colon P \to G_2$ are homomorphisms such that, for every group Q and pair of homomorphisms $q_1\colon Q \to G_1$, $q_2\colon Q \to G_2$ such that $f_1 \circ q_1 = f_2 \circ q_2$, there exists a map $\psi\colon Q \to P$ that makes the following diagram commute:*

$$\begin{tikzcd}
Q \arrow[drr, bend left, "q_2"] \arrow[dr, dashed, "\psi"] \arrow[ddr, bend right, "q_1"'] & & \\
& P \arrow[r, "g_2"'] \arrow[d, "g_1"'] & G_2 \arrow[d, "f_2"] \\
& G_1 \arrow[r, "f_1"'] & H
\end{tikzcd}$$

Proposition 3.13. *Let G_1, G_2, H be groups and let $f_1\colon G_1 \to H$, $f_2\colon G_2 \to H$ be homomorphisms of groups. The pull-back (P, g_1, g_2) of f_1 and f_2 exists and it is unique up to a unique isomorphism. Moreover, the group P can be characterized as*

$$P = \{(x, y) \in G_1 \times G_2 \mid f_1(x) = f_2(y)\}$$

Example 3.14. The pull-back is a generalization of the direct product of groups. Indeed, the direct product $G_1 \times G_2$ can be identified as the pull-back of the trivial maps $G_1 \to \{e\}$ and $G_2 \to \{e\}$. This follows directly from the definition of pull-back and coincides with the characterization given in the proposition.

By using the existence of the pull-back, we can explicitly describe the inflation map in terms of extensions.

Proposition 3.15. *Let $1 \to A^H \xrightarrow{\iota} E \xrightarrow{\pi} G/H \to 1$ be the extension corresponding to a cocycle $c \in \mathrm{H}^2(G/H, A^H)$. Consider the pull-back $(\tilde{E}, p_1, p_2)$ of π and the projection $\pi_H\colon G \to G/H$. Then the extension*

$$1 \to A \to \tilde{E} \xrightarrow{p_2} G \to 1$$

is an extension corresponding to the class of $\inf_{G,H}(c)$.

Proof. See [29, Remark 3.3.11].

Brauer group

We now focus on the applications of cohomology groups in number theory. Let L be a normal extension of a number field K and denote by G the Galois group $\mathrm{Gal}(L/K)$. Then the multiplicative group $L^\times$ is naturally a $\mathbf{Z}[G]$-module and we can study the cohomology group $\mathrm{H}^2(G, L^\times)$. In particular, we can use the properties of the subfields in order to characterize the cohomology group $\mathrm{H}^2(G, L^\times)$ by combining the inflation map and the restriction map:

Proposition 3.16. *Let L be a number field and let $G = \mathrm{Gal}(L/K)$. Let H be a normal subgroup of G and let F be its fixed field. Then the following sequence is exact:*

$$1 \to \mathrm{H}^2(G/H, F^\times) \xrightarrow{\mathrm{inf}_{G,H}} \mathrm{H}^2(G, L^\times) \xrightarrow{\mathrm{res}_{G,H}} \mathrm{H}^2(H, L^\times)$$

Proof. Follows from [60, Chapter VII, Proposition 5] and [60, Chapter X, Proposition 2].

Crossed product algebras Given a cocycle $c \in \mathrm{Z}^2(G, L^\times)$, we can construct a K-algebra as follows. For each element σ of the group, we consider an element u_σ. The elements of the algebra are K-linear combinations of elements of the form $\alpha \mathrm{u}_\sigma$, where $\alpha \in L^\times$. We need to define the multiplication: given two elements $\alpha \mathrm{u}_\sigma$ and $\beta \mathrm{u}_\tau$, we define $\alpha \mathrm{u}_\sigma \cdot \beta \mathrm{u}_\tau = \alpha\sigma(\beta)c(\sigma,\tau)\mathrm{u}_{\sigma\tau}$, and we extend it by distributivity.

Definition 3.17. *The algebra we described above is called a crossed product algebra and denoted by $(L/K, G, c)$.*

This construction depends on the cocycle, but equivalent cocycles give rise to isomorphic algebras:

Lemma 3.18. *Let $c, c' \in \mathrm{Z}^2(G, L^\times)$ be two representatives of the same class of $\mathrm{H}^2(G, L^\times)$. Then $(L/K, G, c)$ is isomorphic to $(L/K, G, c')$.*

Proof. See [58, Theorem 29.6].

Thus, we can associate to every class of $\mathrm{H}^2(G, L^\times)$ an isomorphism class of crossed product algebras.

Definition 3.19. *Let $A = (L/K, G, c)$ be a crossed product algebra. We say that A splits if A is isomorphic as a K-algebra to the matrix algebra $M_n(K)$, where $n = [L : K]$.*

Theorem 3.20. *Let c be a cocycle representing a class in $\mathrm{H}^2(G, L^\times)$ and let A be the corresponding crossed product algebra. Then A splits if and only if the class of c is zero.*

Proof. See [58, Theorem 29.8].

Thus, if we want to determine whether a cocycle represents the trivial cohomology class in $\mathrm{H}^2(G, L^\times)$, we can instead determine whether the corresponding crossed product algebra is isomorphic to a matrix algebra over K. In the case of a cyclic extension, we have an additional criterion to determine whether a crossed product algebra splits.

Proposition 3.21. *Assume that L/K is a cyclic extension and let σ be a generator of the Galois group G. Let $A = (L/K, G, c)$ be a crossed product algebra and consider the element $a = \prod_{i=1}^{n-1} c(\sigma, \sigma^i) \in K$. Then A splits if and only if a is a norm of an element of L.*

Proof. Follows from [58, Theorem 30.3, Theorem 30.4].

3.2 Enumeration of the embedding problems

The existence of an extension of a number field with a given Galois group is related to the so-called embedding problems.

Definition 3.22. *Let K/K_0 be a normal extension with Galois group G. An embedding problem for E over K is an extension $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$.*

We say that the embedding problem is solvable if the restriction map $\psi\colon \mathrm{Gal}(\bar{K}_0/K_0) \to G$ can be lifted to an homomorphism $\varphi\colon \mathrm{Gal}(\bar{K}_0/K_0) \to E$ such that $\pi \circ \varphi = \psi$.

Remark 3.23. According to Definition 3.4, the group A must be abelian. In the literature, embedding problems can be defined in a more general way (see for example [53]).

Remark 3.24. In the definition of solvability of an embedding problem we do not require surjectivity of the lift. However, if a lift exists, there exists a surjective one. This follows from [49, Chapter IV, Theorem 1.8] and [49, Chapter IV, Theorem 2.4]. This means that if an embedding problem is solvable, there exists an extension L/K such that $\mathrm{Gal}(L/K) \simeq E$.

The definition of embedding problem relies on an extension involving G and the target group E. However, there may be various extensions of G isomorphic to E and thus various embedding problems to be considered.

Example 3.25. Let $K = \mathbf{Q}(\sqrt{a}, \sqrt{b})$ and suppose that we are searching for an extension of K with Galois group isomorphic to the dihedral group D_4 of order 8, generated by elements r, s with presentation $r^4 = e$, $s^2 = e$, $rs = sr^3$. The Galois group of K is isomorphic to $C_2 \times C_2$: we identify the element $(1, 0)$ with the automorphism sending $\sqrt{a}$ to $-\sqrt{a}$ and fixing $\sqrt{b}$ and the element $(0, 1)$ with the automorphism sending $\sqrt{b}$ to $-\sqrt{b}$ and fixing $\sqrt{a}$.

We consider two projections $D_4 \to C_2 \times C_2$:

$$\begin{array}{rcl} \pi_1\colon\ D_4 & \longrightarrow & C_2 \times C_2 \\ r & \longmapsto & (1,0) \\ s & \longmapsto & (0,1) \end{array} \qquad \begin{array}{rcl} \pi_2\colon\ D_4 & \longrightarrow & C_2 \times C_2 \\ r & \longmapsto & (0,1) \\ s & \longmapsto & (1,0) \end{array}$$

The maps differ by an automorphism of $C_2 \times C_2$, so we might be led to think that the corresponding embedding problems are related. However, the interpretation in terms of fields clarifies that the two embedding problems are quite different. Indeed, let L_1 be a field with Galois group D_4 such that the restriction homomorphism $\mathrm{res}\colon \mathrm{Gal}(L_1/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q})$ coincides with π_1 (assuming it exists). The extension $L_1/\mathbf{Q}(\sqrt{b})$ corresponds to the subgroup generated by r in D_4; in particular, it is a cyclic extension of order 4. Denote by K_b the subfield $\mathbf{Q}(\sqrt{b})$; then the quadratic extension $K_b(\sqrt{a})$ is embedded into a C_4-extension. Instead, as $(0,1)$ does not admit a preimage of order 4, the same is not true for $K_a = \mathbf{Q}(\sqrt{a})$ inside L_1. The roles are reversed if we consider instead an extension L_2 realizing the projection π_2. This shows that the embedding problems might impose different conditions on the subfields and have an effect on the lattice of subfields of the solutions.

The existence of an extension of K with Galois group E relies on the solvability of any embedding problem that can occur with G and E as a group in the middle. Thus, we focus on the enumeration of the embedding problems that need to be considered to decide the existence of an extension of K with Galois group isomorphic to E. Such an extension will exist if and only if any of the embedding problems is solvable.

Detection of the possible kernels The first step of the algorithm is to detect the isomorphism class of the kernels of any projection $E \to G$.

Example 3.26. Consider the groups $G = C_2$ and $E = C_4 \times C_2$. Then projection $E \to G$ has as kernel isomorphic to either C_4 or $C_2 \times C_2$.

In order to overcome this problem, we list all the normal subgroups of E of order $|E|/|G|$ and check if they give rise to G as factor group.

Enumerate all the extensions Given a group A computed in the first step, we have an induced extension $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$. Starting from this, we list all the possible exact sequences having $\iota(A)$ as kernel.

Every automorphism of A and G gives rise by composition to a different group extension: if $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ is one of the possible embedding problems and $\phi \in \mathrm{Aut}(G)$, $\chi \in \mathrm{Aut}(A)$, the exact sequence

$$1 \to A \xrightarrow{\iota\circ\chi} E \xrightarrow{\phi\circ\pi} G \to 1$$

is another embedding problem and the subgroup in the kernel of the projection is still $\iota(A)$. Following this method, we list all the exact sequences involving the groups E and G.

Cohomological equivalence The number of extensions we found in the previous step depends on the automorphism groups of both G and the kernel, which might be large. In order to reduce their number, we consider them up to cohomological equivalence.

Lemma 3.27. *Let $1 \to A \xrightarrow{\iota_1} E \xrightarrow{\pi_1} G \to 1$ and $1 \to A \xrightarrow{\iota_2} E \xrightarrow{\pi_2} G \to 1$ be two embedding problems over K. If the extensions are equivalent, then either both are solvable, or none of them is.*

Proof. It is enough to show that if one of the two problems is solvable, without loss of generality the first, then the other is solvable too. Let $\varphi \in \mathrm{Aut}(E)$ be the automorphism giving the equivalence between the two extensions and let $\phi\colon \mathrm{Gal}(\bar{K}_0/K_0) \to E$ be a homomorphism such that $\pi_1 \circ \varphi = \psi$. Then it is clear that $\pi_2 \circ \phi \circ \varphi = \psi$, proving that the second problem is solvable.

By Lemma 3.27, we can therefore consider extensions up to cohomological equivalence. Let $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ be one of the extensions. We study the action of $\mathrm{Aut}(E)$ on $\mathrm{Aut}(A) \times \mathrm{Aut}(G)$: let H be the subgroup of $\mathrm{Aut}(E)$ that leaves the image of A invariant, i.e. $H = \{f \in \mathrm{Aut}(E) \mid f(\iota(A)) = \iota(A)\}$. Then we have a map

$$\begin{aligned} \varphi\colon H &\longrightarrow \mathrm{Aut}(G) \times \mathrm{Aut}(A) \\ h &\longmapsto (\pi \circ h \circ \pi^{-1}, \iota^{-1} \circ h \circ \iota) \end{aligned} \tag{3.1}$$

We claim that if (g, a) and (g', a') are in the same coset with respect to the image of φ, then the corresponding cocycles are cohomologous. Indeed, they differ by the image of an element $h \in H$ and we have the following diagram

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\iota \circ a"] \arrow[d, "\mathrm{id}"'] & E \arrow[r, "g \circ \pi"] \arrow[d, "h"'] & G \arrow[r] \arrow[d, "\mathrm{id}"'] & 1 \\
1 \arrow[r] & A \arrow[r, "\iota \circ a'"'] & E \arrow[r, "g' \circ \pi"'] & G \arrow[r] & 1
\end{tikzcd}$$

where the rows are exact and the squares are commutative. This shows that the extensions are equivalent, proving the following proposition:

Proposition 3.28. *Let $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ be an extension. Let φ be the map defined as in* (3.1)*. The extensions of G by A isomorphic to E and with kernel $\iota(A)$ are in correspondence with the cosets of the image of φ in* $\mathrm{Aut}(G) \times \mathrm{Aut}(A)$.

We summarize this as an algorithm:

Algorithm 17 Enumeration of embedding problems

Input: Two groups G and E.
Output: All the extensions of G isomorphic to E up to equivalence.

```
1. Initialize an empty list of exact sequences $L$.
2. Compute all the normal subgroups $A_1, \dots, A_s$ of $E$ such that $E/A_i \simeq G$.
3. For each $i = 1, \dots, s$
    • Denote by $\iota_i$ the inclusion of $A_i$ in $E$ and by $\pi_i$ the corresponding projection from $E$ to $G$.
    • Compute the subgroup $H_i$ of $\mathrm{Aut}(E)$ given by the automorphisms stabilizing $\iota_i(A_i)$.
    • Compute a transversal $(\varphi_1, \psi_1), \dots, (\varphi_t, \psi_t)$ of $H_i$ in $\mathrm{Aut}(A_i) \times \mathrm{Aut}(G)$.
    • For all $j = 1, \dots, t$, add to $L$ the exact sequence given by $\iota_i \circ \varphi_j$, $\psi_j \circ \pi_i$.
4. Return $L$.
```

Remark 3.29. If A is the derived subgroup of E, the description of the extensions is simpler because A is the only subgroup giving rise to such an exact sequence and it is characteristic, so that the domain of the homomorphism φ is the entire automorphism group of E.

Example 3.30. We consider the groups $G = C_2 \times C_2$ and $E = \mathrm{Q}_8$. The only normal subgroup of E with quotient isomorphic to $C_2 \times C_2$ is isomorphic to C_2; thus all the extensions have kernel isomorphic to C_2. Considering the automorphisms, the number of extensions we need to consider is 6 because $\mathrm{Aut}(C_2 \times C_2) \simeq S_3$. However, they are all equivalent: the map $\mathrm{Aut}(Q_8) \to \mathrm{Aut}(C_2 \times C_2)$ induced by the projection is surjective. Thus, in order to extend a field with Galois group $C_2 \times C_2$ to a field with Galois group Q_8 we need to check the solvability of one embedding problem.

Example 3.31. We now consider the groups $G = C_2 \times C_2$ and $E = D_4$. Again, there is only one normal subgroup of order 2 of E, thus the kernel of any extension involving G and E is isomorphic to C_2. This time, the image of the map $\mathrm{Aut}(D_4) \to \mathrm{Aut}(C_2 \times C_2)$ has index 3, meaning that in order to extend a field with Galois group $C_2 \times C_2$ to a field with Galois group D_4 we need to check the solvability of three different embedding problems. In the same notation as in Example 3.25, the three embedding problems depend uniquely on the image of r in $C_2 \times C_2$.

3.3 Criteria for solvability

In this section, we illustrate the main criteria to determine whether an embedding problem is solvable. Let K be a normal extension of a number field K_0 with Galois group G. We consider an embedding problem of a group E over K

$$1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1. \tag{3.2}$$

Denote by $\bar{G}$ the Galois group $\mathrm{Gal}(\bar{K}_0/K_0)$. The inflation homomorphism induced by the projection $\psi\colon \bar{G} \to G$ gives us a way of deciding whether the problem is solvable:

Theorem 3.32 (Hoechsmann, [53, Theorem 3.5.9]). *Let* $c \in \mathrm{H}^2(G, A)$ *be the cohomology class representing the embedding problem in* (3.2)*. Then the embedding problem is solvable if and only if* $\inf_{\bar{G},G}(c)$ *is zero.*

Proof. By Proposition 3.15, we can associate to $\inf_{\bar{G},G}(c)$ the extension

$$1 \to A \to \tilde{E} \to \bar{G} \to 1$$

where $\tilde{E}$ is the pull-back of ψ and π. Assume first that the embedding problem (3.2) has a solution, i.e. there exists a surjective map $\varphi\colon \bar{G} \to E$ such that $\pi \circ \varphi = \psi$. By definition of pull-back, we can lift φ to a section $s\colon \bar{G} \to \tilde{E}$. By Proposition 3.9, this means that $\inf_{\bar{G},G}(\epsilon) = 0$.

Vice versa, assume that $\inf_{\bar{G},G}(\epsilon) = 0$. By Proposition 3.9, there exists a section $s\colon \bar{G} \to \tilde{E}$. The map $\varphi\colon \bar{G} \to E$ given by the composition of s with the projection $\tilde{E} \to E$ gives a solution to the embedding problem.

Even if this criterion is very general, from an algorithmic point of view it is impractical, as it requires the knowledge of the absolute Galois group of K_0.

Split embedding problems We can apply the criterion in the special case of embedding problems represented by a split extension:

Corollary 3.33. *Let* $1 \to A \to E \to G \to 1$ *be an embedding problem over a number field* K*. If it is split, then the embedding problem is solvable.*

Proof. By Proposition 3.9, the cohomology class representing the embedding problem is trivial and it is therefore contained in the kernel of $\inf_{\mathrm{Gal}(\bar{K}_0/K_0),G}$. The claim then follows from Theorem 3.32.

Example 3.34. Every C_3-field can be extended to an A_4-field. Indeed, the corresponding embedding problems are split, because the order of the kernel (isomorphic to $C_2 \times C_2$) is coprime to 3.

Brauer embedding problems The second criterion concerns embedding problems with cyclic kernel.

Definition 3.35. *Let* K *be a number field containing an* n*-th root of unity* ζ_n *and let* $G = \mathrm{Gal}(K/K_0)$*. A Brauer embedding problem is an embedding problem* $1 \to A \to E \to G \to 1$ *over* K *such that* $A \simeq \langle \zeta_n \rangle$ *as* $\mathbf{Z}[G]$*-modules.*

Example 3.36. Let K be a number field with Galois group G and let $1 \to C_2 \to E \to G \to 1$ be an extension of G by C_2. Then the corresponding embedding problem is a Brauer embedding problem, since $-1 \in K$ and any action of G on C_2 is trivial. In particular, the embedding problems involving Q_8 and D_4 as quadratic extensions of a biquadratic field are Brauer embedding problems.

The isomorphism between the kernel of a Brauer embedding problem and the roots of unity in the field allows to embed the kernel as a subgroup of $K^\times$. The inclusion $\langle \zeta_n \rangle \to K^\times$ of the roots of unity in K induces a map $\iota_\zeta \colon \mathrm{H}^2(G, A) \to \mathrm{H}^2(G, K^\times)$.

Theorem 3.37 (Brauer). *Let $1 \to A \to E \to G \to 1$ be a Brauer embedding problem and let $c \in \mathrm{H}^2(G, A)$ be the corresponding cohomology class. Then the embedding problem is solvable if and only if $\iota_\zeta(c)$ is zero.*

Proof. See [45, Theorem 2.4.1].

Consequently, the solvability of a Brauer embedding problem can be reduced to a number theoretical problem: given a cocycle $c \in \mathrm{H}^2(G, K^\times)$, decide whether it is trivial or not.

3.4 Solvability of Brauer embedding problems

Let K be a number field containing the n-th roots of unity. Assume that K is normal over a subfield K_0 and let $G = \mathrm{Gal}(K/K_0)$ be the Galois group. In order to determine if a Brauer embedding problem over K is solvable, we need to check whether the corresponding cohomology class c is zero in $\mathrm{H}^2(G, K^\times)$. In practice, this is not easy, as the group $\mathrm{H}^2(G, K^\times)$ is highly non-trivial and not effectively computable, because $K^\times$ is not finitely generated as an abelian group. Therefore, we approach the problem via a local-global technique.

Remark 3.38. We assume that for every $\sigma \in G$, $c(\sigma, \mathrm{id}) = c(\mathrm{id}, \sigma) = 1$ and that the values of c are roots of unity of K.

Reduction to prime power order kernel Proposition 3.10 allows us to reduce to the case in which n is a prime power. Therefore we assume that the kernel of the embedding problem we are dealing with has order p^k and the values of the cocycle c are roots of unity of order p^k.

Global to local Let $\mathbf{P}$ be the set of places of K_0. Given a place $\mathfrak{p} \in \mathbf{P}$, we denote by $K_\mathfrak{p}$ the completion of K at one of the places of K extending $\mathfrak{p}$ and by $G_\mathfrak{p}$ the Galois group $\mathrm{Gal}(K_\mathfrak{p}/(K_0)_\mathfrak{p})$. As $G_\mathfrak{p}$ corresponds to a subgroup of G and K is naturally embedded in $K_\mathfrak{p}$, we have a map $\iota_\mathfrak{p} \colon \mathrm{H}^2(G, K^\times) \to \mathrm{H}^2(G_\mathfrak{p}, K_\mathfrak{p}^\times)$.

Theorem 3.39 (Albert-Brauer-Hasse-Noether). *Let $c \in H^2(G, K^\times)$ be a cocycle. Then c is zero if and only if its image in $\mathrm{H}^2(G_\mathfrak{p}, K_\mathfrak{p}^\times)$ is zero for all $\mathfrak{p} \in \mathbf{P}$, except at most one.*

Proof. See [53, Theorem 8.1.17].

In terms of maps between the cohomology groups, the theorem reads as follows: given any place $\bar{p} \in \mathbf{P}$, the diagonal map induced by the completions

$$\mathrm{H}^2(G, K^\times) \to \bigoplus_{\substack{\mathfrak{p}\in\mathbf{P} \\ \mathfrak{p}\neq\bar{\mathfrak{p}}}} \mathrm{H}^2(G_\mathfrak{p}, K_\mathfrak{p}^\times)$$

is injective. By means of this theorem, we need to check whether c is split at all primes except one.

Remark 3.40. In the special case $K_0 = \mathbf{Q}$, the best choice for the prime to avoid is p. Indeed, we will see that with this choice we do not have to deal with the wild ramification.

In the rest of the section, we will deal with the following task: given a cocycle $c \in \mathrm{H}^2(G, K^\times)$ and a place $\mathfrak{p}$, decide whether the image of c in $\mathrm{H}^2(G_\mathfrak{p}, K_\mathfrak{p}^\times)$ is trivial or not. We distinguish between the different ramification properties of the places.

Infinite places

Let $\mathfrak{v}_0$ be an infinite place of K_0 and let $\mathfrak{v}$ be a place of K that extends it. We need to distinguish some cases depending on the ramification of $\mathfrak{v}_0$ in K.

- If $\mathfrak{v}_0$ is unramified in K, the cohomology group $\mathrm{H}^2(G_\mathfrak{v}, K_\mathfrak{v}^\times)$ is trivial because the Galois group is the trivial group. As a consequence, c splits at $\mathfrak{v}_0$.
- If $\mathfrak{v}$ is complex and $\mathfrak{v}_0$ is real, the local extension corresponds to $\mathbf{C}/\mathbf{R}$ and the corresponding Galois group is isomorphic to C_2. Recall that the cocycle we are dealing with has values in the roots of unity of order p^k an those roots of unity are contained in K. Since the only roots of unity contained in $\mathbf{R}$ are $1, -1$, it can happen only if $p = 2$ and $k = 1$. In this case, we use the following lemma:

  Lemma 3.41. *Let $\sigma \in \mathrm{Gal}(K/K_0)_\mathfrak{v}$ be the complex conjugation at $\mathfrak{v}$. Then c splits at $\mathfrak{v}$ if and only if $c(\sigma, \sigma) = 1$.*

  Proof. Notice that the Galois group of the completion is given by the identity id and σ and we identify c as an element of $\mathrm{H}^2(C_2, \mathbf{C}^\times)$ with values in the roots of unity of order a power of 2. As $c(\mathrm{id}, \mathrm{id}) = c(\sigma, \mathrm{id}) = c(\mathrm{id}, \sigma) = 1$ by Remark 3.38, the splitting property of c is determined by the value of c at σ. If $c(\sigma, \sigma) = 1$, it splits. Otherwise, $c(\sigma, \sigma) = -1$: since -1 is not a norm of an element of $\mathbf{C}$, c does not split by Proposition 3.21 and Theorem 3.20.

Algorithm 18 Splitting of a cocycle at the infinite place $\mathfrak{v}$

Input: A cocycle $c \in \mathrm{H}^2(G, K^\times)$ with values in the roots of unity of $K^\times$, an infinite place $\mathfrak{v}_0$ of K_0.
Output: Returns true if c is split at $\mathfrak{v}_0$, false otherwise.

```
1. If $\mathfrak{v}_0$ is complex, return true.
```

2. Let $\mathfrak{v}$ be a place extending $\mathfrak{v}_0$. If $\mathfrak{v}$ is real, return true.
3. Compute the complex conjugation $\sigma \in \mathrm{Gal}(K/K_0)$ at $\mathfrak{v}$.
4. If $c(\sigma, \sigma) = 1$, return true. Otherwise, return false.

Unramified primes

We now deal with the finite unramified primes. Since the cocycle has value in the roots of unity of K, the following lemma tells us that we can ignore them:

Lemma 3.42. *Let L/K be an unramified extension of q-adic fields with Galois group G. Let $c \in \mathrm{H}^2(G, L^\times)$ be a cocycle with values in the units of the valuation ring of L. Then c splits.*

Proof. As L/K is unramified, it is a cyclic extension. Let d be its degree and let σ be a generator of G. Then the cocycle splits if and only if $\alpha = \prod c(\sigma, \sigma^i) \in K$ is a norm from L by Proposition 3.21. Since the values of c are units of L, α is a unit of L. The norm is surjective on the units in an unramified extension of local fields by [60, Chapter V, §2, Proposition 1], proving the claim.

Corollary 3.43. *Let $\mathfrak{q}_0$ be a prime ideal of K_0 which is unramified in K and let $\mathfrak{q}$ be a prime ideal of K lying over it. Let $c \in \mathrm{H}^2(G_\mathfrak{q}, K^\times)$ be a cocycle with values in the roots of unity of K. Then c splits.*

Primes not lying over p

Let $\mathfrak{q}_0$ be a prime ideal of K_0 not lying over p and let $c \in \mathrm{H}^2(G_\mathfrak{q}, K_\mathfrak{q}^\times)$ be a cocycle with values in the roots of unity of order a power of p, where $\mathfrak{q}$ is a prime ideal of K lying over $\mathfrak{q}_0$. The first step is to reduce the computation to a tamely ramified extension. We consider a p-Sylow subgroup $(G_\mathfrak{q})_p$ of $G_\mathfrak{q}$ and denote by F its fixed field. The restriction map is injective the p-primary component of the cohomology group by Lemma 3.11 and, since c lies in the p-Sylow subgroup of $\mathrm{H}^2(G_\mathfrak{q}, K_\mathfrak{q}^\times)$, we can study its image in $\mathrm{H}^2((G_\mathfrak{q})_p, K_\mathfrak{q}^\times)$. Moreover, $K_\mathfrak{q}$ is tamely ramified over F, since its degree is coprime to the characteristic of the residue field of F. Let F^{un} be the maximal unramified subextension of $K_\mathfrak{q}/F$. Since the extension is tame, both $K_\mathfrak{q}/F^{\mathrm{un}}$ and F^{un}/F are cyclic extensions; in particular, $(G_\mathfrak{q})_p$ can be generated by two elements.

Lemma 3.44. *Let q be the order of the residue field of F and f be the inertia degree of $K_\mathfrak{q}/F$. There exist elements θ, $\phi \in (G_\mathfrak{q})_p$ such that*

- $\langle \theta, \phi \rangle = (G_\mathfrak{q})_p$
- *θ is a generator of the inertia subgroup,*
- *ϕ generates the quotient by the inertia subgroup,*
- $\phi\theta\phi^{-1} = \theta^{q^f}$.

Proof. See [2, Theorem 9].

Using this presentation, we can establish a criterion to decide whether c splits:

Theorem 3.45. *Let f be the absolute inertia degree of $K_{\mathfrak{q}}$ and let θ and ϕ be generators for $(G_{\mathfrak{q}})_p$ as in Lemma 3.44. Denote by q the order of the residue field of F and let $s = (q^f - 1)/e$. Then c splits in $\mathrm{H}^2((G_{\mathfrak{q}})_p, K_{\mathfrak{q}}^{\times})$ if and only if*

$$\prod_{i=1}^{e-1} c(\theta^i, \theta)^s = 1 \pmod{\mathfrak{q}} \quad \textit{and} \quad c(\phi,\theta)c(\theta^q,\phi)\prod_{i=1}^{q-1} c(\theta^i,\theta) = 1 \pmod{\mathfrak{q}}$$

Proof. By Theorem 3.20, the crossed product algebra $A = (K_{\mathfrak{q}}/F, (G_{\mathfrak{q}})_p, c)$ is split if and only if c is split. Let θ and ϕ be generators for $(G_{\mathfrak{q}})_p$ as in Lemma 3.44. By [35, Theorem 2], A is split if and only if the elements $\lambda, \zeta \in K_{\mathfrak{q}}$ satisfying

$$\mathrm{u}_\theta^e = \zeta, \qquad \mathrm{u}_\phi \mathrm{u}_\theta (\mathrm{u}_\phi)^{-1} = \lambda \mathrm{u}_\theta^q,$$

are such that $\zeta^s = \lambda = 1$ in the residue field of $\mathfrak{q}$, where $\mathrm{u}_\theta, \mathrm{u}_\phi$ are elements of the crossed product algebra as in Definition 3.17. Now, we compute ζ and λ explicitly. Applying inductively the formula $\mathrm{u}_{\theta^s}\mathrm{u}_\theta = c(\theta^s,\theta)\mathrm{u}_{\theta^{s+1}}$, we get

$$\mathrm{u}_\theta^e = c(\theta,\theta)\mathrm{u}_{\theta^2}\mathrm{u}_\theta^{e-2} = \cdots = \prod_{i=1}^{e-1} c(\theta^i,\theta)$$

Therefore, we have an explicit formula for ζ. For λ,

$$\mathrm{u}_\phi\mathrm{u}_\theta = \lambda \mathrm{u}_\theta^q \mathrm{u}_\phi \iff c(\phi,\theta)\mathrm{u}_{\phi\theta} = \lambda c(\theta^q,\phi)\prod_{i=1}^{q-1} c(\theta^i,\theta)\mathrm{u}_{\theta^q\phi}$$

Now, since $\phi\theta\phi^{-1} = \theta^q$, we get

$$\lambda = c(\phi,\theta)c(\theta^q,\phi)\prod_{i=1}^{q-1} c(\theta^i,\theta).$$

Thus, we have an explicit way to decide whether c splits at $\mathfrak{q}$: we compute the values of the cocycle and check if the elements in the statement of the theorem are the identity in the residue field.

Algorithm 19 Splitting of a cocycle at a prime not lying over p

Input: A prime ideal $\mathfrak{q}_0$ of K_0, a cocycle $c \in \mathrm{H}^2(G, K^\times)$ with values in the roots of unity of order a power of p.
Output: Return true if the cocycle splits at $\mathfrak{q}_0$, false otherwise

1. Compute a prime ideal $\mathfrak{q} \subseteq \mathcal{O}_K$ lying over $\mathfrak{q}_0$

```
2. Compute the decomposition group $G_\mathfrak{q}$ of $\mathfrak{q}$ over $K_0$
3. Compute a $p$-Sylow subgroup $(G_\mathfrak{q})_p$ of $G_\mathfrak{q}$
4. Compute generators $\theta$, $\phi$ in $(G_\mathfrak{q})_p$ as in Lemma 3.44
5. If the element as in Theorem 3.45 are both 1 in the residue field of $\mathfrak{q}$,
   return true. Otherwise, return false.
```

Primes lying over p

We now deal with the primes lying over p. Let $\mathfrak{p}_0$ be a prime ideal of K_0 lying over p ramified in K and let $\mathfrak{p}$ be a prime ideal of K lying over $\mathfrak{p}_0$. As we did before, we can reduce to a p-Sylow subgroup $(G_\mathfrak{p})_p$ of $G_\mathfrak{p}$ by Lemma 3.11. Let F be the fixed field of $(G_\mathfrak{p})_p$ and let $\tilde{\mathfrak{p}}_0$ be the prime ideal of F lying over $\mathfrak{p}_0$. If the extension $K_\mathfrak{p}/F$ is unramified, then the cocycle splits by Lemma 3.42. We can therefore assume that the extension is ramified. In the case the extension is cyclic, we can take advantage of Proposition 3.21: the splitting of c is therefore related to the solvability of a norm equation which can be checked as in [1]. In general, the idea is to reduce to this case, as in [57]: we consider a filtration $\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n = (G_\mathfrak{p})_p$ of $(G_\mathfrak{p})_p$ of normal subgroups such that G_{i+1}/G_i is cyclic. Notice that this is possible since the group $(G_\mathfrak{p})_p$ is a p-group, thus nilpotent. Denote by F_i the fixed field of G_i. Then, for each index $i = 0, \cdots, n-1$, we can use Proposition 3.16

$$1 \to \mathrm{H}^2(G_n/G_{i+1}, F_{i+1}^\times) \longrightarrow \mathrm{H}^2(G_n/G_i, F_i^\times) \longrightarrow \mathrm{H}^2(G_{i+1}/G_i, F_i^\times)$$

in order to inductively determine whether c splits. To determine if c splits in every cyclic extension we deal with, we solve the corresponding norm equation.

```
Algorithm 20 Splitting at primes lying over $p$

Input: A prime $\mathfrak{p}_0$ in $K_0$ lying over $p$, a cocycle $c \in H^2(G, K^\times)$ with values
    in the roots of unity of order a power of $p$.
Output: Returns true if $c$ splits, false otherwise.

1. Compute a prime ideal $\mathfrak{p}$ of $K$ lying over $\mathfrak{p}_0$.
2. Compute the decomposition group $G_\mathfrak{p}$ of $\mathfrak{p}$.
3. Compute a $p$-Sylow subgroup $(G_\mathfrak{p})_p$ of $G_\mathfrak{p}$.
4. Find a filtration $\{G_i\}_{i=0,\cdots,k}$ of normal subgroups of $G$ such that $G_{i+1}/G_i$
   is cyclic for all $i$.
5. For $i = 0, \cdots, k-1$
     • Check by solving a norm equation if $c$ splits in the subextension given
       by $G_{i+1}/G_i$. If it does not, return false.
6. Return true.
```

Algorithm

We now summarize to algorithm to decide whether a Brauer embedding problem has a solution.

Algorithm 21 Solvability of a Brauer embedding problem

```
Input: A cocycle $c \in H^2(G, K^\times)$ with values in the roots of unity of order a
    power of $p$.
Output: Returns true if $c$ splits, false otherwise.

1. Compute the real places $L_{\mathrm{inf}}$ of $K_0$ that are ramified in $K$
2. For every $\mathfrak{v}_0$ in $L_{\mathrm{inf}}$, check if $c$ splits at $\mathfrak{v}_0$ using Algorithm 18. If it does
   not, return false.
3. Compute the list $L$ of ramified primes of $K_0$ in $K$.
4. For every prime $\mathfrak{q} \in L$,
    • If $\mathfrak{q}$ lies over $p$, use Algorithm 20, otherwise use Algorithm 19 to de-
      termine whether $c$ splits at $\mathfrak{q}$. If it does not, return false.
5. Return true.
```

Example 3.46. Let K be the totally real subfield of the cyclotomic field $\mathbf{Q}(\zeta_{16})$. The degree of K is 4 and its Galois group is isomorphic to $C_2 \times C_2$. Assume that we want to extend K to a field with Galois group Q_8. The only ramified place of $\mathbf{Q}$ in K is (2). By Corollary 3.43, we only need to test the splitting at (2). However, by Theorem 3.39 we can ignore it and thus the embedding problem is solvable.

Example 3.47. Suppose that we want to embed $K = \mathbf{Q}(\sqrt{5}, \sqrt{13})$ in a Q_8 extension. By Example 3.30, we can consider any extension $1 \to C_2 \to \mathrm{Q}_8 \to C_2 \times C_2 \to 1$. Denote by G the group $C_2 \times C_2$ and identify $(1, 0)$ with the automorphism σ sending $\sqrt{5}$ to $-\sqrt{5}$ and leaving $\sqrt{13}$ fixed and $(0, 1)$ with the automorphism τ sending $\sqrt{13}$ to $-\sqrt{13}$ and leaving $\sqrt{5}$ invariant. We choose the cocycle $c\colon G \times G \to \langle -1 \rangle$ described in the following table

	(0, 0)	(1, 0)	(0, 1)	(1, 1)
(0, 0)	1	1	1	1
(1, 0)	1	-1	1	- 1
(0, 1)	1	-1	-1	1
(1, 1)	1	1	- 1	-1

Since the only places that are ramified in K are (5) and (13), we need to check the splitting at (5) and (13) by Corollary 3.43. Moreover, since by Theorem 3.39 we can ignore one of them, we can check solvability at (5) or (13). We choose to check solvability at (5). Let $\mathfrak{p}$ be any of the prime ideals of K lying over 5. The completion of K at $\mathfrak{p}$ has degree 4 over $\mathbf{Q}_5$, with ramification index 2 and inertia degree 2. We have to apply Algorithm 19. The inertia group G_0 is generated by σ and thus we can take the generators as in Lemma 3.44 to be σ and τ. Thus, it only remains to compute the elements of Theorem 3.45 to see if the cocycle splits. Since $c(\sigma,\sigma) = -1$ and $s = 12$, the first element is 1. Thus we have to check the second element. The product $\prod_{i=1}^{4} c(\sigma^i,\sigma)$ gives 1, while $c(\sigma,\tau)c(\tau,\sigma) = -1$. This means that there is an obstruction and K can't be embedded in a field with Galois group Q_8.

Example 3.48. The field $\mathbf{Q}(\sqrt{-2})$ can't be embedded in a C_4-field. Indeed, the only ramified places are (2) and the infinite place ∞ and by Theorem 3.39 we can ignore one place. Even if algorithmically this is not convenient, for the purpose of the example we ignore the infinite place and check if the cocycle $c\colon C_2 \times C_2 \to C_2$ with values

	id	σ
id	1	1
σ	1	-1

splits at (2), where σ is the non-identical automorphism of $\mathbf{Q}(\sqrt{-1})$. The completion at (2) is cyclic of degree 2 and thus we only have to check if $-1 \in \mathbf{Q}_2$ is a norm of an element of $\mathbf{Q}_2(\sqrt{-2})$. However, -1 is not a norm and thus the cocycle doesn't split.

3.5 Embedding problems with cyclic kernel

In this section, we focus on embedding problems with cyclic kernel: we want to apply the methods we have developed in Section 3.3 to decide their solvability. Let K be a number field which is normal over K_0 with Galois group $G = \mathrm{Gal}(K/K_0)$. We consider the embedding problem given by K and the exact sequence

$$1 \to C_n \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1 \tag{3.3}$$

As usual, we can assume that $n = p^k$ is a prime power by means of Proposition 3.10. If the extension splits, then the problem is solvable by Corollary 3.33. Therefore, we can assume that the embedding problem does not split; in particular, p must divide the order of G. The embedding problem may fail to be a Brauer embedding problem, as the field K may not contain the roots of unity, or the action of the group G on the kernel may differ from the Galois action of the automorphism group on the roots of unity.

Isomorphism with the roots of unity Even if we are dealing with an embedding problem with cyclic kernel of prime power order p^n and the p^n-th roots of unity are contained in K, we might not have a Brauer embedding problem, since A might not be isomorphic to $\langle\zeta_{p^n}\rangle$ as a G-module. To overcome this problem, we reduce to a p-Sylow subgroup G_p of G by means of Proposition 3.11. Notice that the embedding problem given by G is solvable if and only if the embedding problem given by G_p is. The action of G_p on G admits a fixed subgroup:

Lemma 3.49. *Let p be a prime number. Let G be a p-group acting on an abelian p-group A. Then there exists a non trivial subgroup of A fixed by the action of G.*

Proof. See [60, Chapter IX, Lemma 2].

In particular, if A is cyclic of order p, we have the following:

Corollary 3.50. *Let G a p-group acting on a group of order p. Then the action is trivial, i.e. every element acts as the identity.*

Thus, in the case the kernel has order p, G_p acts trivially on both A and the p-th roots of unity, meaning that we have a Brauer embedding problem:

Corollary 3.51. *Let $1 \to C_p \to E \to G \to 1$ be an embedding problem over a field K containing the p-th roots of unity. Then the embedding problem $1 \to C_p \to E_p \to G_p \to 1$ induced by the restriction map $\mathrm{H}^2(G, A) \to \mathrm{H}^2(G_p, A)$ is a Brauer embedding problem.*

Assume now that the kernel does not have order p, so we have an embedding problem

$$1 \to C_{p^n} \xrightarrow{\iota} E_p \xrightarrow{\pi} G_p \to 1 \tag{3.4}$$

with $n \geq 2$ and such that C_{p^n} is not isomorphic to $\langle \zeta_{p^n} \rangle$ as a G-module. In this case, we consider two different Brauer embedding problems:

- The projection $C_{p^n} \to C_p$ induces an homomorphisms $\mathrm{H}^2(G_p, C_{p^n}) \to \mathrm{H}^2(G_p, C_p)$ and consequently the embedding problem

$$1 \to C_p \longrightarrow \tilde{E}_p \longrightarrow G_p \to 1. \tag{3.5}$$

  This is a Brauer embedding problem by Corollary 3.51 and the embedding problem (3.4) is solvable only if (3.5) is.
- Let G_s be the subgroup of G_p given by the elements whose action on the roots of unity and on a generator of the kernel coincide. Then we have the embedding problem given by the restriction of the cocycle to G_s

$$1 \to C_{p^n} \to \pi^{-1}(G_s) \to G_s \to 1 \tag{3.6}$$

  This is by construction a Brauer embedding problem and its solvability gives a necessary condition for the solvability of (3.4).

Thus, the original embedding problem is solvable only if these two are. In some cases, this condition is also sufficient:

Theorem 3.52 (Ledet). *Assume that $n = 4$. Then the embedding problem over K given by* (3.4) *is solvable if and only if the embedding problems given by* (3.5) *and* (3.6) *are solvable.*

Proof. See [44].

Adjoining the roots of unity We now show how to reduce to the case of a field containing the n-th roots of unity. We consider the Galois group $\tilde{G} = \mathrm{Gal}(K(\zeta_n)/K_0)$ and the embedding problem over $K(\zeta_n)/K_0$

$$1 \to A \xrightarrow{\tilde{\iota}} \tilde{E} \xrightarrow{\tilde{\pi}} \tilde{G} \to 1 \tag{3.7}$$

corresponding to the image of (3.3) via the inflation map $\mathrm{H}^2(G, A) \to \mathrm{H}^2(\tilde{G}, A)$ as in Proposition 3.15.

Proposition 3.53. *The embedding problem over K given by* (3.3) *has a solution if and only the embedding problem over $K(\zeta_n)$ given by* (3.7) *has a solution.*

Proof. Since $\tilde{E}$ is the pull-back of π and the projection $p_G \colon \tilde{G} \to G$, the following diagram is commutative:

$$\begin{tikzcd}
\tilde{E} \arrow[r, "\tilde{\pi}"] \arrow[d, "p_E"'] & \tilde{G} \arrow[d, "p_G"] \\
E \arrow[r, "\pi"'] & G
\end{tikzcd}$$

Assume first that the the embedding problem (3.7) has a solution over $K(\zeta_n)$ and let $\varphi\colon \mathrm{Gal}(\bar{K}_0/K_0) \to \tilde{E}$ be the homomorphism given by a solution. Then the composition of φ with p_E gives a solution to the embedding problem over K.

Vice versa, let $\psi\colon \mathrm{Gal}(\bar{K}_0/K_0) \to E$ be a solution to (3.3) over K. Then we have a commutative diagram:

$$\begin{tikzcd}
\mathrm{Gal}(\bar{K}_0/K_0) \arrow[drr, bend left, "\pi_{\tilde{G}}"] \arrow[ddr, bend right, "\psi"'] & & \\
& \tilde{E} \arrow[r, "\tilde{\pi}"'] \arrow[d, "p_E"'] & \tilde{G} \arrow[d, "p_G"] \\
& E \arrow[r, "\pi"'] & G
\end{tikzcd}$$

Since $\tilde{E}$ is the pull-back of p_g and π, we get a map $\tilde{\psi}\colon \mathrm{Gal}(\bar{K}_0/K_0) \to E$, which is the desired solution for the embedding problem over $K(\zeta_n)$.

This proposition allows us to reduce to the case of a Brauer embedding problem in many cases in exchange for an increase in the degree of the field we are dealing with. However, in some particular instances it is possible to avoid the computation of the embedding problem (3.7), as we can predict its behaviour. Assume that we have an embedding problem with cyclic kernel of prime degree p and that all the prime ideals of K_0 that are ramified in K are such that their completions contain the p-roots of unity.

Remark 3.54. If $K_0 = \mathbf{Q}$, the latter condition means that the ramified primes are congruent to 1 modulo p.

In this case, the corresponding embedding problem over $K(\zeta_p)$ induced by the restriction to the p-Sylow subgroup is a Brauer embedding problem by Corollary 3.51. However, the roots of unity are already contained in the completion of K at the ramified primes.

Lemma 3.55. *Let K/K_0 be a normal extension of number fields and let $\mathfrak{p}$ be a prime ideal of K that splits completely in $K(\zeta_p)$. Let $\tilde{\mathfrak{p}}$ be a prime ideal of $K(\zeta_p)$ lying over $\mathfrak{p}$. Then $K_{\mathfrak{p}}$ is isomorphic to $K(\zeta_p)_{\tilde{\mathfrak{p}}}$.*

By means of this lemma, we know that the decomposition group of $\mathfrak{p}$ is isomorphic to the decomposition group of $\tilde{\mathfrak{p}}_0$. Moreover, the restriction homomorphism res: $\mathrm{Gal}(K(\zeta_p)/K_0) \to \mathrm{Gal}(K/K_0)$ induces an isomorphism between the p-Sylow subgroups of $\mathrm{Gal}(K(\zeta_p)/K_0)$ and $\mathrm{Gal}(K/K_0)$, as $[K(\zeta_p) : K]$ is coprime to p. As the action of the elements of a p-Sylow subgroup of $\mathrm{Gal}(K(\zeta_p)/K_0)$ on the p-th roots of unity is trivial, we can therefore test if there is an obstruction without actually computing $K(\zeta_p)$.

Algorithm 22 Embedding problem with cyclic kernel

```
Input: An embedding problem $1 \to C_n \to E \to G \to 1$ over a number field
    $K$.
Output: Returns false if it finds an obstruction, true otherwise.

 1. Factor $n = \prod p_i^{k_i}$.
 2. For every prime $p_i$ dividing $n$,
    a) Construct the corresponding embedding problem with kernel of order
       $p_i^{k_i}$.
    b) If the roots of unity of order $p_i^{k_i}$ are not in the field, replace $K$ by
       $K(\zeta_{p_i^{k_i}})$ and the embedding problem consistently.
    c) If the embedding problem is not a Brauer embedding problem,
       • Pass to the $p_i$-Sylow subgroup of $G$ and the corresponding extension
             $$1 \to C_{p_i^{k_i}} \to E_{p_i} \to G_{p_i} \to 1$$
       • Use the strategy explained above to compute the two Brauer embedding
         problem induced by the projection $C_{p_i^{k_i}} \to C_{p_i}$ and the
         subgroup of $G_{p_i}$ that acts on $C_{p_i^{k_i}}$ in the same way as it acts on
         the roots of unity.
       • Check their solvability using Algorithm 21. If any of them is not
         solvable, return false.
    d) Otherwise, apply Algorithm 21 to the embedding problem. If it is not
       solvable, return false.
 3. All the embedding problems we analysed were solvable. Return true.
```

3.6 Deciding the existence of an extension

In this section, we illustrate the algorithm to decide whether a number field K with Galois group G over K_0 can be extended to a field L abelian over K having Galois group E over K_0. Notice that the reduction to cyclic embedding problems give only necessary conditions and the algorithm might return true even if such an extension does not exists. However, if the algorithm returns false, an extension does not exist.

The idea is to reduce to embedding problems with cyclic kernel and then apply Algorithm 22.

List all the embedding problems The first step is to list all the embedding problem involving E and G by means of Algorithm 17.

Reduction to kernel of prime power order Let $1 \to A \to E \to G \to 1$ be one of the embedding problems and let $c \in \mathrm{H}^2(G, A)$ be the corresponding cocycle. By Proposition 3.10, the embedding problem given by c is solvable if and only if the embedding problems corresponding to every p-Sylow subgroup of A is.

Split embedding problem As we have seen, a split embedding problem is always solvable by Corollary 3.33.

Cyclic kernel In the case the kernel is cyclic, we have seen how to check if the embedding problem is solvable in Section 3.5.

Reduction to embedding problem with cyclic kernel Let $1 \to A \to E \to G \to 1$ be the embedding problem we are dealing with. By hypothesis, the kernel is a non-cyclic p-group and we try to decompose the problem into extensions with cyclic kernels. We first reduce to a p-Sylow subgroup G_p of G by means of Lemma 3.11 and denote by $\tilde{E}$ the corresponding extension. As G_p and A are p-groups, the fixed points of A under the action of G_p are non trivial by Lemma 3.49. This implies that the composition factors of A as a G_p-module are cyclic of order p. As a consequence, there is at least a subgroup H of A such that A/H is cyclic and normal in $\tilde{E}$. In practice, we enumerate all the subgroups with these properties by looking at the normal subgroups N_i of $\tilde{E}$ contained in A and then testing for which of them A/N_i is a cyclic abelian group; among these, we take the minimal elements by containment, as otherwise we would get redundant embedding problems. Let $N_1, \dots, N_s$ be the subgroups found using this procedure. Each of them induces an embedding problem

$$1 \to A/N_i \longrightarrow \tilde{E}/N_i \longrightarrow G_p \to 1$$

which by hypothesis has cyclic kernel. Moreover, the original embedding problem is solvable only if these embedding problems are solvable.

Algorithm 23 Reduction to an embedding problem with cyclic kernel

Input: An embedding problem $1 \to A \to E \to G \to 1$ over K, where A is a p-group.

```
Output: Embedding problems with cyclic kernels that are solvable if and only
    if the input one is.

 1. Compute a $p$-Sylow subgroup $G_p$ of $G$ and pass to the corresponding
    extension
        $1 \to A \to E_p \to G_p \to 1$
 2. Compute the list $L$ of normal subgroups $N_1, \dots, N_s$ of $A$ such that $A/N_i$
    is cyclic.
 3. Remove from $L$ the subgroups that are not normal in $E_p$.
 4. Create the list $L_1$ of subgroups in $L$ that are minimal under containment.
 5. Return the embedding problems corresponding to the subgroups in $L_1$.
```

Example 3.56. Consider the group $E = S_4$, the symmetric group of order 24, and assume that we want to find it as an extension of a S_3-field. The only possible kernel of an extension involving S_4 and S_3 is the subgroup of S_4 isomorphic to $C_2 \times C_2$. Thus, we want to use the algorithm in order to reduce to extensions with cyclic kernel. First, we reduce to a 2-Sylow subgroup of S_3, which is isomorphic to C_2, and we now have to consider the induced extensions

$$1 \to C_2 \times C_2 \to D_4 \to C_2 \to 1$$

By Lemma 3.49 there is a subgroup isomorphic to C_2 which is invariant (and it is unique, since the action can't be trivial). Thus, we check the restriction to this subgroup for obstructions. However, the corresponding extension is

$$1 \to C_2 \to C_2 \times C_2 \to C_2 \to 1$$

which is split.

The algorithm We now present the complete algorithm to check whether a field admits an extension with given Galois group.

Algorithm 24 Test for obstructions

```
Input: A number field $K$ with Galois group $G$, an extension $E$ of $G$.
Output: Returns the list of embedding problems involving $E$ and $G$ that are
    solvable up to equivalence.

 1. Use Algorithm 17 to list all the embedding problems involving $E$ and $G$.
 2. Initialize an empty list of embedding problems $L$.
 3. For each embedding problem $1 \to A \to E \to G \to 1$,
     a) If $A$ is cyclic,
         • Apply Algorithm 22. If it returns true, add the embedding problem
           to $L$.
     b) Use Algorithm 23 to produce a list $L_1$ of embedding problems with
        cyclic kernel.
```

c) For each embedding problem in L_1, apply Algorithm 22. If the algorithm returns true for all of them, add the embedding problem $1 \to A \to E \to G \to 1$ to L.

4. Return L.

The algorithm has been implemented in the number theory package Hecke [25] using the system GAP [28] as support for the group theory, except for Algorithm 20 in the case of a non-cyclic extension. Notice that our test is not exhaustive: the field might not admit an extension with the desired Galois group even if the algorithm returns true. Nevertheless, the algorithm seems to be indispensable for the task: depending on the group, the number of fields for which we find an obstruction might be quite large. To support this statement, we provide here some numerical data. We consider the following groups:

- the quaternion groups Q_8, Q_{16}, Q_{32} of order 8, 16 and 32;
- the dihedral groups D_4, D_8, D_{16} of order 8, 16 and 32;
- the semidihedral groups SD_{16}, SD_{32} of order 16 and 32.

These are all the groups of order 8, 16 and 32 that have a biquadratic extension as a maximal abelian subfield over $\mathbf{Q}$. Given all the biquadratic fields up to absolute discriminant $1.3 \cdot 10^{11}$, we checked for how many of them we find an obstruction. The results are shown in the following tables: under the label of each group, we write the number of fields for which our method does not find any obstructions and the corresponding percentage with respect to the total number.

- Order 8:

# fields	Q_8	D_4
1046530	34932	344717
	3.337888%	32.939046%

- Order 16:

# fields	SD_{16}	Q_{16}	D_8
1046530	211067	50860	183996
	20.168270%	4.859870%	17.581531%

- Order 32:

# fields	SD_{32}	Q_{32}	D_{16}
1046530	156198	38294	146260
	14.925324%	3.659140%	13.975710%

CHAPTER 4

From group theory to number theory

Although the building blocks for the algorithm have already been presented in the previous chapters, we have not yet exploited the relation between the structure of the group we want to realize and the tower of subfields we compute. For instance, information coming from the group allows us to construct fields as composite of subfields or to discard some of the abelian extensions before the computation of a defining equation.

4.1 Choice of the series

The choice of the series of the group G that we use as input in Algorithm 1 is crucial for its efficiency. In principle, no additional hypotheses on the series are required except from normality. However, depending on the chosen series, it might be possible to obtain the same field twice: there exist number fields K with two normal subfields F_1, F_2 such that $\mathrm{Gal}(K/F_1) \simeq \mathrm{Gal}(K/F_2)$ and $\mathrm{Gal}(F_1/\mathbf{Q}) \simeq \mathrm{Gal}(F_2/\mathbf{Q})$. In terms of subgroups, this means that we have normal subgroups H_1, H_2 of G such that $H_1 \simeq H_2$ and $G/H_1 \simeq G/H_2$. Such subgroups are sometimes called *series equivalent.*

Example 4.1. Consider a number field K with Galois group $G = \mathrm{Q}_8$, the quaternion group of order 8. The subgroups of order 4 of G are all series equivalent, as the automorphisms of G act transitively on them.

Thus, we restrict to normal series whose subgroups are not series equivalent to any other subgroup of G. In particular, the subgroups appearing in the series are characteristic subgroups of G (i.e. invariant under the action of the automorphism group of G).

We now give two examples of series that can be used in the construction. For specific groups, it might be possible to choose special series that perform better.

The derived series A good choice for the series is the so-called derived series, defined recursively as

$$\begin{cases} G_0 = G \\ G_{i+1} = G_i' \end{cases}$$

where G_i' denotes the commutator subgroup of G_i. The properties of the commutator subgroups imply that the use of this series maximizes the degree of the abelian extensions we have to construct at every step. In particular, the length of the series is minimal among all the normal series with abelian quotients. Moreover, it is easy to see that the commutator subgroup doesn't admit series equivalent subgroups, meaning that we will not have redundancy in our construction.

Degree minimizing series Even if the properties of the derived series are desirable, it is not the best general choice. Indeed, for the purpose of our algorithm, we would like to minimize the degree of the intermediate fields we construct. In order to achieve this result, we construct a series as follows. We consider the set S of subgroups of G which do not admit a series equivalent subgroups (in particular, S is contained in the set of characteristic subgroups). Notice that S is not empty, as the subgroups of the derived series have this property. We define recursively a (reversed) chain of subgroup starting from $G_0 = \{e\}$; G_{i+1} is any of the maximal subgroups in S (with respect to containment) containing G_i such that G_{i+1}/G_i is abelian. If more than one subgroup has these properties, then we pick any of the subgroups for which the exponent of the abelian group G_{i+1}/G_i is minimal. A series constructed this way has all the relevant properties we want: the subgroups do not admit by definition series equivalent subgroups and, among all the series with this property, it minimizes the degree of the last subfield we need to construct in our method. Unfortunately, it might be longer than the derived series, as the following example shows.

Example 4.2. Let G be the group $C_9 \rtimes C_6$, where C_6 acts faithfully on C_9. The derived subgroup of G is isomorphic to C_9 and the derived series has length 2. On the other hand, G has a unique subgroup H isomorphic to $C_3 \times C_3$, so it does not admit any series equivalent subgroups. Since the exponent of H is 3, we prefer it over the derived subgroup. However, G/H is isomorphic to S_3 and so the series has length 3.

Example 4.3. Consider the group $G = D_4$, the dihedral group of order 8, generated by elements r, s with presentation $r^4 = e$, $s^2 = e$, $rs = sr^3$. The derived subgroup of G is the subgroup generated by r^2 and the derived series is therefore

$$\{e\} \subset \langle r^2 \rangle \subset G.$$

Let K be a number field with Galois group G. The series identifies then by Galois correspondence a subfield F with Galois group isomorphic to $G/\langle r^2\rangle \simeq C_2 \times C_2$ and this subfield is the only one with this property.

We now compute a series following the definition we have given above. The characteristic subgroups of G that do not admit series equivalent subgroups are the trivial subgroups, $\langle r\rangle$, $\langle r^2\rangle$ and $\langle r^2, s\rangle$. Following the construction, we take $G_0 = \{e\}$, $G_1 = \langle r^2, s\rangle$ and $G_2 = G$. The choice of G_1 was unique as even if there are two different subgroups of order 4 (namely $\langle r\rangle$ and $\langle r^2, s\rangle$), G_1 is the unique one with minimal exponent (the exponent of $\langle r\rangle$ is 4, the exponent of $\langle r^2, s\rangle$ is 2). This means that we would try to construct a field with Galois group D_4 as an extension of a quadratic field by a $C_2 \times C_2$ extension.

4.2 Group recognition

The most crucial issue in the algorithm is to understand if a given abelian extension L of K has the correct Galois group. In general, this task can be solved by computing the so-called fundamental class ([63, Theorem 11.5]). However, the literature on this topic suggests that its computation is too expensive for our purposes and further work should be done in that direction [9]. Thus we preferred using simpler criteria that perform well in practice, even though they are not sufficient in general to predict the Galois group.

Sylow decomposition

The first observation that we make is that we can reduce to the case of an extension of prime power degree. Let L be an abelian extension of K which is normal over $\mathbf{Q}$. Then we have an exact sequence

$$1 \to \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbf{Q}) \longrightarrow \mathrm{Gal}(K/\mathbf{Q}) \to 1.$$

The extension corresponds to a class $c \in \mathrm{H}^2(\mathrm{Gal}(K/\mathbf{Q}), \mathrm{Gal}(L/K))$, which encodes the isomorphism class of $\mathrm{Gal}(L/\mathbf{Q})$. Consider the decomposition of $\mathrm{Gal}(L/K)$ as a sum of Sylow subgroups $\mathrm{Gal}(L/K) = \bigoplus \mathrm{Gal}(L_p/K)$, so that L_p is the maximal subextension of L/K of p-power degree. Such a decomposition induces exact sequences for every p:

$$1 \to \mathrm{Gal}(L_p/K) \longrightarrow \mathrm{Gal}(L_p/\mathbf{Q}) \longrightarrow \mathrm{Gal}(K/\mathbf{Q}) \to 1$$

which is the explicit interpretation of the map between the cohomology groups

$$\mathrm{H}^2(\mathrm{Gal}(K/\mathbf{Q}), \mathrm{Gal}(L/K)) \to \bigoplus \mathrm{H}^2(\mathrm{Gal}(K/\mathbf{Q}), \mathrm{Gal}(L_p/K))$$

given by Proposition 3.10.

Lemma 4.4. *Let L be an abelian extension of K which is normal over $\mathbf{Q}$. For every prime number p dividing the degree of L over K, let L_p be the maximal subextension of p-power degree. Then the Galois group* $\mathrm{Gal}(L_p/\mathbf{Q})$ *is determined by the isomorphism class of* $\mathrm{Gal}(L/\mathbf{Q})$.

Proof. Follows from the argument above and Proposition 3.10.

Thus, we have a necessary condition for the extension to have the correct Galois group.

Split extensions

Let G be the Galois group of the number field K and assume we are searching for extensions with Galois group E which is isomorphic to $A \rtimes G$ for an abelian group A. Assume additionally that the order of G and A are coprime. In this case, we can predict whether an extension has the correct Galois group, since the isomorphism class of the semidirect product is determined by the action of G on A (by Corollary 3.3, the cohomology group $\mathrm{H}^2(G, A)$ is trivial). Let now L be an abelian extension of K with Galois group $\mathrm{Gal}(L/K) \simeq A$. We assume that L is given by a congruence subgroup $A_{\mathfrak{m}}$ of the ray class group $\mathrm{Cl}_{\mathfrak{m}}$ and that it is normal over $\mathbf{Q}$. This means that the Galois group $\mathrm{Gal}(L/\mathbf{Q})$ fits in the exact sequence

$$1 \to \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbf{Q}) \longrightarrow \mathrm{Gal}(K/\mathbf{Q}) \to 1$$

The Artin map $\Phi_{L/K}$ gives us a canonical isomorphism between $\mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}}$ and $\mathrm{Gal}(L/K)$. Since we are assuming that L is normal over $\mathbf{Q}$, $\mathrm{Gal}(K/\mathbf{Q})$ acts on $\mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}}$. Precisely, $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ acts by sending the class $[I]$ to $[\sigma(I)]$. This action translates via the Artin map to the conjugation on $\mathrm{Gal}(L/K)$ and allows us to determine the group theoretical action, as we did in Section 2.2.

In order to apply this strategy in an effective way, it has to be applied after decomposing $\mathrm{Gal}(L/K)$ into Sylow subgroups and following Lemma 4.4. The following example shows why this is crucial:

Example 4.5. Consider the non trivial semidirect product $G = C_3 \rtimes Q_8$ and assume we are constructing number fields with Galois group G using the derived series. As the derived subgroup of G is isomorphic to C_6, the construction process requires two steps: first, we need $C_2 \times C_2$ extensions of $\mathbf{Q}$ and then extend these fields with C_6 extensions. G is not a semidirect product of $C_2 \times C_2$ and C_6, thus we can't apply directly the strategy we explained above. However, if we consider the group extension corresponding to the subgroup of C_6 isomorphic to C_3 is isomorphic to the dihedral group D_6, which is a semidirect product of $C_2 \times C_2$ and C_3. Thus, we can apply the criterion above in order to understand if an extension might give rise to the correct Galois group.

Identification of Galois group

We now focus on the final step for the recognition: we assume that we have an abelian extension L/K and a defining polynomials for the corresponding relative extension. Moreover, by applying the method we discussed in Section 2.3, we can assume that we have generators for the automorphism group of $L/\mathbf{Q}$ at our disposal.

In this case, we realize the Galois group as a permutation group and then check if its isomorphism class is correct.

Realizing the automorphism group as a permutation group In our construction, the field L is given as an extension of K by some linearly disjoint cyclic extensions $L_1, \dots, L_s$ of K. In practical terms, K is an extension of $\mathbf{Q}$, represented as $\mathbf{Q}[x]/(f(x))$ for a given monic polynomial f, and L is given by monic polynomials $g_1, \dots, g_s$ so that

$$L \simeq {}^{\mathbf{Q}[x, y_1, \dots, y_s]}\big/_{(f(x), g_1(x, y_1), \dots, g_s(x, y_s))}.$$

Under this assumption, an automorphism is uniquely determined by the image of the variables $x, y_1, \dots, y_s$. Assume first that we have all the automorphisms $\varphi_1, \dots, \varphi_n$ in $\mathrm{Gal}(L/\mathbf{Q})$. Then we could associate to every automorphism φ_k a permutation $\sigma \in S_n$, where $\sigma(i)$ is equal to the index j such that $\varphi_k \varphi_i = \varphi_j$. However, in order to perform this strategy directly, we would need the entire set of automorphisms and we would need to compose the automorphisms. Both these computation might be too expensive, in particular because we would need to perform them for every candidate field. In order to avoid these expensive computation, we perform the compositions modularly.

Proposition 4.6. *Let p be a prime number such that p doesn't divide the discriminant of f and that doesn't divide $N_{K/\mathbf{Q}}(\operatorname{disc} g_i)$ for any i. Then the projection $\mathcal{O}_L \to \mathcal{O}_L/p\mathcal{O}_L$ induces an isomorphism between* $\mathrm{Gal}(L/K)$ *and* $\mathrm{Aut}(\mathcal{O}_L/p\mathcal{O}_L)$ *as a $\mathbf{F}_p$-algebra.*

Proof. First of all, we notice that $\mathcal{O}_L/p\mathcal{O}_L$ is isomorphic as a $\mathbf{F}_p$-algebra to $\mathbf{F}_p[x, y_1, \dots, y_s]/(\bar{f}(x), \bar{g}_1(x, y_1), \dots, \bar{g}_s(x, y_s))$ because of the choice of p. Thus, an automorphism $\psi \in \mathrm{Aut}(\mathcal{O}_L/p\mathcal{O}_L)$ must send x to a root p_i of $\bar{f}$ and y_i to a root of $\bar{g}_i(p_i, y_i)$. As the field L is normal over $\mathbf{Q}$, this means that the projection induces a surjection onto the automorphism group. In order to show injectivity, we need to show that the images in $\mathcal{O}_L/p\mathcal{O}_L$ of the conjugates in L of $x, y_1, \dots, y_s$ are all distinct. The hypotheses implies that the roots $x = \bar{\alpha}_1, \dots, \bar{\alpha}_t$ of $\bar{f}(x)$ are distinct. As the norm of the discriminant of g_i correspond to the discriminant of the norm of g_i, the same holds for the g_i, proving the claim.

Thus, we can compute a representation of $\mathrm{Gal}(L/K)$ as a permutation group by composing with the projection modulo $p\mathcal{O}_L$ for a suitable p satisfying the hypotheses of the theorem. Computing the automorphism group of $\mathcal{O}_L/p\mathcal{O}_L$ is then straightforward. As $\mathcal{O}_L/p\mathcal{O}_L$ is isomorphic to the quotient $\mathbf{F}_p[x, y_1, \dots, y_s]/(\bar{f}(x), \bar{g}_1(x, y_1), \dots, \bar{g}_s(x, y_s))$, composition of automorphisms corresponds to composition of polynomials modulo the ideal $(\bar{f}(x), \bar{g}_1(x, y_1), \dots, \bar{g}_s(x, y_s))$. The particular choice of the polynomial defining the field implies that $\bar{f}(x), \bar{g}_1(x, y_1), \dots, \bar{g}_s(x, y_s)$ is a Gröbner basis for the ideal and thus we have unique representation for elements in $\mathcal{O}_L/p\mathcal{O}_L$.

Remark 4.7. The representation of $\mathrm{Gal}(L/\mathbf{Q})$ into S_n that we get has degree equal to the order of $\mathrm{Gal}(L/\mathbf{Q})$. One could get a representation into a smaller symmetric group by acting on a primitive element of a non-normal subfield having L as a Galois closure. Depending on the structure of the Galois group, it could be easy to find such an element; however the algorithm we described performs quite well and in practice suffices for our purpose.

Example 4.8. Let L be the number field generated by $\sqrt[3]{2}$ over $\mathbf{Q}(\zeta_3)$. Then we would represent $\mathrm{Gal}(L/\mathbf{Q})$ as a subgroup of S_6 looking at the action of $\mathrm{Gal}(L/\mathbf{Q})$ over the tuple $(\zeta_3, \sqrt[3]{2})$. However, the action on the orbit of $\sqrt[3]{2}$ would give us an embedding of $\mathrm{Gal}(L/\mathbf{Q})$ into S_3.

Check the isomorphism class The identification of the isomorphism class of $\mathrm{Gal}(L/K)$, given as a permutation group, is the second step. This is a purely group theoretic task and we are not going to discuss the low level function. Notice that we just need to check if the isomorphism class of the group is correct. In our implementation, we are thus calling the "IdGroup" function from GAP [28]. Some improvements upon the standard algorithm are possible even in this step of the algorithm, at a higher level, by applying Lemma 4.4. First, we order the prime divisors $p_1, \dots, p_l$ of the order of $\mathrm{Gal}(L/K)$ by ascending degree $[K(\zeta_{p_i^{s_i}}) : K]$. Then, for every p, we compute defining polynomial for L_p and check the isomorphism class of $\mathrm{Gal}(L_p/\mathbf{Q})$. If this subextension has the wrong Galois group, then we are sure that L doesn't have the correct Galois group and we discard the field; otherwise, we continue with the next Sylow subgroup. Notice that we don't need to check the Galois group of L_p if p doesn't divide the degree of K, as in this case the corresponding extension is a split extension.

At the end, we might need to check anyway the isomorphism class of $L/\mathbf{Q}$. Indeed, the isomorphism classes of the extensions $L_p/\mathbf{Q}$ are not enough to determine the isomorphism classes of $L/\mathbb{Q}$.

Example 4.9. We consider the groups G, H with identification number $(24, 6)$ and $(24, 8)$ in the Small Group library ([6], available in GAP [28]). Those group have derived subgroup isomorphic to C_6, and the quotients of G and H by the Sylow subgroups of the derived subgroup are isomorphic to D_4 and D_6 respectively for both G and H.

In cohomological terms, $\mathrm{H}^2(C_2 \times C_2, C_6)$ decomposes as $\mathrm{H}^2(C_2 \times C_2, C_2) \oplus \mathrm{H}^2(C_2 \times C_2, C_3)$. The groups G and H correspond to two different classes c_1 and c_2. As $H^2(C_2 \times C_2, C_3)$ is trivial, $\mathrm{H}^2(C_2 \times C_2, C_6)$ is isomorphic to $\mathrm{H}^2(C_2 \times$

$C_2, C_2)$; denote by $\bar{c}_1$ and $\bar{c}_2$ the image of c_1 and c_2 under this isomorphism. As we discuss above, the classes $\bar{c}_1$ and $\bar{c}_2$ must correspond to an extension isomorphic to D_4 and there are two different classes in $\mathrm{H}^2(C_2 \times C_2, C_2)$. Thus, establishing that the extension L_2 has Galois group D_4 does not determine the cohomology class.

4.3 Control over the Galois group

In this section, we focus on some restriction imposed by the group structure on the conductors of abelian extensions. These constraints are crucial for certain groups, as they provide a way to detect the fact that a field does not admit an extension satisfying the requirements.

Analysis of the ramification groups

Let L be an abelian extension of K with absolute Galois group E. Let $\mathfrak{p}$ be a prime ideal of K and let $\mathfrak{q}$ be a prime ideal of L lying over $\mathfrak{p}$. The projection $\pi \colon E \to G$ behaves well with respect to the decomposition groups and the inertia groups, as we have seen in Lemma 1.6.

This gives us constraints in the computation of the conductors of abelian extensions, as the following examples show.

Example 4.10. Let L be a normal number field with Galois group Q_8, the quaternion group, and let K be its normal subfield with Galois group $C_2 \times C_2$. Let p be a prime number ramified in K, let $\mathfrak{p}$ be a prime ideal of K lying over p and $\mathfrak{q}$ be a prime ideal of L over $\mathfrak{p}$. Since the preimage of every non trivial subgroup of $C_2 \times C_2$ under the projection $\pi \colon Q_8 \to C_2 \times C_2$ has order greater than the subgroup, the extension L/K must be ramified at $\mathfrak{p}$. This means that the conductor of L/K must be divisible by all the primes that are already ramified in K.

Example 4.11. Let L be a normal number field with Galois group S_3, the symmetric group of order 6, and let K be its normal subfield with Galois group C_2. Let p be a prime number different from $2, 3$ that is ramified in K. As the inertia group of a tamely ramified prime is cyclic, p cannot be totally ramified in L. This means that the conductor of L/K cannot be divisible by the primes dividing the discriminant of K, with the exceptions of 2 and 3.

In general, we consider all the embedding problems involving G and E that are solvable in the sense of Chapter 3, up to cohomological equivalence. Then, for every prime number p ramified in K, we consider a prime ideal $\mathfrak{p}$ lying over p and compute its inertia group G_0 in K. For every embedding problem, we compute the set of possible preimages of the inertia group. If all of them have the same order as G_0, then $\mathfrak{p}$ must be unramified in L. Instead, if all of them have order greater than G_0, $\mathfrak{p}$ must ramify further in L.

Embedding in the symmetric group

Let K be a normal number field and let f be the minimal polynomial of the given primitive element of K. Then it is well known that the action of the automorphisms on K restricts to an action on the roots of f in K and that this gives an embedding of $\mathrm{Gal}(K/\mathbf{Q})$ into the symmetric group S_n, where n is the degree of f. In particular, we have the following:

Lemma 4.12. *Let K be a normal number field and let $H < S_n$ be the image of $\mathrm{Gal}(K/\mathbf{Q})$ given by the action of $\mathrm{Gal}(K/\mathbf{Q})$ on the roots of f in K. Then H is contained in the alternating group A_n if and only if the discriminant of f is a square in $\mathbf{Q}$.*

Proof. Denote by $\alpha_1, \ldots, \alpha_n$ the roots of f in K. Then $\operatorname{disc} f = \prod(\alpha_i - \alpha_j)^2$. If $H \langle A_n$, then every element of $\mathrm{Gal}(K/\mathbf{Q})$ fixes $\prod(\alpha_i - \alpha_j)$, proving that the discriminant is a square. Conversely, if $\prod(\alpha_i - \alpha_j)$ is in $\mathbf{Q}$, then every element in $\mathrm{Gal}(K/\mathbf{Q})$ fixes the product. Therefore H must be contained in A_n.

Thus, knowing the information about the containment of H in A_n gives us a condition on the discriminant of the number field K. However, the way we have stated the theorem does not allow yet to get any restrictions on the conductors, as H depends on the choice of f. The action of $\mathrm{Gal}(K/\mathbf{Q})$ on the roots of f corresponds to the Cayley representation of G. This comes from the following bijection between the roots and G: given a root α_i of f, we map it to the unique automorphism of G sending α_1 to α_i.

As a consequence, we get the following result:

Proposition 4.13. *Let K be a normal number field with Galois group G. Then the discriminant of K is a square if and only if the image of the Cayley representation of G is contained in the alternating group.*

Proof. Follows from the discussion above and from the fact that the discriminant of a polynomial differ from the discriminant of the field by a square.

Example 4.14. Let G be the quaternion group Q_8. The image of the Cayley representation of G in S_8 is contained in A_8; thus the discriminant of a field having Galois group Q_8 is a square. Let L be a field with Galois group G and let K be its subfield with Galois group $C_2 \times C_2$. Then the discriminant of L can be factored as $\operatorname{disc} L = \operatorname{disc} K^2 N(\operatorname{disc} L/K)$ by [60, Chapter III, Proposition 8]. Since $\operatorname{disc} L$ is a square, the norm of the relative discriminant $N(\operatorname{disc} L/K)$ must be a square too. Assume that 2 is totally ramified in K. Then the norm of the unique prime $\mathfrak{p}$ lying over 2 will be 2, thus the exponent of $\mathfrak{p}$ in the factorization of $\operatorname{disc} L/K$ must be even. However, the valuation at $\mathfrak{p}$ of the discriminant is equal to twice the valuation at $\mathfrak{p}$ of the conductor minus two, which is even if and only the valuation at $\mathfrak{p}$ of the conductor is even.

We implemented this criterion in the case of cyclic extensions of prime degree. Let K be a normal number field with Galois group G and assume we want to find cyclic extensions of K of prime degree p with absolute Galois group E. First of all, by computing the Cayley representation of E in $S_{|E|}$, we know whether the discriminant of the extension must be a square or not. Then, we distinguish two cases. If p is different from 2, then the norm of the discriminant of the extension we are searching for will always be a square. Thus,

- if the discriminant of the extension must be a square, we check if the discriminant of K is a square; if it is, we don't have any condition on the discriminant; otherwise, such an extension can not exist;
- if the discriminant should not be a square, we check if the discriminant of K is a square; if it is not, we don't have any condition on the discriminant; otherwise, such an extension can not exist.

Assume now $p = 2$. In this case, we only need to care about the norm of the relative discriminant. If the number of prime ideals of K lying over 2 is even or their inertia degree is even, the discriminant will always be a square. So assume that the number of prime ideals is odd and the same is true for their inertia degree. Then the discriminant will be a square depending only on the exponent of the prime ideals in the factorization of the finite part of the conductor: if it is odd, then the discriminant won't be a square, otherwise it will be.

Ramification at infinite places

Given a totally complex field K with Galois group G, the complex conjugations represent a conjugacy class of involutions of G. Let $G = G_0 \supsetneq G_1 = G' \supsetneq G_2 \supsetneq \dots \supsetneq G_{n-1} \supsetneq G_n = \{e\}$ be the given series of G. Depending on the properties of the subgroups, we can predict the behaviour of the infinite places in the subextensions we construct by means of the following lemma:

Lemma 4.15. *Let K be a number field with Galois group isomorphic to G. Let H be the subgroup of G generated by all the elements of order 2. Then the field corresponding to H under the Galois correspondence is totally real.*

Proof. If K itself is totally real, there is nothing to prove. Assume that K is totally complex. Let F be the fixed field of H. Notice that H contains the complex conjugations of K. Given an embedding $\sigma\colon K \to \mathbf{C}$, we have that the image of F under σ is fixed by the complex conjugation. This means that F is totally real, as claimed.

Assume now that G_i contains all the involutions of G. By means of the lemma, the fixed field of G_i must be totally real. This easy observation provide a constraint for the fields we construct.

Example 4.16. Consider the group $G = \mathrm{Q}_8$. G has a unique element of order 2, which generates its center. If we consider the series $G \supsetneq Z(G) \supsetneq \{e\}$, then the fixed field of $Z(G)$ must be totally real. Therefore, in the first step of our construction, we just need to construct abelian extensions of $\mathbf{Q}$ with Galois group $G/Z(G) \simeq C_2 \times C_2$ that are totally real.

4.4 Maximal abelian subextension

Our strategy to construct number fields having Galois group isomorphic to a given solvable group G consists in creating a tower of number fields with Galois groups isomorphic to the quotient of G by the i-th subgroup of a given series. More precisely, let $G = G_0 \supsetneq G_1 = G' \supsetneq G_2 \supsetneq \ldots \supsetneq G_{n-1} \supsetneq G_n = \{e\}$ be the given series of G: we construct at every step a field K_i with Galois group G/G_i for every $i = 1, \ldots, k$. We now take advantage of the properties of the derived subgroup. Indeed, the maximal abelian subextension of K_{i+1} over K_{i-1} has Galois group isomorphic to the quotient of G_{i-1}/G_{i+1} by its derived subgroup (usually called the abelianization of G_{i-1}/G_{i+1}). We want to exploit this information at every step: we discuss a method to compute the maximal abelian subextension of an abelian extension A of a field K_i over a subfield K_{i-1}.

$$\begin{tikzcd}
 & K_{i+1} \arrow[dl, dash] \arrow[dr, dash] & \\
A \arrow[dr, dash] & & K_i \arrow[dl, dash] \\
 & K_{i-1} \arrow[d, dash] & \\
 & \mathbf{Q} &
\end{tikzcd}$$

The algorithm

In our setting, A is given as a subgroup $A_{\mathfrak{f}}$ of the ray class group $\mathrm{Cl}_{\mathfrak{f}}$ modulo $\mathfrak{f}$. We want to find the largest abelian extension L of K_{i-1} which is contained in A as an ideal class of K_{i-1}. The following theorem gives a characterization of this extension:

Theorem 4.17. *Let A be an abelian extension of K_i and let L be the maximal abelian subextension of A over K_{i-1}. Let $\mathfrak{m}$ be an admissible modulus for L over K_{i-1}. Then the ideal class corresponding to L is represented in $\mathrm{Cl}_{\mathfrak{m}}$ by the subgroup given by $N(I_A^{\mathfrak{m}})$, the norm of the ideals of A coprime to $\mathfrak{m}$.*

Proof. See [30].

Thus, we need to compute the norm group of A in a suitable ray class group over K_{i-1}.

Admissible modulus First, we need to find an admissible modulus $\mathfrak{m}$. The prime ideals of K_{i-1} that are ramified in the maximal abelian subextension L are a subset of the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ that are ramified in the extension A/K_{i-1}. Therefore we can take $\mathfrak{m}_0$ as a product $\prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$. We need to discuss suitable exponents. Denote by p_i is the prime number underneath $\mathfrak{p}_i$. If p_i does not divide the degree $[A\colon K_{i-1}]$, then we can choose $e_i = 1$ by Lemma 1.35. Therefore we are left with the primes $\mathfrak{p}_i$ lying over a prime number p_i dividing $[A\colon K_{i-1}]$. We can assume that we know the maximal order of K_i and the discriminant of A/K_i. Therefore, we can use the bounds for the maximal exponent we gave in Section 1.4 in order to get an admissible modulus.

Computation of the norm group The first idea is to compute the norm group $U_\mathfrak{m}$ in $\mathrm{Cl}_\mathfrak{m}$ via the direct method: we take the norm of prime ideals of A over K_{i-1} and compute the corresponding element in $\mathrm{Cl}_\mathfrak{m}$. The termination criterion is provided by the Bach-Sorenson bound:

Theorem 4.18 (GRH). *Let L/K_{i-1} be a Galois extension of number fields and assume $[A\colon \mathbf{Q}] = n > 1$. Let d be the absolute discriminant of A and let σ be an element of $\mathrm{Gal}(L/K_{i-1})$. There is a prime ideal $\mathfrak{p}$ of K_{i-1} of residue degree one such that its Frobenius automorphism is conjugated to σ and*

$$N(\mathfrak{p}) \leq (4 \log d + 2.5n + 5)^2$$

Proof. See [3, Theorem 5.1].

The problem of this method is that, even if the bound is conditional on GRH, it is too large to be practical. If correctness is not needed, it is possible to abort the computation before reaching the bound.

We now show how to compute the norm group correctly and with a clear termination criterion. By hypothesis, we know the congruence subgroup $A_\mathfrak{f}$ of A/K_i in a ray class group $\mathrm{Cl}_\mathfrak{f}^{K_i}$. However, the norm map $\mathrm{Cl}_\mathfrak{f}^{K_i} \to \mathrm{Cl}_\mathfrak{m}^{K_{i-1}}$ is not well defined as the modulus $\mathfrak{m}$ contains also the primes that ramify in K_i/K_{i-1}. The idea is therefore to write the norm group of A in K_i in a suitable ray class group and then compute the norm map defined on it.

Let $\mathfrak{n}$ be a modulus of K_i such that the norm map $N\colon \mathrm{Cl}_\mathfrak{n}^{K_i} \to \mathrm{Cl}_\mathfrak{m}^{K_{i-1}}$ is well defined and such that $\mathfrak{f} \mid \mathfrak{n}$. Then we can find the norm group $A_\mathfrak{n}$ of A in $\mathrm{Cl}_\mathfrak{n}$ as the kernel of the composition $\mathrm{Cl}_\mathfrak{n} \to \mathrm{Cl}_\mathfrak{f} \to \mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f}$. In order to establish this map, we compute ideals generating $\mathrm{Cl}_\mathfrak{n}$ as in Section 2.2 and compute their image in $\mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f}$. Then, using the same generators, we compute their norms over K_{i-1} and compute the corresponding image in $\mathrm{Cl}_\mathfrak{m}$. The norm group $U_\mathfrak{m}$ of L is therefore the image of the norm group $A_\mathfrak{m}$ under this map.

The only remaining issue is the choice of a suitable modulus $\mathfrak{n}$ such that the norm map $N\colon \mathrm{Cl}_\mathfrak{n}^{K_i} \to \mathrm{Cl}_\mathfrak{m}^{K_{i-1}}$ is well defined.

Proposition 4.19. *Let L/K_{i-1} be an abelian extension with admissible modulus $\mathfrak{m}$ and let K_i be an extension of K_{i-1}. Then the extension $\mathfrak{m}K_i$ of $\mathfrak{m}$ to K_i is an admissible modulus for LK_i/K_i.*

Proof. See [15, Proposition 3.5.5].

Therefore we can take $\mathfrak{n}$ to be the least common multiple of $\mathfrak{f}$ and the extension of $\mathfrak{m}$ to K_i. We now summarize the algorithm:

Algorithm 25 Maximal abelian subextension

```
Input: The norm group $A_\mathfrak{f} < \mathrm{Cl}_\mathfrak{f}$ of an abelian extension $A$ of $K_i$, a subfield
    $K_{i-1}$ of $K_i$.
Output: The norm group of the maximal abelian subextension $L$ over $K_{i-1}$.

1. Compute an admissible modulus $\mathfrak{m}$ for $L$ over $K_{i-1}$.
2. Compute a modulus $\mathfrak{n}$ over $K_i$ such that $\mathfrak{f} \mid \mathfrak{n}$ and the norm map $N\colon \mathrm{Cl}_\mathfrak{n} \to$
   $\mathrm{Cl}_\mathfrak{m}$ is well defined.
3. Find ideals $I_1, \dots, I_k$ generating $\mathrm{Cl}_\mathfrak{n}$ as in Section 2.2.
4. Compute the class of $I_1, \dots, I_k$ in $\mathrm{Cl}_\mathfrak{f}$ and establish the map $f\colon \mathrm{Cl}_\mathfrak{n} \to$
   $\mathrm{Cl}_\mathfrak{f}/A_\mathfrak{f}$.
5. Compute the kernel $S$ of $f$.
6. Compute the norm of $I_1, \dots, I_k$ and establish the map $N\colon \mathrm{Cl}_\mathfrak{n} \to \mathrm{Cl}_\mathfrak{m}$.
7. Return the image of $S$ under $N$.
```

4.5 Computing abelian extensions over subfields

The computation of an abelian extension L of a number field K requires, in general, the S-unit group of $K(\zeta_n)$ for a suitable set of places S, where n is the exponent of the extension L/K, which might be expensive if $K(\zeta_n)$ is larger than K. However, the number field L might be found also as a composite between K and an abelian extension of a subfield of K.

Example 4.20. Suppose we are searching for number fields with Galois group isomorphic to $G = \mathrm{D}_4$. Consider the presentation of G given by generators r, s and relations $r^4 = e$, $s^2 = e$, $rs = sr^3$. We use the derived series as a chain of subgroups: the derived subgroup of G is generated by r^2, and the quotient of G by the derived subgroup is isomorphic to $C_2 \times C_2$. Thus, in our construction, we would start with a $C_2 \times C_2$ extension K of $\mathbf{Q}$ and extend it with a quadratic extension. However, this quadratic extension can be seen as a quadratic extension of a subfield of K, as the following concrete example shows. Consider the field $F = \mathbf{Q}(i, \sqrt[4]{2})$, which has Galois group isomorphic to G. Its biquadratic subextension is given by $K = \mathbf{Q}(i, \sqrt{2})$ and $L = K(\sqrt[4]{2})$. In our construction, we would normally construct L as a quadratic extension of K; however, L is an abelian extension of the subextension $\mathbf{Q}(\sqrt{2})$ of K and we could have constructed it over this subfield, which has smaller degree.

Characterization of the subfield We now generalize the idea of the example to arbitrary fields. Let K be a number field with Galois group $\tilde{G}$ and L be an abelian extension with Galois group G over $\mathbf{Q}$. Denote by H be the Galois group $\mathrm{Gal}(L/K)$. In field theoretic terms, we want to give a characterization of a subfield $\tilde{K}$ of K that admits an abelian extension $\tilde{L}$ of $\tilde{K}$ such that $L = \tilde{L}K$.

$$\begin{tikzcd}
 & L \arrow[dl, dash, "\mathrm{Gal}(L/K) = H"'] \arrow[dr, dash, "\mathrm{Gal}(L/\tilde{L}) = \tilde{H}"] & \\
K \arrow[dr, dash] & & \tilde{L} \arrow[dl, dash, "\mathrm{Gal}(\tilde{L}/\tilde{K}) \simeq H"] \\
 & \tilde{K} \arrow[d, dash] & \\
 & \mathbf{Q} &
\end{tikzcd}$$

In particular, notice that $\tilde{L}$ is a normal extension of $\tilde{K}$. Denote by $\tilde{H}$ the Galois group $\mathrm{Gal}(L/\tilde{L})$. In group theoretic terms, $\tilde{H}$ must be a normal subgroup of $\mathrm{Gal}(L/\tilde{K})$ with trivial intersection with H. In particular, this means that such a subgroup $\tilde{H}$ must commute with H. This observation immediately leads to a way of finding $\tilde{K}$:

Lemma 4.21. *Let L/K be an abelian extension and let $G = \mathrm{Gal}(L/\mathbf{Q})$. Let H be the Galois group $\mathrm{Gal}(L/K)$ and suppose there exists a subgroup $\tilde{H}$ of $C_G(H)$ such that $H \cap \tilde{H} = \{e\}$. Denote by $\tilde{K}$ the fixed field of $H\tilde{H}$. Then there exists an abelian extension $\tilde{L}$ of $\tilde{K}$ such that $\tilde{L}K = L$.*

In practice, as we want to work on the smallest possible subfield, we take $\tilde{H}$ to be the largest subgroup (by cardinality) satisfying the properties of the lemma. Now, we need to construct a field $\tilde{K}$ as in the diagram. $\tilde{K}$ corresponds to the fixed field of the image of $\tilde{H}$ in $\mathrm{Gal}(K/\mathbf{Q})$. As we saw in Chapter3, there might be more then one embedding problem involving $\tilde{G}$ and G, and in particular more than one projection: thus we need to consider not just $\tilde{H}$, but all the images of $\tilde{H}$ under the automorphism group of G. Let $\tilde{K}_1, \dots, \tilde{K}_s$ be the subfields fixed by the subgroups in the orbit of $\tilde{H}$ under the action of the automorphisms. By Lemma 4.21, if L has the right Galois group over $\mathbf{Q}$, at least one of these fields must have an abelian extension with the required properties.

Translation of the extension In order to check if the abelian extension exists and to find it, we try to translate the abelian extension L/K into an abelian extension $\tilde{L}_i/\tilde{K}_i$. As usual, we consider an admissible modulus $\mathfrak{m}$ for the extension $L/\tilde{K}_i$.

The first step is to compute the the norm groups $A_{\mathfrak{m}}, B_{\mathfrak{m}}$ in $\mathrm{Cl}_{\mathfrak{m}}^{\tilde{K}_i}$ for the extensions $K/\tilde{K}_i$ and $L/\tilde{K}_i$ respectively. We follow a similar strategy as before: $B_{\mathfrak{m}}$ corresponds to the maximal abelian subextension of L over $\tilde{K}_i$: we have already discussed how to compute it in Section 4.4. Notice that, via group theory, we know already what structure the quotient $\mathrm{Cl}_{\mathfrak{m}}/B_{\mathfrak{m}}$ should have: it must be isomorphic to the abelianization of $H \times \tilde{H}_i$. Thus, if the two groups are not isomorphic, we can directly discard $\tilde{K}_i$ and restart with the next one. Then we pass to the computation of $A_{\mathfrak{m}}$. Notice that, as $K \subseteq L$, we have $B_{\mathfrak{m}} \subseteq A_{\mathfrak{m}}$. Thus we can directly compute the norm group in the quotient $\mathrm{Cl}_{\mathfrak{m}}/B_{\mathfrak{m}}$. In this case, we know that $\mathrm{Cl}_{\mathfrak{m}}/B_{\mathfrak{m}}$ is isomorphic to the abelianization of $\tilde{H}_i$. This means that we have a stopping condition for the naive algorithm: we start compute norm of prime ideals of K over $\tilde{K}_i$ until we reach the desired index. Even if the bound given by Theorem 4.18 is quite large, in practice we can stop as soon as we reach the right index.

Assume now that the computation of the norm groups $A_{\mathfrak{m}}$ and $B_{\mathfrak{m}}$ was successful. If an extension $\tilde{L}_i$ exists, then there exists a complement $C_{\mathfrak{m}}$ of $B_{\mathfrak{m}}$ in $A_{\mathfrak{m}}$ such that $\mathrm{Cl}_{\mathfrak{m}}/C_{\mathfrak{m}}$ is isomorphic to H. If such a complement does not exist, then we need to try a different field $\tilde{K}_j$. Otherwise, we have found the abelian extension we searched for: we can compute the defining polynomial and translate it back to K.

If this computation fails for every field K_i, then the extension $\mathrm{Gal}(L/K)$ has a different Galois group than the one we are searching for, and we can discard it.

Algorithm 26 Compute the defining polynomial over a subfield

```
Input: An abelian extension $L/K$, the target Galois group $G$, the Galois group
    $\tilde{G}$ of $K$ and the subgroup $H$ of $G$ such that $G/H \simeq \tilde{G}$.
Output: Either an abelian extension $\tilde{L}$ of a subfield $\tilde{K}$ of $K$ such that $K\tilde{L} = L$
    or an error in the case $L$ doesn't have the correct Galois group.
1. Compute the largest normal subgroup $\tilde{H}$ of $C_G(H)$ with trivial intersection with $H$.
2. Compute the images $\tilde{H}_1, \dots, \tilde{H}_s$ of $\tilde{H}$ under the action of the automorphism group of $G$
3. Compute the images $\bar{H}_1, \dots, \tilde{H}_s$ of $\tilde{H}_1, \dots, \tilde{H}_s$ in $G$
4. For each subgroup $\bar{H}_i$,
    • Compute the fixed field $\tilde{K}_i$ of $\bar{H}_i$.
    • Compute the norm group $A_{\mathfrak{m}}$ of $L/\tilde{K}_i$ as in Section4.4.
    • If $\mathrm{Cl}_{\mathfrak{m}}/A_{\mathfrak{m}}$ is not isomorphic to $H \times \bar{H}_i/\bar{H}_i'$, continue with another subgroup.
    • Compute the norm group $B_{\mathfrak{m}}$ of $K/\tilde{K}_i$ in $\mathrm{Cl}_{\mathfrak{m}}$ by computing the norm of prime ideals of $K$.
    • If $A_{\mathfrak{m}}$ has a complement $C_{\mathfrak{m}}$ in $B_{\mathfrak{m}}$, compute a defining equation for $C_{\mathfrak{m}}$ and return it. Otherwise, continue with the next subgroup.
```

4.6 Fields with decomposable Galois group

In this section, we discuss how to construct number fields with Galois group G which decomposes as a direct product $G = G_1 \times G_2$. Such a field K can be seen as the composite of two linearly disjoint subfield K_1, K_2 having Galois group G_1, G_2 respectively. Therefore, we aim at constructing these fields by enumerating fields having Galois group G_1 and G_2 and then computing the composite fields, since this approach allows us to work with fields of smaller degree. However, this method suffers from some problems, as the following example shows.

Example 4.22. If we want to compute fields with Galois group $C_2 \times C_2$, we enumerate quadratic extensions of $\mathbf{Q}$ and compute their composite in order to get $C_2 \times C_2$ extensions. However, the composite field of $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{2})$ is the field $\mathbf{Q}(i, \sqrt{2})$, the same as the composite of $\mathbf{Q}(\sqrt{-2})$ and $\mathbf{Q}(\sqrt{2})$.

This small example shows that in general, depending on the group, different extensions with Galois group G_1 and G_2 might give rise to the same field with Galois group G. We now discuss a method to handle this problem without having too much overhead in the computation.

Redundancy and best decomposition

The first step of the algorithm is the recognition of decomposable groups and, in case of positive answer, the choice of suitable subgroups G_1, G_2 such that $G \simeq G_1 \times G_2$. Since such subgroups are by definition normal, we compute the normal subgroups of G and we collect the pairs of normal subgroups (N_1, N_2) such that $N_1 \cap N_2$ is trivial and $N_1 N_2 = G$. If we can not find any, then the group is not decomposable. Otherwise, we choose among all the pairs the one such that the minimum of the orders of N_1, N_2 is highest. This choice makes sense because, by Galois correspondence, it means that we need to compute fields with Galois group N_1 and N_2: we are trying to keep their degree as small as possible.

We have seen that we can have different linearly disjoint fields with Galois group G_1 and G_2 giving the same extension K with Galois group $G = G_1 \times G_2$. In order to handle this issue, we count the number of fields K_1 and K_2 giving rise to the same field K. Moreover, it is also helpful to count the number of fields K_2 with Galois group G_2 such that the composite with a given field K_1 having Galois group G_1 gives the same field K and vice versa. Under the group theoretic point of view, this means that, given a pair (N_1, N_2) of normal subgroups of G such that $N_1 \times N_2 = G$, we want to count:

- the number of pairs (H, K) of normal subgroups in direct sum such that $N_1 \simeq H$ and $N_2 \simeq K$;
- the number of pairs (N_1, K) such that G is the direct sum of N_1 and K;
- the number of pairs (H, N_1) such that G is the direct sum of N_1 and K.

All these numbers can be easily computed by brute force, as G is usually quite small.

Definition 4.23. *Let $G = G_1 \times G_2$ be a direct product of group. We define the redundancy parameters of the decomposition as a triple (m, m_1, m_2) such that*

- *m_1 is the number of normal subgroups isomorphic to G_1 that are in direct product with a given a normal subgroup N of G isomorphic to G_2;*
- *m_2 is the number of normal subgroups isomorphic to G_2 that are in direct product with a given a normal subgroup N of G isomorphic to G_1;*
- *m is the number of tuples of subgroups (N_1, N_2) such that $G \simeq N_1 \times N_2$.*

Discriminant of the composite

The construction of fields with Galois group $G = G_1 \times G_2$ up to a discriminant bound B as composite of subfields with Galois group G_1 and G_2 requires the knowledge of a bound on the discriminant of the subfields. By exploiting the linear disjointness of the subfields, the following theorem provides a first result in this direction.

Theorem 4.24. *Let K_1 and K_2 be linearly disjoint fields and denote by K the composite field of K_1 and K_2. Let $\mathcal{O}_{K_1}$, $\mathcal{O}_{K_2}$, $\mathcal{O}_K$ be the maximal orders of K_1, K_2 and K respectively. Let $d = \gcd(\operatorname{disc} K_1, \operatorname{disc} K_2)$. Then $\mathcal{O}_K \subseteq \frac{\mathcal{O}_{K_1}\mathcal{O}_{K_2}}{d}$. In particular,*

$$\frac{\operatorname{disc} K_1^{\deg K_2} \operatorname{disc} K_2^{\deg K_1}}{d^{2\deg(K)-2}} \leq \operatorname{disc} K \leq \operatorname{disc} K_1^{\deg K_2} \operatorname{disc} K_2^{\deg K_1}$$

Proof. See [50, Theorem 12].

Corollary 4.25. *In the notations of Theorem 4.24, if $d = \delta^2$ is a square in $\mathbf{Z}$, then $\mathcal{O}_K \subseteq \frac{\mathcal{O}_{K_1}\mathcal{O}_{K_2}}{\delta}$.*

Proof. Follows from the proof of Theorem 4.24 and [50, Theorem 12].

Corollary 4.26. *Let K be a normal number field with Galois group $G = G_1 \times G_2$ and let K_1, K_2 be subfield with Galois group isomorphic to G_1 and G_2 respectively. Then $\operatorname{disc} K_1^{\deg K_2} \leq \operatorname{disc} K$ and $\operatorname{disc} K_2^{\deg K_1} \leq \operatorname{disc} K$.*

Example 4.27. The bound is sharp, as K/K_1 might be unramified. A concrete example of this behaviour is given by the fields $K_1 = \mathbf{Q}(\sqrt{-5})$ and $K_2 = \mathbf{Q}(i)$, as $\operatorname{disc} \mathbf{Q}(i, \sqrt{5}) = \operatorname{disc} \mathbf{Q}(\sqrt{-5})^2$.

Corollary 4.28. *Let K_1, K_2 be linearly disjoint number fields of degree d_1, d_2 respectively. Then $\operatorname{disc} K_1K_2$ and $\operatorname{disc} K_1^{d_2} \operatorname{disc} K_2^{d_1}$ differ by a square.*

By virtue of Corollary 4.26, we have a discriminant bound for the fields with Galois group G_1 and G_2. However, the bound gives only a necessary condition on the discriminant of the subfields. We now give a better lower bound for the discriminant of the composite than the bound given by Theorem 4.24.

Indeed, it is crucial to recognize as early as possible whether the discriminant of the composite of two linearly disjoint fields K_1, K_2 is larger than the bound B.

The problem of the bound in Theorem 4.24 is that the denominator of the formula might even be larger than the numerator: the estimate is too rough. To overcome this problem, we analyze the discriminant locally, prime by prime. If p is a prime number which is ramified in K_1 but not in K_2, then we know that $v_p(\operatorname{disc} K) = \deg(K_2) v_p(\operatorname{disc}(K_1))$ by Theorem 4.24. We now split the remaining cases into tamely ramified primes and wildly ramified primes.

Tamely ramified primes

Suppose now that p divides the discriminants of K_1 and K_2 and p is tamely ramified in both fields. In this case, exploiting the fact that K_1 and K_2 are normal, we can predict the ramification index of every prime lying over p in K:

Proposition 4.29. *Let K_1 and K_2 be Galois extensions of $\mathbf{Q}$ and assume that they are linearly disjoint. Let p be a prime number which is tamely ramified in both K_1 and K_2 with ramification indices e_1, e_2 respectively. If K is the composite field of K_1 and K_2, then the ramification index e of p in K is the least common multiple of e_1 and e_2.*

Proof. Let $\mathfrak{p}$ be a prime of K lying over p and let $\mathfrak{p}_{K_1}$, $\mathfrak{p}_{K_2}$ be the prime ideals of K_1, K_2 respectively lying underneath $\mathfrak{p}$. Let H, H_1, H_2 be the inertia subgroup of $\mathfrak{p}$, $\mathfrak{p}_{K_1}$ and $\mathfrak{p}_{K_2}$. As p is tamely ramified, the three subgroups are cyclic (as we have seen in Lemma 3.44). Denote by π_i the projection $G \to G_i$; then $\pi_i(H) = H_i$ and the image of a generator of H is a generator of H_i by Lemma 1.6. Let (c_1, c_2) be a generator of H seen as a subgroup of $G = G_1 \times G_2$. Then we know that $c_i \in H_i$ and it is a generator of H_i. As $c_i^{e_i}$ is the identity, also $(c_1, c_2)^{\operatorname{lcm}(e_1,e_2)}$ must be the identity. As (c_1, c_2) has order e, we get $e \mid \operatorname{lcm}(e_1, e_2)$. The multiplicativity of the ramification index in towers implies that $\operatorname{lcm}(e_1, e_2) \mid e$ and this proves the claim.

By virtue of the proposition, we therefore know the ramification index of p in K. Since K is normal and p is tamely ramified, this determines the valuation of the discriminant:

Lemma 4.30. *Let K be a normal field of degree n and let p be a prime number with ramification index e which is tamely ramified. Then $v_p(\operatorname{disc} K) = n(e-1)/e$.*

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ be a prime ideal lying over p. As it is tamely ramified, the valuation of the different ideal $\mathcal{D}_K$ at $\mathfrak{p}_i$ is $e-1$ for all i. Therefore $\mathcal{D}_K = J \prod_{i=1}^{r} \mathfrak{p}_i^{e-1}$, where J is an ideal coprime to p. Since $\operatorname{disc} K = N(\mathcal{D}_K)$ and the norm is multipicative, we get

$$v_p(\operatorname{disc} K) = v_p(N(\mathcal{D}_K)) = v_p(\prod_{i=1}^{r} N(\mathfrak{p}_i)^{e-1})$$
$$= (e-1)\sum_{i=1}^{r} v_p(N(\mathfrak{p}_i)) = (e-1)rf.$$

As $rf = \frac{n}{e}$, the claim follows.

Wildly ramified primes

Assume now that p is wildly ramified in K_1 or K_2. In this case, we can't use the same technique as before, as the inertia groups might not be cyclic and the ramification index is not enough to determine the valuation of the discriminant at p.

Example 4.31. Consider $K_1 = \mathbf{Q}(i)$ and $K_2 = \mathbf{Q}(\sqrt{2})$. 2 is wildly ramified in both fields and it is totally ramified in the composite field K. The inertia subgroup is thus isomorphic to $C_2 \times C_2$, in particular it is not cyclic. Moreover, predicting the valuation of the discriminant from the valuation of the discriminants of K_1 and K_2 is hard: $\operatorname{disc} K_1 = 4$, $\operatorname{disc} K_2 = 8$, while $\operatorname{disc} K_1K_2 = 256$. However, we could have constructed the same field by considering K_2 and $K_3 = \mathbf{Q}(\sqrt{-2})$, and in this case the valuation of the discriminant at 2 is equal to 3 for both fields.

Therefore, we just use the fact that $\operatorname{disc} K = \operatorname{disc} K_1^{\deg K_2} N(\operatorname{disc} K/K_1) = \operatorname{disc} K_2^{\deg K_1} N(\operatorname{disc} K/K_2)$ to get that

$$v_p(\operatorname{disc} K) \geq \max\{\deg K_2 v_p(\operatorname{disc} K_1), \deg K_1 v_p(\operatorname{disc} K_2)\}.$$

Computation of the bound

Algorithm 27 computes a lower bound for the discriminant of the composite field K of the number fields K_1, K_2 by using the results obtained so far.

Algorithm 27 Lower bound on the discriminant of the composite field

```
Input: Two linearly disjoint fields $K_1, K_2$.
Output: A lower bound on the discriminant of the composite field $K_1K_2$

1. Compute the greatest common divisor $d$ of the discriminants of $K_1$ and $K_2$.
2. Let $s_1$ and $s_2$ be the largest divisors of $\operatorname{disc} K_1$, $\operatorname{disc} K_2$ coprime to $d$
3. Set disc $= s_1^{\deg K_2} s_2^{\deg K_1}$
4. Compute the prime divisors $p_1, \dots, p_s$ of $d$.
5. For $i \in \{1, \dots, s\}$,
    • If $p$ divides the degree of $K_1$ or $K_2$,
        – multiply $s$ by $p_i^{\max\{\deg K_2 v_{p_i}(\operatorname{disc} K_1), \deg K_1 v_{p_i}(\operatorname{disc} K_2)\}}$.
    • Otherwise,
        – compute the ramification indices $e_1$, $e_2$ of $p_i$ in $K_1$ and $K_2$.
        – Compute the least common multiple $e$ of $e_1$ and $e_2$.
        – Multiply $s$ by $p_i^{\deg K_1 \deg K_2 (e-1)/e}$.
6. Return $s$.
```

Test for linearly disjointness

Let K_1, K_2 be a number field with Galois group G_1 and G_2 respectively. As we want the Galois group of the composite to be $G = G_1 \times G_2$, K_1 and K_2 must be linearly disjoint. Thus, we need an algorithm to decide whether two fields K_1 and K_2 are linearly disjoint.

Example 4.32. Consider the fields $K_1 = \mathbf{Q}(\zeta_3, \sqrt[3]{2})$ and $K_2 = \mathbf{Q}(\zeta_3, \sqrt[3]{3})$. They have both Galois group isomorphic to S_3. However, the degree of the composite is 18 and thus it doesn't provide a number field with Galois group $S_3 \times S_3$.

In order to test if K_1 and K_2 are linearly disjoint, we use again information coming from group theory:

Proposition 4.33. *Let K_1, K_2 be normal number fields with solvable Galois group. Let $K_{1,ab}$ and $K_{2,ab}$ be the maximal abelian subextensions of K_1, K_2 respectively. Then K_1 and K_2 are linearly disjoint if and only if $K_{1,ab}$ and $K_{2,ab}$ are linearly disjoint.*

Proof. Let F be the intersection of K_1 and K_2, which is well defined as K_1 and K_2 are normal. Then F is normal too and its Galois group is solvable, as quotients of solvable groups are solvable. If F is abelian, we are done. Otherwise, the maximal abelian subextension of F must be non trivial (as $\mathrm{Gal}(F/\mathbf{Q})$ is solvable) and it is contained in $K_{1,ab}$ and $K_{2,ab}$.

Thus, we can just look at their maximal abelian subextension over $\mathbf{Q}$ and decide if they are linearly disjoint. Notice that in our construction we always have the maximal abelian subextension at our disposal, as we are constructing subextensions corresponding to the subgroups appearing in the derived series. In particular, we have the following criterion:

Corollary 4.34. *Let d_1, d_2 be the degrees of $K_{1,ab}$ and $K_{2,ab}$ respectively. If* $\gcd(d_1, d_2) = 1$*, then K_1 and K_2 are linearly disjoint.*

The same criterion can be given in terms of properties of the derived subgroup:

Corollary 4.35. *If* $\gcd([G_1 \colon G_1'], [G_2 \colon G_2']) = 1$*, then K_1 and K_2 are linearly disjoint.*

Suppose now that the degree of $K_{1,ab}$ and $K_{2,ab}$ are not coprime. An arithmetic criterion to recognise if two fields are linearly disjoint comes from the analysis of the discriminant of the fields:

Lemma 4.36. *If* $\gcd(\operatorname{disc} K_{1,ab}, \operatorname{disc} K_{2,ab}) = 1$*, then* K_1 *and* K_2 *are linearly disjoint.*

Proof. Let F be the intersection of $K_{1,ab}$ and $K_{2,ab}$, which is well defined as K_1 and K_2 are normal. Assume that $[F\colon \mathbf{Q}] > 1$. Then there is a prime number p which is ramified in F and consequently in $K_{1,ab}$ and $K_{2,ab}$. This gives a contradiction since the ramified primes always divide the discriminant.

If this does not work, then the greatest common divisor of the discriminant is not trivial: its factors give us information about the ramification in the intersection over $\mathbf{Q}$. In particular, we can find an admissible modulus $\mathfrak{m}$ divisible only by the primes that ramify in both $K_{1,ab}$ and $K_{2,ab}$. We compute then $\mathrm{Cl}_{\mathfrak{m}}$ and the norm groups $A_{1,\mathfrak{m}}$, $A_{2,\mathfrak{m}}$ of $K_{1,ab}$ and $K_{2,ab}$.

Lemma 4.37. *Let* $\mathfrak{m}$ *be an admissible modulus for* $K_{1,ab} \cap K_{2,ab}$ *and let* $A_{1,\mathfrak{m}}$, $A_{2,\mathfrak{m}}$ *be the norm groups in* $\mathrm{Cl}_{\mathfrak{m}}$ *corresponding to* $K_{1,ab}$ *and* $K_{2,ab}$ *respectively.* $K_{1,ab}$ *and* $K_{2,ab}$ *are linearly disjoint if and only if* $A_{1,\mathfrak{m}} A_{2,\mathfrak{m}} = \mathrm{Cl}_{\mathfrak{m}}$.

Proof. Let F be the class field of $\mathrm{Cl}_{\mathfrak{m}}$. The norm group $A_{1,\mathfrak{m}}$, $A_{2,\mathfrak{m}}$ correspond to the intersection of $K_{1,ab}$ and $K_{2,ab}$ with F. As $\mathfrak{m}$ is an admissible modulus for the intersection $K_{1,ab} \cap K_{2,ab}$, $F \cap K_{1,ab}$ and $F \cap K_{2,ab}$ contain the intersection $K_{1,ab} \cap K_{2,ab}$. The statement follows from the fact the the extension corresponding to $A_{1,\mathfrak{m}} A_{2,\mathfrak{m}}$ is $F \cap K_{1,ab} \cap K_{2,ab}$.

By virtue of the lemma, we have a criterion to check if $K_{1,ab}$ and $K_{2,ab}$ are disjoint. However, in some particular cases, it is possible to do better. For instance, if the maximal abelian subextensions $K_{1,ab}$ and $K_{2,ab}$ are cyclic of prime degree, then they are either disjoint or equal. Therefore it is enough to check if the extensions are the same, for example by checking their discriminant and the splitting of prime ideals.

Algorithm 28 Test for linearly disjointness

```
Input: Fields $K_1$, $K_2$ with solvable Galois group $G_1$, $G_2$ and their maximal
    abelian subextensions $K_{1,ab}$, $K_{2,ab}$.
Output: True if $K_1$ and $K_2$ are linearly disjoint, false otherwise.

1. If $(\deg K_{1,ab}, \deg K_{2,ab}) = 1$, return true.
2. If $(\operatorname{disc} K_{1,ab}, \operatorname{disc} K_{2,ab}) = 1$, return true.
3. Compute an admissible modulus $\mathfrak{m}$ for $K_{1,ab} \cap K_{2,ab}$ over $\mathbf{Q}$.
4. Compute the ray class group $\mathrm{Cl}_{\mathfrak{m}}$ modulo $\mathfrak{m}$.
5. Compute the norm groups $A_{\mathfrak{m},1}$, $A_{\mathfrak{m},2}$ corresponding to $K_{1,ab}$, $K_{2,ab}$.
6. If $A_{\mathfrak{m},1} A_{\mathfrak{m},2} = \mathrm{Cl}_{\mathfrak{m}}$, return true. Otherwise, return false.
```

Arithmetically equivalent fields

Let K_1, L_1 be number fields with Galois group G_1 and K_2, L_2 be number fields with Galois group G_2. We want to decide whether the composite field $K = K_1K_2$ coincides with $L = L_1L_2$ without computing an isomorphism between the two fields. We assume that we already know that the signature, the ramified primes and the maximal abelian subextensions of K and L coincide, as at this point of the algorithm we have already tested this properties.

It is well known that, if two fields are isomorphic, the splitting behaviour of prime numbers in the maximal order must be the same in both fields. This property goes under the name of "arithmetic equivalence":

Definition 4.38. *Let K be a number field and let p be a prime number. Denote by $\mathcal{O}_K$ the ring of integers of K and let $p\mathcal{O}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$ be the decomposition of $p\mathcal{O}_K$ into prime ideals. We define the splitting profile of p as the multiset consisting of the tuples (e_i, f_i), where f_i is the inertia degree of $\mathfrak{p}_i$.*

Definition 4.39. *Let F, L be number fields of the same degree. We say that F, L are arithmetically equivalent if the splitting profile of the prime ideals in K and L coincides.*

In general, being arithmetically equivalent is not the same as being isomorphic. However, for normal fields it is true, as the Frobenius density theorem shows.

Definition 4.40. *Let $\sigma \in G$ be an element of order n a group G. The division of σ is the set of elements of G that are conjugate to an element of the form σ^m for m coprime to n.*

Theorem 4.41. *Let F be a Galois extension of $\mathbf{Q}$ and let $\sigma \in \mathrm{Gal}(F/\mathbf{Q})$. Let t be the cardinality of the division of σ and let S be the set of prime numbers p such that the conjugacy class of the Frobenius automorphism of p is contained in the division of σ. Then S has density $t/|G|$.*

Proof. See [36, Theorem 5.2].

Corollary 4.42. *Two normal fields K, L are isomorphic if and only if they are arithmetically equivalent.*

Proof. By [36, Corollary 5.5], it follows that if the set of primes that split completely in K, L coincides up to a finite number of primes, then K and L are isomorphic. Since being arithmetically isomorphic implies this behaviour of the totally split primes, the claim follows.

In algorithmic terms, it is important to have a bound on the smallest prime number for which the behaviour in K_1K_2 and L_1L_2 is different, assuming that the fields are not isomorphic. We make use of Theorem 4.18 in order to get such a bound. Let F be the composite field KL and let E be the intersection $L \cap K$. The Galois group $\mathrm{Gal}(F/E)$ decomposes as a direct product $\mathrm{Gal}(K/E) \times \mathrm{Gal}(L/E)$. Let $\mathfrak{p}$ be a prime ideal of E with different behaviour in K and L and let σ be the corresponding Frobenius conjugacy class in $\mathrm{Gal}(F/E)$. As the conjugacy class determines the prime splitting in K and L, we need to bound the norm of the smallest prime ideals $\mathfrak{p}$ of E having σ as a Frobenius class. By Theorem 4.18, under GRH, there exists a prime ideal $\mathfrak{p}$ with this property such that

$$N_{E/\mathbf{Q}}(p) \leq (4 \log \operatorname{disc} F + 2.5[F\colon \mathbf{Q}] + 5)^2$$

and this gives us the bound we were searching for.

4.6.1 Sieving algorithm

We show how to patch together the information coming from the analysis of the subfields in order to compute efficiently the composite field.

More specifically, our task is to compute number fields with Galois group G up to an absolute discriminant bound B. We suppose that we have a decomposition $G = G_1 \times G_2$ and we have already computed fields with Galois group G_1 and G_2 up to discriminant $\sqrt[|G_2|]{B}$ and $\sqrt[|G_1|]{B}$ respectively.

First sieving step

The first step in the algorithm consists in splitting the list of possible fields into smaller sublists depending on the algebraic properties of the composite. Assume we have lists l_1, l_2 of number fields with Galois group G_1, G_2 respectively. First of all, we create a set of pairs of fields such that for every pair $(K_1, K_2) \in l_1 \times l_2$ we have the following properties:

- K_1 and K_2 are linearly disjoint (Algorithm 28);
- the lower bound on the discriminant of K_1K_2 given by Algorithm 27 is lower than B.

Now, we group the pairs into subsets depending on the ramification in the composite field. Specifically, we sieve the pairs with respect to the following properties:

- the set of ramified primes in the composite;
- the signature of the composite;
- the set of ramified primes in the maximal abelian subextension;
- the discriminant of the composite field up to squares.

These properties might be check quite efficiently but they might be not enough for our purpose.

Using the redundancy parameters

As a second step of the algorithm, we use the redundancy parameters in order to discard some of the fields. Let $G = G_1 \times G_2$ be the given decomposition of the group G and let m, m_1, m_2 be the redundancy parameters as in Definition 4.23. Consider a set of pairs S of fields obtained by the first part of the sieving.

Remark 4.43. All the invariants that we chose in the first part of the sieving depend on properties of the composite fields. Therefore all the m pairs that give rise to the same composite field will be grouped in the same list.

For each field K with Galois group G and discriminant lower than the givn bound B, there are m pairs in S giving rise to it. Thus, if the cardinality of S is lower than m, we can discard all the fields. The other redundancy parameters give different constraints. Let K_1 be a field appearing as a first component of one of the pairs in S. Then K_1 must appear as a first component in at least m_1 pairs. The same holds for the fields appearing as second components: they must occur at least m_2 times. This process must be repeated until all the redundancy parameters are satisfied.

Algorithm 29 Sieving by redundancy parameters

```
Input: A set of pairs $S$ of fields given by the first sieve, redundancy parameters
    $m, m_1, m_2$.
Output: A set of pairs of fields which satisfies the constraints given by the
    redundancy parameters.

1. If $|S| < m$, return an empty list.
2. Collect all the first components $F_1$ of the pairs in $S$.
3. For each $K$ in $F_1$,
     • Count the number of pairs $s_K$ in $S$ having $K$ as a first component.
     • If $s_K < m_1$, remove all these pairs by $S$ creating a new set $S_1$. Restart
       the algorithm with $S_1$, $m, m_1, m_2$.
4. Collect all the first components $F_2$ of the pairs in $S$.
5. For each $K$ in $F_2$,
     • Count the number of pairs $s_K$ in $S$ having $K$ as a second component.
     • If $s_K < m_2$, remove all these pairs by $S$ creating a new set $S_1$. Restart
       the algorithm with $S_1$, $m, m_1, m_2$.
6. Return $S$.
```

In practice, this operation is cheap as it is purely combinatorial. However, its effectiveness depends on the criteria used in the first sieving step.

Sieving using splitting profiles

As the final step of the algorithm, we use the Frobenius density theorem in order to split the subsets of pairs that are larger than the redundancy parameters. Let S be a set of pairs of fields given in output by Algorithm 29. The idea of the algorithm is to find prime ideals with different splitting behaviour in the composite fields corresponding to the pairs in S. In this way, we create clusters of fields of length at most m (the first of the redundancy parameters).

The only part we need to clarify is the choice of the set of primes to test. As we can ignore a finite set of prime ideals in order to test if two fields are arithmetically isomorphic, we restrict ourselves to unramified primes. For those, we can compute the splitting behaviour in the composite from the splitting behaviour in the components:

Lemma 4.44. *Let K_1, K_2 be Galois extensions of $\mathbf{Q}$ and let p be a prime number which is unramified in both K_1 and K_2. Let f_1, f_2 be the inertia degrees of the prime ideals of K_1, K_2 respectively lying over p. Let $\mathfrak{p}$ be a prime ideal of K_1K_2 lying over $\mathfrak{p}$. Then the inertia degree of $\mathfrak{p}$ is equal to* $\operatorname{lcm}(f_1, f_2)$.

Proof. The proof is the same as the proof of Lemma 4.29, as the inertia subgroups are trivial (p is unramified), the decomposition groups are cyclic and they behave well with respect to subfields.

As the prime numbers are unramified in K_1K_2, denoted by f the inertia degree of p in K_1K_2, we deduce that the number of prime ideals lying over p is $[K_1K_2 \colon \mathbf{Q}]/f$, because K_1K_2 is normal.

Algorithm 30 Sieving using splitting profiles

```
Input: A set of pairs of fields $S$, a prime number $p$ to start sieving, the first
    redundancy parameter $m$.
Output: A set of sets of pairs of fields smaller than $m$.

1. Create an empty list $L_{\text{final}}$.
2. Compute the splitting profile of $p$ in the composite fields corresponding
   to the elements of $S$.
3. Sieve the fields by the splitting profile, i.e. group all the pairs such that $p$
   has the same splitting profile in the corresponding composite field.
4. For all the subsets $S_i$ created this way,
     • If the length of $S_i$ is smaller than $m$, discard $S_i$.
     • If the length of $S_i$ is exactly $m$, put $S_i$ in $L_{\text{final}}$.
     • Otherwise, compute a prime number $q$ larger than $p$ and reapply the
       algorithm on $S_i$ and $q$. Merge the result of this recursive call with
       $L_{\text{final}}$.
5. Return $L_{\text{final}}$.
```

The algorithm

We are now ready to illustrate the algorithm to merge the fields in order to get a unique number field for every isomorphism class.

Algorithm 31 Sieve fields

```
Input: A discriminant bound $B$, lists $l_1$, $l_2$ of the number fields with Galois groups $G_1$, $G_2$ up to absolute discriminant $\sqrt[|G_2|]{B}$, $\sqrt[|G_1|]{B}$, redundancy parameters $n, n_1, n_2$ as in Definition 4.23
Output: The list of number fields with Galois group $G$ up to discriminant bound $B$.

1. Initialize an empty list $L_{\text{final}}$.
2. Using Algorithm 28 and Algorithm 27, create a list $L$ of pairs $(K_1, K_2) \in l_1 \times l_2$ such that
     • $K_1$ and $K_2$ are linearly disjoint;
     • the lower bound on the discriminant of $K_1K_2$ is lower than $B$.
3. Split $L$ in sublists $L_1, \ldots, L_s$ of tuples of fields satisfying the following properties:
     • signature of the composite field,
     • ramified primes in the composite field;
     • ramified primes in the maximal abelian subextension of the composite.
     • discriminant of the composite up to a square.
4. Apply Algorithm 29 on every list $L_1, \cdots, L_s$.
5. Sieve the remaining field by using Algorithm 30.
6. For every subset of field, compute the composite field and check if its discriminant is lower than $B$. If it is, insert it in $L_{\text{final}}$.
```

CHAPTER 5

Numerical results

In this last chaper, we present a guided example of Algorithm 1, in order to clarify how it works. In the second section, we focus on its performance. Indeed, we have implemented our algorithm in the package Hecke [25] using GAP [28] for the group theoretic tasks. The algorithm performs quite well in practice: we show its efficiency by computing some large degree fields that were out of reach before.

5.1 An example: fields with Galois group $\mathbf{Q_8}$

We consider the quaternion group $G = \mathrm{Q}_8$ and the discriminant bound $B = 10^{12}$. We want to find all the fields with Galois group isomorphic to G and discriminant bounded by B.

The first step is to compute a normal series for G. In this case, the derived series and the degree minimizing series we defined in Section 4.1 coincide: the first subgroup is given by the center of G and it is isomorphic to C_2. The quotient $G/Z(G)$ is abelian and isomorphic to $C_2 \times C_2$: thus the algorithm constructs first $C_2 \times C_2$-fields and then extends them with a quadratic extension.

The first layer of fields we need to construct is given by biquadratic extensions of $\mathbf{Q}$ with discriminant bounded by $\sqrt{B} = 10^6$. In this case, we use the condition of Section 4.3 on the ramification at the infinite places, which allows us to restrict to totally real biquadratic fields, as Example 4.16 shows. By means of Lemma 1.36, the prime numbers that can divide the conductor of the biquadratic fields are bounded by 1000: combining them we get 399 conductors. We then compute the ray class group for each of them and subgroups with quotient isomorphic to $C_2 \times C_2$: we get 196 totally real number fields with discriminant bounded by 10^6.

The second step is to check if the embedding problems for Q_8 are solvable. As we have seen in Example 3.30, for each field we have to check the solvability of one embedding problem. Since the kernel is cyclic of order 2, the embedding problem is of Brauer type and we can apply directly Algorithm 21: the embedding problem is solvable for 53 out of the 196 fields.

We now try to extend the remaining 53 fields to Q_8 extensions. By Example 4.10, we know that every prime number ramified in a biquadratic field must ramify further. Applying this criterion, we see that the discriminant of a Q_8 extension of 50 of the 53 fields would be larger than 10^{12}. Thus, we only need to extend 3 fields, namely the fields with defining equations $x^4 - 10x^2 + 1$, $x^4 - 2x^3 - 13x^2 + 14x + 19$ and $x^4 - 26x^2 + 81$, corresponding to $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbf{Q}(\sqrt{6}, \sqrt{5})$ respectively. The first one admits 2 extensions with the correct Galois group, the other none.

Thus, we have found the fields defined by $x^8 - 12x^6 + 36x^4 - 36x^2 + 9$ and $x^8 + 12x^6 + 36x^4 + 36x^2 + 9$.

5.2 Minimal discriminants

In this section, we address the problem of finding the fields with minimal discriminant: given a solvable group G, find the field(s) with smallest absolute discriminant among the fields with Galois group G.

In particular, we focus on 2-groups: since the results are already known for the degree 8 fields (see [41]), we apply our methods for the groups of order 16, 32 and 64. We have done the same computation for all the groups up to order 50, but we decided to focus here on 2-groups as they provide the most challenging example for our algorithm.

For each group G, we will give tables containing the minimal discriminant of a field with Galois group G for both possible signatures. Because of the large number of groups, we do not list all the defining polynomials of the fields, which were anyway computed as they are crucial to verify the correctness of the Galois group.

Odlyzko's bounds The problem of finding the minimal discriminant for a fields of degree n with signature (r_1, r_2) has been extensively studied in the literature. In particular, there are some asymptotic predictions.

Theorem 5.1 (GRH). *Let K be a number field of degree n with signature (r_1, r_2). Then*

$$\operatorname{disc} K \geq 55^{r_1} 21^{2r_2} + \epsilon(n)$$

with $\epsilon(n) \to 0$ when $n \to \infty$.

Proof. See [54, Theorem 1].

For a fixed degree, it is possible to give a precise estimate of the function $\epsilon(n)$. In particular, these bounds were computed in [19].

Definition 5.2. *Let K be a number field of degree n. We define the root discriminant of K as $\operatorname{rd}(K) = \sqrt[n]{\operatorname{disc} K}$.*

In the case of fields of degree 16, the bounds for the root discriminant of a field is 9.073029 for signature $(0, 8)$ and 20.726503 for a totally real field.

The bounds for root discriminant of a field is 12.918270 for signature $(0, 16)$ and 33.770867 for a totally real field.

The bounds for the degree 64 cases are 16.852151 for signature $(0, 32)$ and 48.940648 for a totally real field.

The discriminants we have found are quite far from the expectation in the case of totally real fields: the reason is that we are restricting our search to normal fields. Moreover, there is a clear dependency of the problem on the Galois group: for different groups, the difference between the minimal discriminants might be significant. However, minimal discriminant bounds depending on the Galois group are not available in the literature.

Strategy Algorithm 1 allows us to find every field with a given Galois group with absolute discriminant bounded by B. In order to find the fields with minimal discriminant, we need to refine our strategy. Let n be the degree of the field we are searching for. Using Odlyzko's bounds, there is a constant C such that every field of degree n has discriminant larger than C. Then, for every group G, we apply Algorithm 1 with discriminant bound $10^5 \cdot C$. If the output is empty, we restart then the algorithm increasing the bound by a factor 10^5. Otherwise, we check the signature of the fields we get in output. If we have both totally real fields and totally complex fields, we then compare the discriminants and output one of the fields with minimal discriminant. Otherwise, we continue our search for the missing signature increasing the bound by 10^5, as above.

Results

The following tables contains the minimal discriminants of fields with Galois group of order 16, 32, 64 for both possible signature. In particular, the first column is the group identifier as in the Small Group library ([6], available in GAP [28]), the second column contains the minimal discriminant of totally complex fields and the fourth the same information for totally real fields. The third and the fifth columns contain a percentage describing how far the values are from the GRH bounds. In order to make the table readable, we do not include the polynomials defining these fields.

Id	Signature $(0, 8)$	% bound	Signature $(16, 0)$	% bound
1	17^{15}	56.961653 %	$17^{15} \cdot 3^8$	19.009179 %
2	$5^{12} \cdot 2^{44}$	147.91779 %	$5^{12} \cdot 2^{48}$	29.059939 %
3	$5^{12} \cdot 2^{24}$	4.236591 %	$7^8 \cdot 2^{54}$	32.433916 %
4	$2^{54} \cdot 3^{12}$	160.65429 %	$2^{54} \cdot 3^{12}$	14.101445 %
5	2^{64}	76.346841 %	$5^8 \cdot 17^{14}$	28.706884 %
6	$5^{14} \cdot 3^{12}$	2.72766 %	$5^{14} \cdot 2^{40}$	11.595764 %
7	$5^8 \cdot 19^8$	7.426024 %	$113^8 \cdot 2^{24}$	45.06351 %
8	$2^{32} \cdot 3^{14}$	15.289244 %	$2^{58} \cdot 3^{14}$	55.66422 %

9	$7^{14} \cdot 2^{32} \cdot 3^{12}$	451.581153 %	$7^{14} \cdot 2^{32} \cdot 3^{12}$	141.454711 %
10	$5^{12} \cdot 2^{16} \cdot 3^{8}$	27.66323 %	$5^{12} \cdot 2^{32} \cdot 3^{8}$	11.769186 %
11	$7^{8} \cdot 2^{32}$	16.642471 %	$2^{32} \cdot 17^{8} \cdot 3^{8}$	37.822158 %
12	$2^{48} \cdot 3^{12}$	100.991934 %	$5^{8} \cdot 2^{48} \cdot 3^{12}$	96.738745 %
13	$2^{40} \cdot 3^{8}$	7.989944 %	$5^{8} \cdot 13^{8} \cdot 2^{24}$	10.021013 %
14	$5^{8} \cdot 2^{32} \cdot 3^{8}$	70.747094 %	$5^{8} \cdot 7^{8} \cdot 2^{32} \cdot 3^{8}$	97.755517 %

The field with the smallest discriminant has a root discriminant of 9.320510 and Galois group $(16, 6)$. For totally real fields, the minimum of the root discriminants is 22.803508, given by the minimal field for the group $(16, 13)$.

The difficulty of the problem increases with the order of the group, mainly for two reasons: the number of groups and the degree of the fields we encounter during the algorithm get larger. We now present the results for the degree 32 groups.

Id	Signature $(0, 16)$	% bound	Signature $(32, 0)$	% bound
1	2^{191}	384.806495 %	2^{191}	85.451596 %
2	$5^{24} \cdot 29^{24}$	223.460791 %	$2^{96} \cdot 17^{24}$	98.328199 %
3	$5^{24} \cdot 17^{28}$	208.791937 %	$5^{24} \cdot 2^{128}$	58.418273 %
4	$5^{28} \cdot 13^{28}$	198.603456 %	$5^{28} \cdot 2^{104}$	15.187149 %
5	2^{134}	41.045342 %	$2^{64} \cdot 17^{28}$	41.305995 %
6	2^{122}	8.760827 %	$2^{108} \cdot 17^{16}$	26.665542 %
7	$5^{28} \cdot 11^{16}$	4.976174 %	$5^{28} \cdot 29^{16} \cdot 3^{24}$	48.62658 %
8	$7^{24} \cdot 2^{134}$	506.991039 %	$7^{24} \cdot 2^{134}$	132.190489 %
9	$5^{24} \cdot 19^{16}$	12.823598 %	$7^{16} \cdot 2^{134}$	42.747962 %
10	$13^{24} \cdot 2^{64} \cdot 3^{24}$	383.230223 %	$13^{24} \cdot 2^{64} \cdot 3^{24}$	84.84863 %
11	$5^{24} \cdot 2^{64}$	3.534034 %	$7^{16} \cdot 2^{126}$	20.036249 %
12	$2^{134} \cdot 3^{24}$	221.513853 %	$2^{134} \cdot 3^{24}$	22.987745 %
13	$2^{126} \cdot 3^{28}$	210.157544 %	$2^{126} \cdot 3^{28}$	18.643649 %
14	$5^{24} \cdot 101^{24}$	724.639581 %	$2^{108} \cdot 17^{28}$	266.502407 %
15	$2^{134} \cdot 3^{28}$	268.841558 %	$2^{134} \cdot 3^{28}$	41.091872 %
16	$17^{30} \cdot 3^{16}$	90.942293 %	$5^{24} \cdot 17^{30}$	41.00391 %
17	$2^{32} \cdot 17^{30}$	120.481169 %	$2^{48} \cdot 17^{30}$	19.274786 %
18	$41^{16} \cdot 2^{48}$	40.195013 %	$5^{16} \cdot 461^{16}$	42.165185 %
19	2^{146}	82.913179 %	$5^{24} \cdot 181^{16} \cdot 3^{24}$	203.644572 %
20	$7^{24} \cdot 2^{160}$	966.029323 %	$7^{24} \cdot 2^{160}$	307.785048 %
21	$5^{24} \cdot 2^{96}$	107.068069 %	$5^{24} \cdot 2^{96} \cdot 3^{16}$	37.194249 %
22	$5^{24} \cdot 2^{72}$	23.12341 %	$7^{16} \cdot 2^{108} \cdot 3^{16}$	40.780879 %
23	$2^{108} \cdot 3^{24}$	83.068161 %	$5^{16} \cdot 2^{108} \cdot 3^{24}$	56.588538 %
24	$2^{104} \cdot 3^{24}$	67.874244 %	$5^{24} \cdot 2^{80} \cdot 3^{24}$	27.673635 %
25	$5^{24} \cdot 2^{32} \cdot 3^{24}$	18.003281 %	$5^{16} \cdot 2^{108} \cdot 3^{16}$	18.981559 %
26	$5^{24} \cdot 2^{96} \cdot 3^{24}$	372.013124 %	$5^{24} \cdot 2^{104} \cdot 3^{24}$	114.720604 %
27	$5^{16} \cdot 2^{92}$	26.981918 %	$2^{88} \cdot 11^{16} \cdot 3^{24}$	50.600898 %
28	$2^{96} \cdot 3^{16}$	7.262091 %	$5^{16} \cdot 2^{48} \cdot 11^{16} \cdot 3^{24}$	41.587551 %
29	$2^{100} \cdot 3^{24}$	53.94136 %	$5^{16} \cdot 2^{104} \cdot 3^{24}$	43.592322 %
30	$2^{84} \cdot 3^{24}$	8.85298 %	$5^{16} \cdot 2^{96} \cdot 3^{24}$	20.746269 %

31	$2^{96} \cdot 3^{24}$	41.16485 %	$5^{24} \cdot 2^{96} \cdot 3^{24}$	80.557786 %
32	$5^{24} \cdot 2^{104} \cdot 3^{24}$	461.321365 %	$5^{24} \cdot 2^{104} \cdot 3^{24}$	114.720604 %
33	$2^{104} \cdot 3^{24}$	67.874244 %	$5^{24} \cdot 2^{96} \cdot 3^{24}$	80.557786 %
34	$2^{100} \cdot 3^{24}$	53.94136 %	$5^{24} \cdot 2^{48} \cdot 11^{16} \cdot 3^{24}$	111.722771 %
35	$5^{24} \cdot 2^{108} \cdot 3^{24}$	512.125289 %	$5^{24} \cdot 2^{108} \cdot 3^{24}$	134.154479 %
36	$2^{128} \cdot 3^{16}$	114.524181 %	$5^{16} \cdot 2^{128} \cdot 3^{16}$	83.494648 %
37	$5^{28} \cdot 2^{32} \cdot 3^{24}$	44.299668 %	$5^{28} \cdot 2^{80} \cdot 3^{16}$	18.629352 %
38	$5^{28} \cdot 2^{32} \cdot 3^{16}$	9.644037 %	$5^{28} \cdot 7^{16} \cdot 2^{32} \cdot 3^{16}$	10.967598 %
39	$5^{16} \cdot 3^{16} \cdot 19^{16}$	30.682692 %	$5^{16} \cdot 113^{16} \cdot 2^{48}$	99.079713 %
40	$2^{80} \cdot 3^{28}$	14.512192 %	$13^{16} \cdot 2^{80} \cdot 3^{24}$	37.671928 %
41	$7^{28} \cdot 2^{64} \cdot 3^{24}$	287.397987 %	$7^{28} \cdot 2^{80} \cdot 3^{24}$	109.572602 %
42	$7^{16} \cdot 2^{32} \cdot 3^{28}$	7.116348 %	$2^{80} \cdot 17^{16} \cdot 3^{16}$	19.623875 %
43	$5^{16} \cdot 2^{84}$	6.77864 %	$2^{72} \cdot 11^{16} \cdot 3^{28}$	22.166666 %
44	$5^{16} \cdot 2^{116}$	113.557279 %	$7^{16} \cdot 2^{116} \cdot 3^{16}$	67.417623 %
45	$5^{24} \cdot 2^{64} \cdot 3^{16}$	79.326208 %	$5^{24} \cdot 7^{16} \cdot 2^{64} \cdot 3^{16}$	81.490932 %
46	$7^{16} \cdot 2^{64} \cdot 3^{16}$	41.894408 %	$5^{16} \cdot 2^{72} \cdot 11^{16} \cdot 3^{16}$	80.932778 %
47	$5^{16} \cdot 2^{96} \cdot 3^{24}$	215.6542 %	$5^{16} \cdot 7^{16} \cdot 2^{96} \cdot 3^{24}$	219.464599 %
48	$5^{16} \cdot 2^{64} \cdot 3^{16}$	19.922663 %	$5^{16} \cdot 7^{16} \cdot 2^{64} \cdot 3^{24}$	59.7323 %
49	$5^{16} \cdot 2^{72} \cdot 3^{16}$	42.612884 %	$5^{16} \cdot 7^{16} \cdot 2^{72} \cdot 3^{16}$	44.334426 %
50	$7^{16} \cdot 2^{32} \cdot 11^{16} \cdot 3^{16}$	135.305256 %	$5^{16} \cdot 7^{16} \cdot 2^{96} \cdot 3^{16}$	142.740603 %
51	$5^{16} \cdot 7^{16} \cdot 2^{64} \cdot 3^{16}$	217.285543 %	$5^{16} \cdot 7^{16} \cdot 2^{64} \cdot 11^{16} \cdot 3^{16}$	302.53975 %

The minimal discriminant for a totally complex field is attained by the group $(32, 11)$, with a root discriminant equal to 13.374806. For the totally real case, the minimum is attained by the group $(32, 38)$, with root discriminant equal to 37.474720.

Id	Signature $(0, 32)$	% bound	Signature $(64, 0)$	% bound
1	2^{447}	651.365 %	2^{447}	158.724 %
2	$2^{248} \cdot 17^{56}$	938.673 %	$2^{248} \cdot 17^{56}$	257.655 %
3	$5^{56} \cdot 2^{264}$	323.343 %	$5^{56} \cdot 2^{264}$	45.773 %
4	2^{282}	25.822 %	$2^{268} \cdot 17^{32}$	53.503 %
5	$13^{48} \cdot 17^{56}$	384.669 %	$7^{48} \cdot 2^{282}$	86.452 %
6	2^{286}	31.393 %	$7^{32} \cdot 2^{286}$	19.704 %
7	$7^{48} \cdot 2^{286}$	465.452 %	$7^{48} \cdot 2^{286}$	94.707 %
8	2^{266}	5.804 %	$5^{48} \cdot 181^{32} \cdot 3^{32}$	59.205 %
9	$13^{48} \cdot 2^{136} \cdot 3^{48}$	303.954 %	$13^{48} \cdot 2^{136} \cdot 3^{48}$	39.097 %
10	$5^{56} \cdot 2^{136}$	5.836 %	$5^{56} \cdot 2^{136} \cdot 19^{32}$	58.853 %
11	$7^{48} \cdot 2^{286}$	465.452 %	$7^{48} \cdot 2^{286}$	94.707 %
12	2^{286}	31.393 %	$2^{286} \cdot 31^{32}$	151.906 %
13	$7^{48} \cdot 2^{286}$	465.452 %	$7^{48} \cdot 2^{286}$	94.707 %
14	$5^{48} \cdot 2^{192} \cdot 17^{56}$	1793.673 %	$5^{48} \cdot 2^{192} \cdot 17^{56}$	552.065 %
15	$2^{286} \cdot 3^{56}$	243.6 %	$2^{286} \cdot 3^{56}$	18.315 %
16	$2^{268} \cdot 17^{56}$	1189.884 %	$2^{268} \cdot 17^{56}$	344.157 %
17	$2^{176} \cdot 17^{56}$	376.234 %	$2^{192} \cdot 17^{56}$	95.013 %
18	$5^{56} \cdot 41^{48}$	293.126 %	$5^{48} \cdot 29^{48} \cdot 3^{32}$	47.883 %
19	$5^{56} \cdot 29^{56}$	361.893 %	$5^{56} \cdot 29^{56} \cdot 2^{64}$	218.095 %
20	$5^{48} \cdot 29^{48}$	147.954 %	$2^{216} \cdot 17^{48}$	77.477 %
21	$5^{48} \cdot 101^{48}$	532.14 %	$2^{216} \cdot 17^{56}$	152.9 %
22	$5^{56} \cdot 29^{56}$	361.893 %	$5^{56} \cdot 29^{56} \cdot 3^{32}$	175.479 %
23	$5^{48} \cdot 29^{48}$	147.954 %	$5^{48} \cdot 29^{48} \cdot 2^{64}$	70.76 %

24	$13^{48} \cdot 17^{56}$	384.669 %	$5^{56} \cdot 29^{48} \cdot 3^{48}$	137.995 %
25	$5^{56} \cdot 29^{56}$	361.893 %	$2^{216} \cdot 17^{56}$	152.9 %
26	$5^{48} \cdot 17^{60}$	182.565 %	$5^{48} \cdot 17^{60} \cdot 3^{32}$	68.525 %
27	$2^{176} \cdot 17^{60}$	468.49 %	$2^{176} \cdot 17^{60}$	95.753 %
28	$5^{60} \cdot 13^{60}$	197.133 %	$5^{60} \cdot 2^{232}$	13.985 %
29	$2^{64} \cdot 17^{60}$	69.013 %	$2^{128} \cdot 17^{60}$	16.395 %
30	2^{326}	102.636 %	$13^{32} \cdot 2^{64} \cdot 17^{60}$	109.835 %
31	$2^{64} \cdot 17^{60}$	69.013 %	$7^{32} \cdot 2^{326}$	84.608 %
32	2^{274}	15.38 %	$2^{244} \cdot 17^{32}$	18.367 %
33	$5^{56} \cdot 29^{48}$	203.209 %	$7^{48} \cdot 2^{274}$	70.977 %
34	2^{274}	15.38 %	$7^{48} \cdot 2^{274}$	70.977 %
35	$5^{48} \cdot 41^{48}$	221.485 %	$2^{244} \cdot 17^{48}$	140.35 %
36	2^{282}	25.822 %	$2^{282} \cdot 31^{32}$	141.226 %
37	$7^{48} \cdot 2^{282}$	441.479 %	$7^{48} \cdot 2^{282}$	86.452 %
38	2^{302}	56.254 %	$5^{48} \cdot 181^{32} \cdot 3^{48}$	109.526 %
39	$7^{48} \cdot 2^{326}$	772.047 %	$7^{48} \cdot 2^{326}$	200.279 %
40	2^{302}	56.254 %	$5^{56} \cdot 3^{32} \cdot 101^{32}$	45.429 %
41	2^{302}	56.254 %	$7^{32} \cdot 2^{326}$	84.608 %
42	$5^{56} \cdot 19^{32}$	5.76 %	$5^{56} \cdot 11^{32} \cdot 31^{32}$	54.279 %
43	$13^{56} \cdot 53^{48}$	999.644 %	$5^{48} \cdot 89^{60}$	359.315 %
44	$2^{326} \cdot 3^{48}$	361.91 %	$2^{326} \cdot 3^{48}$	59.053 %
45	$2^{326} \cdot 3^{56}$	429.904 %	$2^{326} \cdot 3^{56}$	82.466 %
46	$2^{302} \cdot 3^{60}$	337.654 %	$2^{302} \cdot 3^{60}$	50.701 %
47	$2^{252} \cdot 17^{60}$	1194.78 %	$2^{252} \cdot 17^{60}$	345.843 %
48	$2^{252} \cdot 17^{60}$	1194.78 %	$2^{252} \cdot 17^{60}$	345.843 %
49	$2^{268} \cdot 17^{60}$	1439.762 %	$2^{268} \cdot 17^{60}$	430.199 %
50	2^{384}	279.773 %	$2^{384} \cdot 3^{32}$	126.501 %
51	$17^{62} \cdot 3^{48}$	110.467 %	$5^{56} \cdot 17^{62}$	29.995 %
52	$113^{32} \cdot 7^{32}$	66.891 %	$31^{32} \cdot 3^{32} \cdot 373^{32}$	280.563 %
53	2^{354}	174.421 %	$2^{128} \cdot 3^{48} \cdot 433^{32}$	287.682 %
54	$2^{384} \cdot 31^{48}$	4889.372 %	$2^{384} \cdot 31^{48}$	1618.033 %
55	$5^{48} \cdot 13^{48} \cdot 2^{176}$	813.823 %	$5^{48} \cdot 13^{48} \cdot 2^{192}$	274.201 %
56	$2^{176} \cdot 17^{48} \cdot 3^{32}$	478.861 %	$5^{48} \cdot 29^{48} \cdot 2^{64} \cdot 3^{32}$	195.765 %
57	$5^{48} \cdot 13^{48} \cdot 2^{176}$	813.823 %	$5^{48} \cdot 13^{48} \cdot 2^{176}$	214.665 %
58	$5^{48} \cdot 2^{200}$	73.098 %	$5^{48} \cdot 2^{216} \cdot 3^{32}$	22.771 %
59	$5^{48} \cdot 2^{208} \cdot 3^{48}$	330.289 %	$5^{48} \cdot 2^{208} \cdot 3^{48}$	48.165 %
60	$7^{32} \cdot 2^{216}$	62.881 %	$7^{32} \cdot 2^{216} \cdot 17^{32}$	131.249 %
61	$2^{224} \cdot 3^{48}$	53.035 %	$7^{32} \cdot 2^{224} \cdot 3^{48}$	39.42 %
62	$2^{192} \cdot 17^{48}$	297.44 %	$5^{48} \cdot 29^{48} \cdot 2^{96} \cdot 3^{32}$	318.275 %
63	$2^{216} \cdot 17^{48} \cdot 3^{48}$	1074.894 %	$2^{216} \cdot 17^{48} \cdot 3^{48}$	304.561 %
64	$5^{48} \cdot 13^{48} \cdot 29^{48}$	1597.572 %	$5^{48} \cdot 41^{48} \cdot 2^{176}$	644.695 %
65	$2^{216} \cdot 11^{48} \cdot 3^{48}$	747.63 %	$2^{216} \cdot 11^{48} \cdot 3^{48}$	191.872 %
66	$2^{220} \cdot 3^{48}$	46.547 %	$5^{32} \cdot 2^{224} \cdot 3^{48}$	17.831 %
67	$2^{224} \cdot 3^{32}$	16.281 %	$7^{48} \cdot 2^{220} \cdot 3^{32}$	65.008 %
68	$5^{48} \cdot 2^{208} \cdot 3^{48}$	330.289 %	$5^{48} \cdot 2^{208} \cdot 3^{48}$	48.165 %
69	$2^{212} \cdot 3^{48}$	34.384 %	$5^{48} \cdot 2^{192} \cdot 3^{48}$	24.592 %
70	$5^{48} \cdot 2^{216} \cdot 3^{48}$	369.234 %	$5^{48} \cdot 2^{216} \cdot 3^{48}$	61.575 %
71	$5^{48} \cdot 2^{96} \cdot 3^{48}$	27.926 %	$5^{48} \cdot 2^{96} \cdot 11^{32} \cdot 3^{48}$	46.097 %
72	$5^{48} \cdot 2^{224} \cdot 3^{48}$	411.703 %	$5^{48} \cdot 2^{224} \cdot 3^{48}$	76.199 %
73	$13^{32} \cdot 2^{96} \cdot 3^{48}$	37.944 %	$2^{176} \cdot 11^{48} \cdot 3^{48}$	89.255 %
74	$2^{224} \cdot 3^{48}$	53.035 %	$2^{224} \cdot 3^{48} \cdot 23^{32}$	152.72 %
75	$2^{196} \cdot 3^{48}$	13.003 %	$7^{48} \cdot 2^{196} \cdot 3^{48}$	67.455 %
76	$7^{48} \cdot 2^{220} \cdot 3^{48}$	530.666 %	$7^{48} \cdot 2^{220} \cdot 3^{48}$	117.163 %
77	$2^{220} \cdot 3^{48}$	46.547 %	$7^{48} \cdot 2^{220} \cdot 3^{48}$	117.163 %
78	$2^{224} \cdot 3^{48}$	53.035 %	$2^{224} \cdot 3^{48} \cdot 23^{32}$	152.72 %
79	$7^{48} \cdot 2^{212} \cdot 3^{48}$	478.324 %	$7^{48} \cdot 2^{212} \cdot 3^{48}$	99.139 %
80	$2^{212} \cdot 3^{48}$	34.384 %	$2^{212} \cdot 3^{48} \cdot 23^{32}$	121.92 %
81	$7^{48} \cdot 2^{224} \cdot 3^{48}$	558.588 %	$7^{48} \cdot 2^{224} \cdot 3^{48}$	126.777 %

82	$13^{48} \cdot 17^{48} \cdot 53^{48}$	6581.066 %	$13^{48} \cdot 17^{48} \cdot 53^{48}$	2200.548 %
83	$5^{48} \cdot 2^{256}$	217.462 %	$5^{48} \cdot 2^{256} \cdot 3^{32}$	89.338 %
84	$5^{56} \cdot 2^{208}$	130.829 %	$5^{56} \cdot 2^{208} \cdot 3^{32}$	37.669 %
85	$5^{56} \cdot 2^{208}$	130.829 %	$5^{56} \cdot 2^{200} \cdot 3^{48}$	66.146 %
86	$5^{56} \cdot 2^{216}$	151.721 %	$5^{56} \cdot 2^{216} \cdot 3^{32}$	50.129 %
87	$2^{268} \cdot 3^{32}$	87.27 %	$2^{128} \cdot 17^{56} \cdot 3^{32}$	68.886 %
88	$5^{56} \cdot 2^{168}$	49.674 %	$5^{56} \cdot 2^{168} \cdot 11^{32}$	70.934 %
89	$5^{56} \cdot 2^{96} \cdot 3^{32}$	18.864 %	$5^{56} \cdot 2^{96} \cdot 11^{32} \cdot 3^{32}$	35.747 %
90	$5^{48} \cdot 2^{112} \cdot 3^{32}$	15.594 %	$7^{32} \cdot 2^{244} \cdot 3^{32}$	31.558 %
91	$7^{32} \cdot 2^{208}$	49.362 %	$5^{48} \cdot 2^{244} \cdot 3^{32}$	66.263 %
92	$5^{56} \cdot 2^{152}$	25.861 %	$5^{56} \cdot 2^{152} \cdot 19^{32}$	88.909 %
93	$7^{48} \cdot 2^{268}$	365.298 %	$13^{56} \cdot 2^{168} \cdot 3^{48}$	171.066 %
94	$5^{56} \cdot 2^{184}$	77.994 %	$7^{32} \cdot 2^{268} \cdot 3^{32}$	70.609 %
95	$5^{48} \cdot 3^{32} \cdot 19^{32}$	49.799 %	$7^{32} \cdot 2^{268} \cdot 3^{32}$	70.609 %
96	$13^{48} \cdot 2^{128} \cdot 3^{48}$	270.427 %	$13^{48} \cdot 2^{160} \cdot 3^{48}$	80.386 %
97	$5^{48} \cdot 2^{128} \cdot 3^{32}$	37.465 %	$5^{48} \cdot 29^{32} \cdot 2^{64} \cdot 3^{32}$	27.452 %
98	$5^{56} \cdot 2^{128} \cdot 3^{32}$	68.099 %	$7^{32} \cdot 2^{252} \cdot 3^{32}$	43.465 %
99	$5^{48} \cdot 2^{168}$	22.398 %	$5^{56} \cdot 2^{168} \cdot 11^{32}$	70.934 %
100	$13^{48} \cdot 2^{128} \cdot 3^{48}$	270.427 %	$5^{56} \cdot 2^{252} \cdot 3^{48}$	191.793 %
101	$5^{48} \cdot 2^{160}$	12.24 %	$5^{48} \cdot 2^{160} \cdot 11^{32}$	28.183 %
102	$5^{48} \cdot 2^{64} \cdot 11^{32}$	31.613 %	$2^{216} \cdot 17^{32} \cdot 3^{32}$	51.388 %
103	$2^{268} \cdot 3^{48}$	146.461 %	$5^{32} \cdot 2^{268} \cdot 3^{48}$	89.766 %
104	$5^{56} \cdot 7^{48} \cdot 3^{48}$	138.017 %	$5^{56} \cdot 2^{200} \cdot 3^{48}$	66.146 %
105	$5^{56} \cdot 7^{48} \cdot 3^{48}$	138.017 %	$5^{56} \cdot 7^{48} \cdot 2^{64} \cdot 3^{48}$	63.917 %
106	$2^{252} \cdot 3^{56}$	137.756 %	$5^{32} \cdot 2^{252} \cdot 3^{56}$	83.064 %
107	$2^{216} \cdot 17^{56}$	634.452 %	$2^{216} \cdot 17^{56} \cdot 3^{32}$	338.036 %
108	$2^{252} \cdot 3^{56}$	137.756 %	$7^{32} \cdot 2^{252} \cdot 3^{56}$	116.604 %
109	$2^{252} \cdot 3^{56}$	137.756 %	$5^{32} \cdot 2^{252} \cdot 3^{56}$	83.064 %
110	$2^{268} \cdot 3^{56}$	182.741 %	$5^{32} \cdot 2^{268} \cdot 3^{56}$	117.701 %
111	$2^{268} \cdot 3^{56}$	182.741 %	$5^{32} \cdot 2^{268} \cdot 3^{56}$	117.701 %
112	$2^{264} \cdot 3^{48}$	136.012 %	$7^{32} \cdot 2^{264} \cdot 3^{48}$	115.015 %
113	$5^{56} \cdot 2^{208}$	130.829 %	$5^{56} \cdot 2^{168} \cdot 3^{48}$	17.483 %
114	$2^{264} \cdot 3^{48}$	136.012 %	$5^{56} \cdot 2^{192} \cdot 3^{48}$	52.356 %
115	$2^{264} \cdot 3^{32}$	79.33 %	$5^{32} \cdot 2^{268} \cdot 3^{32}$	44.191 %
116	$5^{56} \cdot 2^{64} \cdot 3^{48}$	10.615 %	$5^{56} \cdot 2^{192} \cdot 3^{32}$	15.766 %
117	$5^{56} \cdot 2^{192}$	94.104 %	$5^{56} \cdot 2^{192} \cdot 3^{48}$	52.356 %
118	$5^{48} \cdot 13^{32} \cdot 3^{32}$	23.909 %	$2^{252} \cdot 11^{32} \cdot 3^{32}$	79.843 %
119	$2^{208} \cdot 3^{56}$	47.63 %	$13^{32} \cdot 2^{208} \cdot 3^{48}$	59.768 %
120	$7^{56} \cdot 2^{208} \cdot 3^{48}$	606.308 %	$7^{56} \cdot 2^{208} \cdot 3^{48}$	143.209 %
121	$5^{48} \cdot 2^{212}$	97.122 %	$5^{56} \cdot 2^{232} \cdot 3^{32}$	78.535 %
122	$5^{48} \cdot 2^{232} \cdot 3^{56}$	540.158 %	$5^{48} \cdot 2^{232} \cdot 3^{56}$	120.431 %
123	$5^{56} \cdot 2^{96} \cdot 3^{32}$	18.864 %	$5^{48} \cdot 7^{32} \cdot 17^{32} \cdot 3^{32}$	29.09 %
124	$5^{48} \cdot 2^{64} \cdot 3^{56}$	3.773 %	$5^{32} \cdot 13^{32} \cdot 2^{192}$	31.788 %
125	$2^{232} \cdot 3^{32}$	26.806 %	$5^{32} \cdot 2^{252} \cdot 3^{32}$	21.25 %
126	$5^{48} \cdot 2^{264} \cdot 3^{48}$	689.154 %	$7^{48} \cdot 2^{264} \cdot 3^{48}$	249.739 %
127	$5^{56} \cdot 2^{200} \cdot 3^{48}$	382.506 %	$5^{56} \cdot 2^{200} \cdot 3^{48}$	66.146 %
128	$2^{144} \cdot 17^{32}$	16.382 %	$2^{128} \cdot 17^{32} \cdot 19^{32}$	46.89 %
129	$7^{32} \cdot 2^{128} \cdot 3^{56}$	64.223 %	$5^{32} \cdot 2^{252} \cdot 3^{56}$	83.064 %
130	$5^{32} \cdot 2^{196}$	10.85 %	$2^{184} \cdot 11^{32} \cdot 3^{56}$	30.008 %
131	$2^{192} \cdot 3^{56}$	24.141 %	$13^{32} \cdot 2^{192} \cdot 3^{48}$	34.349 %
132	$7^{56} \cdot 2^{128} \cdot 3^{48}$	196.966 %	$7^{48} \cdot 2^{236} \cdot 3^{32}$	96.229 %
133	$2^{236} \cdot 3^{48}$	74.274 %	$5^{32} \cdot 7^{56} \cdot 2^{96} \cdot 3^{56}$	85.482 %
134	$5^{32} \cdot 2^{204}$	20.882 %	$7^{32} \cdot 2^{176} \cdot 17^{32}$	49.946 %
135	$7^{32} \cdot 2^{192}$	25.598 %	$2^{216} \cdot 11^{32} \cdot 3^{56}$	83.859 %
136	$2^{204} \cdot 3^{56}$	41.371 %	$2^{192} \cdot 11^{32} \cdot 3^{56}$	41.774 %
137	$7^{32} \cdot 2^{216}$	62.881 %	$13^{32} \cdot 2^{220} \cdot 3^{48}$	81.942 %
138	$7^{32} \cdot 2^{184}$	15.174 %	$5^{32} \cdot 2^{244} \cdot 3^{48}$	46.33 %
139	$2^{204} \cdot 3^{48}$	23.231 %	$2^{192} \cdot 11^{32} \cdot 3^{48}$	23.583 %

140	$5^{32} \cdot 2^{212}$	31.823 %	$7^{32} \cdot 2^{240} \cdot 3^{48}$	65.799 %
141	$2^{208} \cdot 3^{56}$	47.63 %	$5^{48} \cdot 2^{240} \cdot 3^{56}$	140.382 %
142	$2^{240} \cdot 3^{48}$	81.99 %	$7^{32} \cdot 2^{240} \cdot 3^{48}$	65.799 %
143	$7^{56} \cdot 2^{208} \cdot 3^{48}$	606.308 %	$7^{56} \cdot 2^{208} \cdot 3^{48}$	143.209 %
144	$5^{32} \cdot 2^{128} \cdot 3^{48}$	20.985 %	$2^{192} \cdot 17^{32} \cdot 3^{48}$	53.633 %
145	$2^{236} \cdot 3^{48}$	74.274 %	$5^{48} \cdot 2^{240} \cdot 3^{56}$	140.382 %
146	$2^{192} \cdot 3^{56}$	24.141 %	$7^{32} \cdot 2^{240} \cdot 3^{56}$	90.205 %
147	$2^{240} \cdot 3^{32}$	38.283 %	$13^{32} \cdot 61^{32} \cdot 2^{64} \cdot 3^{32}$	99.323 %
148	$7^{56} \cdot 2^{128} \cdot 3^{48}$	196.966 %	$7^{56} \cdot 2^{192} \cdot 3^{48}$	104.514 %
149	$2^{240} \cdot 3^{48}$	81.99 %	$7^{56} \cdot 2^{196} \cdot 3^{48}$	113.568 %
150	$2^{196} \cdot 3^{56}$	29.637 %	$2^{196} \cdot 3^{56} \cdot 23^{32}$	114.082 %
151	$2^{240} \cdot 3^{56}$	108.78 %	$5^{56} \cdot 2^{240} \cdot 3^{48}$	156.231 %
152	$2^{216} \cdot 3^{32}$	6.631 %	$7^{32} \cdot 2^{216} \cdot 3^{56}$	46.668 %
153	$13^{32} \cdot 2^{64} \cdot 3^{56}$	11.899 %	$5^{32} \cdot 41^{32} \cdot 7^{32} \cdot 3^{48}$	76.44 %
154	$2^{216} \cdot 3^{56}$	60.991 %	$5^{56} \cdot 2^{216} \cdot 3^{56}$	126.666 %
155	$2^{252} \cdot 3^{48}$	107.248 %	$7^{32} \cdot 2^{252} \cdot 3^{48}$	88.81 %
156	$5^{48} \cdot 2^{252} \cdot 3^{56}$	694.985 %	$5^{48} \cdot 2^{252} \cdot 3^{56}$	173.744 %
157	$2^{208} \cdot 3^{56}$	47.63 %	$2^{200} \cdot 11^{32} \cdot 3^{56}$	54.606 %
158	$7^{56} \cdot 2^{208} \cdot 3^{48}$	606.308 %	$7^{56} \cdot 2^{208} \cdot 3^{48}$	143.209 %
159	$2^{220} \cdot 3^{56}$	68.119 %	$5^{32} \cdot 2^{264} \cdot 3^{48}$	81.721 %
160	$5^{48} \cdot 2^{264} \cdot 3^{48}$	689.154 %	$5^{48} \cdot 2^{264} \cdot 3^{48}$	171.736 %
161	$2^{264} \cdot 3^{32}$	79.33 %	$7^{56} \cdot 2^{212} \cdot 3^{48}$	153.977 %
162	$2^{176} \cdot 3^{56}$	4.39 %	$5^{32} \cdot 2^{240} \cdot 3^{56}$	60.753 %
163	$2^{196} \cdot 3^{56}$	29.637 %	$2^{196} \cdot 3^{56} \cdot 23^{32}$	114.082 %
164	$2^{240} \cdot 3^{56}$	108.78 %	$5^{32} \cdot 2^{240} \cdot 3^{56}$	60.753 %
165	$13^{48} \cdot 2^{128} \cdot 3^{48}$	270.427 %	$7^{56} \cdot 2^{176} \cdot 3^{48}$	71.975 %
166	$2^{240} \cdot 3^{56}$	108.78 %	$7^{56} \cdot 2^{196} \cdot 3^{48}$	113.568 %
167	$2^{240} \cdot 3^{48}$	81.99 %	$7^{48} \cdot 2^{240} \cdot 3^{48}$	169.685 %
168	$7^{48} \cdot 2^{240} \cdot 3^{48}$	683.198 %	$7^{48} \cdot 2^{240} \cdot 3^{48}$	169.685 %
169	$2^{240} \cdot 3^{48}$	81.99 %	$5^{48} \cdot 7^{48} \cdot 2^{240}$	295.589 %
170	$2^{240} \cdot 3^{48}$	81.99 %	$5^{56} \cdot 2^{128} \cdot 11^{32} \cdot 3^{48}$	152.654 %
171	$2^{240} \cdot 3^{48}$	81.99 %	$5^{56} \cdot 2^{240} \cdot 3^{48}$	156.231 %
172	$5^{56} \cdot 2^{240} \cdot 3^{48}$	644.127 %	$5^{56} \cdot 2^{240} \cdot 3^{48}$	156.231 %
173	$2^{208} \cdot 3^{56}$	47.63 %	$2^{208} \cdot 3^{56} \cdot 23^{32}$	143.794 %
174	$7^{56} \cdot 2^{96} \cdot 3^{48}$	109.987 %	$2^{176} \cdot 73^{32} \cdot 3^{48}$	167.71 %
175	$2^{216} \cdot 17^{56} \cdot 3^{48}$	1574.19 %	$2^{216} \cdot 17^{56} \cdot 3^{48}$	476.488 %
176	$2^{220} \cdot 3^{56}$	68.119 %	$2^{220} \cdot 3^{56} \cdot 23^{32}$	177.63 %
177	$2^{212} \cdot 3^{56}$	54.166 %	$5^{56} \cdot 2^{128} \cdot 11^{32} \cdot 3^{48}$	152.654 %
178	$5^{56} \cdot 2^{128} \cdot 3^{48}$	121.23 %	$5^{56} \cdot 2^{128} \cdot 11^{32} \cdot 3^{48}$	152.654 %
179	$2^{200} \cdot 11^{48} \cdot 3^{56}$	717.691 %	$2^{200} \cdot 11^{48} \cdot 3^{56}$	181.562 %
180	$7^{56} \cdot 2^{220} \cdot 3^{48}$	704.335 %	$7^{56} \cdot 2^{220} \cdot 3^{48}$	176.964 %
181	$7^{56} \cdot 2^{208} \cdot 3^{48}$	606.308 %	$7^{56} \cdot 2^{208} \cdot 3^{48}$	143.209 %
182	$7^{56} \cdot 2^{212} \cdot 3^{48}$	637.578 %	$7^{56} \cdot 2^{212} \cdot 3^{48}$	153.977 %
183	$2^{64} \cdot 17^{60} \cdot 3^{32}$	192.739 %	$2^{128} \cdot 17^{60} \cdot 3^{32}$	101.603 %
184	$2^{64} \cdot 17^{60} \cdot 3^{32}$	192.739 %	$5^{32} \cdot 2^{96} \cdot 17^{60}$	84.037 %
185	$2^{320} \cdot 3^{32}$	228.893 %	$5^{32} \cdot 2^{320} \cdot 3^{32}$	153.236 %
186	$41^{32} \cdot 2^{144}$	80.74 %	$2^{176} \cdot 17^{32} \cdot 19^{32}$	147.038 %
187	$5^{32} \cdot 7^{60} \cdot 3^{48}$	87.478 %	$7^{32} \cdot 2^{192} \cdot 71^{32}$	264.417 %
188	$7^{48} \cdot 2^{320}$	717.181 %	$7^{48} \cdot 2^{320} \cdot 3^{32}$	387.376 %
189	$5^{32} \cdot 3^{32} \cdot 37^{32}$	39.795 %	$5^{32} \cdot 113^{32} \cdot 2^{96}$	37.372 %
190	$5^{32} \cdot 11^{32} \cdot 3^{56}$	15.082 %	$29^{32} \cdot 2^{96} \cdot 3^{32} \cdot 19^{32}$	134.97 %
191	$7^{60} \cdot 2^{160}$	108.065 %	$2^{160} \cdot 193^{32} \cdot 3^{48}$	266.037 %
192	$5^{48} \cdot 2^{192} \cdot 3^{32}$	174.93 %	$5^{48} \cdot 7^{32} \cdot 2^{192} \cdot 3^{32}$	150.471 %
193	$5^{48} \cdot 2^{144} \cdot 3^{32}$	63.475 %	$5^{48} \cdot 2^{144} \cdot 11^{32} \cdot 3^{32}$	86.695 %
194	$5^{32} \cdot 2^{216} \cdot 3^{48}$	213.796 %	$5^{48} \cdot 7^{48} \cdot 2^{128} \cdot 3^{48}$	168.091 %
195	$5^{48} \cdot 2^{160} \cdot 3^{48}$	155.852 %	$5^{48} \cdot 7^{32} \cdot 2^{160} \cdot 3^{48}$	133.09 %
196	$5^{48} \cdot 2^{128} \cdot 3^{32}$	37.465 %	$5^{48} \cdot 7^{32} \cdot 2^{128} \cdot 3^{48}$	64.819 %
197	$5^{48} \cdot 7^{32} \cdot 2^{208} \cdot 3^{48}$	1038.439 %	$5^{48} \cdot 7^{32} \cdot 2^{208} \cdot 11^{32} \cdot 3^{48}$	1200.144 %

198	$5^{48} \cdot 2^{160} \cdot 3^{32}$	94.405 %	$5^{48} \cdot 7^{32} \cdot 2^{160} \cdot 3^{32}$	77.11 %
199	$5^{48} \cdot 2^{144} \cdot 3^{32}$	63.475 %	$5^{48} \cdot 7^{32} \cdot 2^{144} \cdot 3^{32}$	48.931 %
200	$5^{48} \cdot 2^{192} \cdot 3^{48}$	261.829 %	$5^{48} \cdot 7^{48} \cdot 2^{160} \cdot 3^{48}$	279.138 %
201	$5^{48} \cdot 2^{160} \cdot 3^{32}$	94.405 %	$5^{32} \cdot 7^{32} \cdot 2^{216} \cdot 3^{32}$	117.221 %
202	$5^{32} \cdot 2^{184} \cdot 3^{32}$	68.598 %	$5^{32} \cdot 41^{32} \cdot 2^{128} \cdot 3^{32}$	102.688 %
203	$7^{32} \cdot 2^{128} \cdot 3^{48}$	43.151 %	$5^{32} \cdot 2^{144} \cdot 11^{32} \cdot 3^{48}$	64.312 %
204	$5^{32} \cdot 2^{192} \cdot 3^{48}$	141.969 %	$5^{32} \cdot 7^{32} \cdot 2^{208} \cdot 3^{48}$	162.152 %
205	$5^{32} \cdot 2^{168} \cdot 3^{48}$	86.584 %	$5^{32} \cdot 7^{48} \cdot 2^{128} \cdot 3^{48}$	79.283 %
206	$5^{32} \cdot 2^{128} \cdot 3^{48}$	20.985 %	$5^{32} \cdot 7^{32} \cdot 2^{168} \cdot 3^{48}$	69.984 %
207	$5^{48} \cdot 2^{144} \cdot 3^{48}$	115.145 %	$5^{48} \cdot 2^{144} \cdot 11^{32} \cdot 3^{48}$	145.704 %
208	$5^{48} \cdot 2^{208} \cdot 3^{48}$	330.289 %	$5^{48} \cdot 7^{32} \cdot 2^{208} \cdot 3^{48}$	292.008 %
209	$5^{32} \cdot 2^{208} \cdot 3^{48}$	187.752 %	$5^{48} \cdot 7^{32} \cdot 2^{192} \cdot 3^{48}$	229.638 %
210	$5^{32} \cdot 2^{160} \cdot 3^{48}$	71.098 %	$5^{32} \cdot 7^{32} \cdot 2^{160} \cdot 3^{48}$	55.876 %
211	$5^{32} \cdot 2^{176} \cdot 3^{48}$	103.471 %	$5^{48} \cdot 2^{144} \cdot 11^{32} \cdot 3^{48}$	145.704 %
212	$5^{48} \cdot 2^{216} \cdot 3^{48}$	369.234 %	$5^{32} \cdot 7^{48} \cdot 2^{200} \cdot 3^{48}$	291.02 %
213	$7^{32} \cdot 2^{160} \cdot 3^{32}$	53.826 %	$5^{32} \cdot 7^{32} \cdot 2^{176} \cdot 3^{48}$	85.369 %
214	$5^{48} \cdot 2^{192} \cdot 3^{48}$	261.829 %	$5^{32} \cdot 7^{48} \cdot 2^{192} \cdot 3^{48}$	258.567 %
215	$5^{32} \cdot 2^{168} \cdot 3^{32}$	41.773 %	$5^{32} \cdot 2^{168} \cdot 11^{32} \cdot 3^{32}$	61.911 %
216	$5^{32} \cdot 2^{184} \cdot 3^{32}$	68.598 %	$5^{32} \cdot 13^{32} \cdot 2^{184} \cdot 3^{32}$	109.319 %
217	$5^{32} \cdot 2^{192} \cdot 3^{48}$	141.969 %	$5^{32} \cdot 7^{48} \cdot 2^{200} \cdot 3^{32}$	197.111 %
218	$7^{32} \cdot 2^{64} \cdot 11^{32} \cdot 3^{32}$	80.377 %	$5^{32} \cdot 7^{32} \cdot 2^{208} \cdot 3^{32}$	99.192 %
219	$5^{32} \cdot 2^{168} \cdot 3^{32}$	41.773 %	$5^{32} \cdot 7^{32} \cdot 2^{192} \cdot 3^{32}$	67.5 %
220	$5^{32} \cdot 2^{208} \cdot 3^{32}$	118.644 %	$5^{32} \cdot 7^{32} \cdot 2^{216} \cdot 3^{32}$	117.221 %
221	$5^{32} \cdot 7^{32} \cdot 2^{64} \cdot 3^{32}$	21.61 %	$5^{32} \cdot 7^{32} \cdot 2^{168} \cdot 3^{32}$	29.16 %
222	$5^{48} \cdot 2^{192} \cdot 3^{48}$	261.829 %	$5^{48} \cdot 2^{192} \cdot 11^{32} \cdot 3^{48}$	313.224 %
223	$5^{48} \cdot 2^{160} \cdot 3^{32}$	94.405 %	$5^{32} \cdot 7^{32} \cdot 2^{192} \cdot 3^{48}$	120.442 %
224	$5^{32} \cdot 2^{200} \cdot 3^{48}$	163.87 %	$5^{32} \cdot 7^{32} \cdot 2^{200} \cdot 3^{48}$	140.394 %
225	$5^{48} \cdot 2^{200} \cdot 3^{48}$	294.577 %	$5^{48} \cdot 7^{32} \cdot 2^{200} \cdot 3^{48}$	259.473 %
226	$7^{32} \cdot 2^{144} \cdot 3^{32}$	29.352 %	$5^{32} \cdot 2^{184} \cdot 11^{32} \cdot 3^{32}$	92.546 %
227	$5^{32} \cdot 2^{144} \cdot 3^{32}$	9.322 %	$5^{32} \cdot 7^{32} \cdot 2^{144} \cdot 3^{48}$	31.076 %
228	$5^{32} \cdot 2^{192} \cdot 3^{32}$	83.857 %	$5^{32} \cdot 7^{32} \cdot 2^{208} \cdot 3^{32}$	99.192 %
229	$5^{32} \cdot 2^{176} \cdot 3^{48}$	103.471 %	$5^{32} \cdot 2^{192} \cdot 3^{32} \cdot 19^{32}$	175.958 %
230	$5^{32} \cdot 2^{200} \cdot 3^{48}$	163.87 %	$5^{32} \cdot 7^{32} \cdot 2^{200} \cdot 3^{48}$	140.394 %
231	$5^{32} \cdot 2^{176} \cdot 3^{32}$	54.605 %	$5^{32} \cdot 13^{32} \cdot 7^{32} \cdot 2^{64} \cdot 3^{48}$	98.704 %
232	$5^{32} \cdot 2^{160} \cdot 3^{48}$	71.098 %	$5^{32} \cdot 7^{32} \cdot 2^{168} \cdot 3^{48}$	69.984 %
233	$5^{32} \cdot 2^{192} \cdot 3^{48}$	141.969 %	$5^{32} \cdot 7^{48} \cdot 2^{160} \cdot 3^{48}$	153.545 %
234	$5^{32} \cdot 2^{160} \cdot 3^{32}$	30.007 %	$5^{32} \cdot 7^{32} \cdot 2^{160} \cdot 3^{48}$	55.876 %
235	$5^{32} \cdot 2^{192} \cdot 3^{48}$	141.969 %	$5^{32} \cdot 7^{32} \cdot 2^{192} \cdot 3^{48}$	120.442 %
236	$5^{48} \cdot 2^{160} \cdot 3^{32}$	94.405 %	$5^{32} \cdot 7^{48} \cdot 2^{160} \cdot 3^{32}$	92.652 %
237	$5^{48} \cdot 2^{160} \cdot 3^{48}$	155.852 %	$5^{32} \cdot 7^{48} \cdot 2^{160} \cdot 3^{48}$	153.545 %
238	$5^{48} \cdot 7^{48} \cdot 2^{192} \cdot 3^{48}$	1457.136 %	$5^{48} \cdot 7^{48} \cdot 2^{192} \cdot 3^{48}$	436.182 %
239	$5^{48} \cdot 7^{48} \cdot 2^{192} \cdot 3^{48}$	1457.136 %	$5^{48} \cdot 7^{48} \cdot 2^{192} \cdot 3^{48}$	436.182 %
240	$5^{32} \cdot 2^{192} \cdot 3^{32}$	83.857 %	$5^{32} \cdot 7^{32} \cdot 2^{192} \cdot 3^{48}$	120.442 %
241	$5^{32} \cdot 2^{168} \cdot 3^{32}$	41.773 %	$5^{32} \cdot 7^{32} \cdot 2^{184} \cdot 3^{32}$	53.598 %
242	$5^{32} \cdot 2^{192} \cdot 3^{48}$	141.969 %	$5^{48} \cdot 7^{32} \cdot 2^{200} \cdot 3^{32}$	173.141 %
243	$5^{32} \cdot 7^{48} \cdot 2^{64} \cdot 3^{32}$	97.808 %	$5^{32} \cdot 7^{32} \cdot 2^{200} \cdot 3^{32}$	82.66 %
244	$5^{32} \cdot 2^{216} \cdot 3^{48}$	213.796 %	$5^{48} \cdot 7^{32} \cdot 2^{200} \cdot 3^{32}$	173.141 %
245	$5^{48} \cdot 7^{48} \cdot 2^{208} \cdot 3^{48}$	1751.758 %	$5^{48} \cdot 7^{48} \cdot 2^{208} \cdot 3^{48}$	537.631 %
246	$5^{32} \cdot 2^{256} \cdot 3^{32}$	267.714 %	$5^{32} \cdot 7^{32} \cdot 2^{256} \cdot 3^{32}$	235.0 %
247	$5^{56} \cdot 2^{128} \cdot 3^{48}$	121.23 %	$5^{56} \cdot 7^{32} \cdot 2^{160} \cdot 3^{32}$	116.578 %
248	$5^{56} \cdot 2^{128} \cdot 3^{32}$	68.099 %	$5^{56} \cdot 7^{32} \cdot 2^{128} \cdot 3^{32}$	53.144 %
249	$5^{56} \cdot 2^{144} \cdot 3^{32}$	99.904 %	$5^{56} \cdot 7^{32} \cdot 2^{144} \cdot 3^{32}$	82.119 %
250	$7^{32} \cdot 2^{176} \cdot 3^{32}$	82.931 %	$7^{48} \cdot 2^{128} \cdot 17^{32} \cdot 3^{32}$	151.188 %
251	$5^{32} \cdot 2^{160} \cdot 3^{56}$	96.284 %	$5^{32} \cdot 13^{32} \cdot 2^{160} \cdot 3^{48}$	112.424 %
252	$7^{56} \cdot 2^{160} \cdot 3^{48}$	319.973 %	$5^{32} \cdot 7^{56} \cdot 2^{160} \cdot 3^{48}$	223.364 %
253	$5^{32} \cdot 2^{160} \cdot 3^{32}$	30.007 %	$5^{32} \cdot 29^{32} \cdot 2^{128} \cdot 3^{32}$	70.465 %
254	$2^{128} \cdot 11^{32} \cdot 3^{32}$	36.352 %	$5^{32} \cdot 7^{32} \cdot 2^{64} \cdot 17^{32} \cdot 3^{32}$	72.655 %
255	$7^{32} \cdot 2^{160} \cdot 3^{56}$	132.247 %	$5^{32} \cdot 7^{56} \cdot 2^{160} \cdot 3^{32}$	145.704 %

256	$7^{32} \cdot 2^{128} \cdot 3^{32}$	8.771 %	$5^{32} \cdot 2^{128} \cdot 11^{32} \cdot 3^{56}$	58.509 %
257	$7^{32} \cdot 2^{144} \cdot 3^{32}$	29.352 %	$5^{32} \cdot 13^{32} \cdot 2^{168} \cdot 3^{32}$	76.016 %
258	$5^{32} \cdot 2^{160} \cdot 3^{32}$	30.007 %	$5^{32} \cdot 2^{160} \cdot 11^{32} \cdot 3^{32}$	48.473 %
259	$5^{32} \cdot 2^{160} \cdot 3^{48}$	71.098 %	$13^{32} \cdot 7^{32} \cdot 2^{160} \cdot 3^{32}$	90.979 %
260	$5^{48} \cdot 7^{32} \cdot 2^{128} \cdot 3^{32}$	263.699 %	$5^{48} \cdot 7^{32} \cdot 2^{128} \cdot 11^{32} \cdot 3^{32}$	315.359 %
261	$5^{32} \cdot 7^{32} \cdot 2^{128} \cdot 3^{32}$	143.22 %	$5^{32} \cdot 13^{32} \cdot 7^{32} \cdot 2^{128} \cdot 3^{32}$	201.965 %
262	$5^{32} \cdot 7^{32} \cdot 2^{192} \cdot 3^{48}$	540.191 %	$5^{32} \cdot 7^{32} \cdot 2^{192} \cdot 11^{32} \cdot 3^{48}$	631.125 %
263	$5^{32} \cdot 7^{32} \cdot 2^{128} \cdot 3^{32}$	143.22 %	$5^{32} \cdot 7^{32} \cdot 2^{128} \cdot 11^{32} \cdot 3^{32}$	177.767 %
264	$5^{32} \cdot 7^{32} \cdot 2^{128} \cdot 3^{32}$	143.22 %	$5^{32} \cdot 7^{32} \cdot 2^{128} \cdot 11^{32} \cdot 3^{32}$	177.767 %
265	$5^{32} \cdot 7^{32} \cdot 2^{160} \cdot 3^{32}$	243.965 %	$5^{32} \cdot 7^{32} \cdot 2^{128} \cdot 11^{32} \cdot 3^{48}$	265.562 %
266	$5^{32} \cdot 7^{32} \cdot 2^{128} \cdot 3^{32}$	143.22 %	$5^{32} \cdot 7^{32} \cdot 2^{128} \cdot 11^{32} \cdot 3^{32}$	177.767 %
267	$5^{32} \cdot 7^{32} \cdot 2^{128} \cdot 11^{32} \cdot 3^{32}$	706.67 %	$5^{32} \cdot 13^{32} \cdot 7^{32} \cdot 2^{128} \cdot 11^{32} \cdot 3^{32}$	901.505 %

In the case of degree 64 fields, the minimum is attained at the group $(64, 124)$ for the totally complex fields: the root discriminant is 17.487937. For the totally real fields, the minimum is attained by the group $(64, 28)$, with root discriminant equal to 55.785086.

For the groups $(64, 54)$ and $(64, 82)$, the task is particularly difficult as the minimal discriminants are quite large. In order to find them, we used some ad-hoc constraints. By using the derived series, the quotient by the derived subgroup is isomorphic to $C_2 \times C_2$ in the case of $(64, 54)$, while in the case of $(64, 82)$ it is isomorphic to C_2^3. The second step is to extend these fields by C_{16} and C_2^3 extensions respectively.

By Lemma 1.6, we notice that every prime ideal ramified in the maximal abelian subextension must ramify further. This allows us to get a better bound for the discriminant of the extensions of the first layer. We now discuss this for both cases.

$(64, 54)$ Let L be a field with Galois group isomorphic to Q_{64}, the generalized quaternion group of order 64 and let K be its subfield with Galois group isomorphic to $C_2 \times C_2$. Let p be a prime number different from 2 which is ramified in K. Since every prime of K lying over p must ramify in L, for each prime $\mathfrak{p}$ lying over p we have $v_{\mathfrak{p}}(\operatorname{disc} L/K) \geq 8$ by Lemma 4.30. Thus we have $v_p(\operatorname{disc} L) \geq 16 v_p(\operatorname{disc} K) + 16$. Applying again Lemma 4.30, we get $v_p(\operatorname{disc} K) = 2$ and consequently $v_p(\operatorname{disc} L) \geq 24 v_p(\operatorname{disc} K)$. We now consider the case $p = 2$ and assume that it ramifies in K. Then 2 must be wildly ramified in L/K and $\mathfrak{p}^2$ divides the conductor of L/K by Lemma 1.16, where $\mathfrak{p}$ is any prime ideal of K lying over 2. Thus the valuation of $\operatorname{disc} L/K$ at $\mathfrak{p}$ is greater than 16 by Lemma 1.38, meaning that $v_2(\operatorname{disc} L) \geq 16 v_2(\operatorname{disc} K) + 16$. As $v_2(\operatorname{disc} K) \leq 8$, we get that $v_2(\operatorname{disc} L) \geq 18 v_2(\operatorname{disc} K)$. This proves the following:

Lemma 5.3. *Let L be a number field with Galois group isomorphic to Q_{64} and let K be its subfield with Galois group $C_2 \times C_2$. Then $|\operatorname{disc} K| \leq \sqrt[18]{|\operatorname{disc} L|}$.*

This bound reduces the number of $C_2 \times C_2$ extensions that we have to compute. Furthermore, before extending these fields, we check if they satisfy the bounds we have found above. For each field F with Galois group

C_2^2, we factor its discriminant as $\operatorname{disc} F = 2^k d$ with d odd. If $k \neq 0$, we check whether $d^8 2^{16} \operatorname{disc} F^{16} \leq B$; if not we can discard the field. In the case $k = 0$, we check if $\operatorname{disc} F^{24} \leq B$ and discard F if it does not satisfy the condition.
As a result, we found the two minimal fields as extensions of the biquadratic field $\mathbf{Q}(\sqrt{31}, \sqrt{2})$ defined by the polynomial $f = x^4 - 32x^2 + 225$. Denote by $\mathbf{Q}(\alpha)$ the number field $\mathbf{Q}[x]/f$. Then their defining polynomials over $\mathbf{Q}(\alpha)$ are the following:

$$\begin{gathered}
y^{16} + (16\alpha^2 + 240)y^{14} + (-248\alpha^3/5 + 6448\alpha^2 + 4216\alpha/5 - 5952)y^{12} + \\
(-13888\alpha^3 + 970176\alpha^2 + 222208\alpha - 5743680)y^{10} + \\
(-23763608\alpha^3/15 + 68699968\alpha^2 + 332021656\alpha/15 - 550007208)y^8 + \\
(-1537000336\alpha^3/15 + 2427747392\alpha^2 + 18772512272\alpha/15 - 21822572512)y^6 + \\
(-52710527104\alpha^3/15 + 41090607136\alpha^2 + 593740826528\alpha/15 - 389385052960)y^4 + \\
(-49034556032\alpha^3 + 294188269952\alpha^2 + 533709816576\alpha - 2862393638336)y^2 + \\
(-2243251902941\alpha^3/15 + 702068052368\alpha^2 + 24370682075917\alpha/15 - 6956525366852)
\end{gathered}$$

and

$$\begin{gathered}
y^{16} + (-32\alpha^3/15 - 16\alpha^2 + 1504\alpha/15 - 240)y^{14} + \\
(-496\alpha^3/5 + 6448\alpha^2 - 105648\alpha/5 + 13888)y^{12} + \\
(670592\alpha^3/5 - 1176512\alpha^2 + 4769536\alpha/5 + 4370752)y^{10} + \\
(-263913664\alpha^3/15 + 106893952\alpha^2 + 1005713408\alpha/15 - 733573584)y^8 + \\
(4586230272\alpha^3/5 - 4844116544\alpha^2 - 33470230784\alpha/5 + 41198023872)y^6 + \\
(-21487652480\alpha^3 + 106355299968\alpha^2 + 189499359360\alpha - 997290189184)y^4 + \\
(1136820746752\alpha^3/5 - 1086890077440\alpha^2 - 10943289616384\alpha/5 + 10746091309312)y^2 + \\
(-13262655528328\alpha^3/15 + 4143757457152\alpha^2 + 133966525148936\alpha/15 - 42282130831936).
\end{gathered}$$

$(64, 82)$ Let L be a field with Galois group isomorphic to the group with identifier $(64, 82)$ and let K be its subfield with Galois group isomorphic to C_2^3. We now apply the same technique as above. By Lemma 4.30, we have that $v_p(\operatorname{disc} L) = 12 v_p(\operatorname{disc} K)$ for all the primes ramified in K different from 2, since the ramification index must be 4. For the prime number 2, let $\mathfrak{p}$ be a prime ideal of K lying over 2. Then $\mathfrak{p}^2$ divides the conductor of L/K, meaning that $\mathfrak{p}^8$ divides $\operatorname{disc} L/K$. As the ramification index of $\mathfrak{p}$ over $\mathbf{Q}$ is at most 4 and using the fact that the conductor must be invariant under Galois action, we get that $N_{K/\mathbf{Q}}(\operatorname{disc} L/K) \geq 16$. Since $v_2(\operatorname{disc} K) \leq 16$, we have proven the following:

Lemma 5.4. *Let L be a number field with Galois group isomorphic to the group with identifier $(64, 82)$ and let K be its subfield with Galois group isomorphic to C_2^3. Then $|\operatorname{disc} L| \geq |\operatorname{disc} K|^9$.*

Thus, we compute all the C_2^3-fields up to $\sqrt[9]{B}$. However, we know the exact valuation of an extension with the correct Galois group at the tamely ramified primes. For each field F with Galois group C_2^3 that we compute, we factor its discriminant as $\operatorname{disc} F = 2^k d$ with d odd. If $k \neq 0$, we check whether $2^8 d^4 \operatorname{disc} F^8 \leq B$; if not we can discard the field. If $k = 0$, we check if $\operatorname{disc} F^{12} \leq B$. As a result, we found the two minimal fields as extensions of the field $\mathbf{Q}(\sqrt{13}, \sqrt{17}, \sqrt{53})$ defined by $f = x^8 - 12x^7 - 20x^6 + 558x^5 - 769x^4 - 4890x^3 + 6796x^2 + 10608x - 14144$. Their defining polynomials over $\mathbf{Q}(\alpha) = \mathbf{Q}[x]/f$ are

$$\begin{gathered}
y^8 + (29\alpha^7/12780 + \alpha^6/852 - 715\alpha^5/2556 + 61\alpha^4/852 + 46957\alpha^3/6390- \\
5389\alpha^2/710 - 14926\alpha/639 + 7874/213)y^7 + (2233\alpha^7/51120 - 11117\alpha^6/17040+ \\
2051\alpha^5/51120 + 100121\alpha^4/3408 - 185042\alpha^3/3195 - 59863\alpha^2/284 + 898123\alpha/6390+ \\
435284/1065)y^6 + (2767\alpha^7/12780 - 43\alpha^6/17040 - 1532959\alpha^5/51120 + 51835\alpha^4/1136+ \\
44130043\alpha^3/51120 - 17898883\alpha^2/8520 - 41525863\alpha/12780 + 7731709/1065)y^5+ \\
(47977\alpha^7/6390 - 498161\alpha^6/5112 - 1582003\alpha^5/25560 + 21379415\alpha^4/5112- \\
217436537\alpha^3/25560 - 308396267\alpha^2/12780 + 97478884\alpha/3195 + 94498988/3195)y^4+ \\
(233723\alpha^7/8520 - 5365151\alpha^6/25560 - 15623033\alpha^5/8520 + 63114883\alpha^4/5112+ \\
129899009\alpha^3/4260 - 1163289167\alpha^2/6390 - 26878128\alpha/355 + 1404641974/3195)y^3+ \\
(2708083\alpha^7/5112 - 133532983\alpha^6/25560 - 481063217\alpha^5/25560 + 1185770537\alpha^4/5112- \\
73655617\alpha^3/2556 - 22622131229\alpha^2/12780 - 159083596\alpha/3195 + 12290575937/3195)y^2+ \\
(105424577\alpha^7/51120 - 1072183217\alpha^6/51120 - 731057983\alpha^5/10224 + 9764049301\alpha^4/10224- \\
6832993409\alpha^3/25560 - 100360111817\alpha^2/12780 + 11555071276\alpha/3195 + 7405207684/639)y+ \\
(-453082901\alpha^7/51120 + 2569941779\alpha^6/17040 - 18649193233\alpha^5/51120- \\
6097164409\alpha^4/1136 + 744532473077\alpha^3/25560- \\
1689852364\alpha^2/213 - 513763253029\alpha/3195 + 214044733288/1065)
\end{gathered}$$

and

$$\begin{gathered}
y^8 + (-217\alpha^7/25560 + 401\alpha^6/6390 + 671\alpha^5/1278 - 8207\alpha^4/2556 - 213607\alpha^3/25560+ \\
101801\alpha^2/2556 + 214267\alpha/6390 - 62552/639)y^7 + (-3313\alpha^7/51120 + 32479\alpha^6/51120+ \\
155413\alpha^5/51120 - 347183\alpha^4/10224 - 177311\alpha^3/6390 + 1405618\alpha^2/3195+ \\
1012067\alpha/6390 - 3833914/3195)y^6 + (4471\alpha^7/4260 - 57443\alpha^6/6390 - 259753\alpha^5/4260+ \\
635671\alpha^4/1278 + 1959253\alpha^3/2130 - 4418606\alpha^2/639 - 1402311\alpha/355+ \\
58704418/3195)y^5 + (466667\alpha^7/51120 - 590983\alpha^6/6390 - 2725867\alpha^5/6390+ \\
25932227\alpha^4/5112 + 202531817\alpha^3/51120 - 347257715\alpha^2/5112 - 247733741\alpha/12780+ \\
560716313/3195)y^4 + (-5706373\alpha^7/51120 + 6488751\alpha^6/5680 + 225551317\alpha^5/51120- \\
193303333\alpha^4/3408 - 180621877\alpha^3/12780 + 1304328437\alpha^2/2130 + 95469133\alpha/1278- \\
518404814/355)y^3 + (-4379137\alpha^7/6390 + 7936913\alpha^6/1136 + 1479810611\alpha^5/51120- \\
1230176261\alpha^4/3408 - 8261679131\alpha^3/51120 + 36453457363\alpha^2/8520 + 8579121509\alpha/12780- \\
3699025197/355)y^2 + (25819283\alpha^7/6390 - 1141199449\alpha^6/25560 - 3020599709\alpha^5/25560+ \\
10622558099\alpha^4/5112 - 29612370223\alpha^3/25560 - 46845914569\alpha^2/2556 + 23937278287\alpha/6390+ \\
122680128824/3195)y + (166154207\alpha^7/8520 - 5394327283\alpha^6/25560 - 5389497449\alpha^5/8520+ \\
51397326299\alpha^4/5112 - 4466240123\alpha^3/1420 - 306029998427\alpha^2/3195+ \\
11303383873\alpha/1065 + 664579764527/3195).
\end{gathered}$$

References

[1] V. Acciaro and J. Klüners. Computing local Artin maps, and solvability of norm equations. *J. Symbolic Comput.*, 30(3):239–252, 2000.

[2] A. A. Albert. On p-Adic Fields and Rational Division Algebras. *Ann. of Math.*, 41(3):674–693, 1940.

[3] E. Bach and J. Sorenson. Explicit bounds for primes in residue classes. *Math. Comp.*, 65(216):1717–1735, 1996.

[4] D. J. Bernstein. Factoring into coprimes in essentially linear time. *J. Algorithms*, 54(1):1 – 30, 2005.

[5] D. J. Bernstein, H. W. Lenstra, Jr., and J. Pila. Detecting perfect powers by factoring into coprimes. *Math. Comp.*, 76(257):385–388, 2007.

[6] H. U. Besche, B. Eick, and E. O'Brien. A millennium project: Constructing small groups. *IJAC*, 12:623–644, 2002.

[7] J.-F. Biasse and C. Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS J. Comput. Math.*, 17(suppl. A):385–403, 2014.

[8] J.-F. Biasse, C. Fieker, T. Hofmann, and A. Page. Norm relations and computational problems in number fields, 2020.

[9] W. Bley and R. Debeerst. Algorithmic proof of the epsilon constant conjecture. *Math. Comp.*, 82(284):2363–2387, 2013.

[10] K. S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original.

[11] J. A. Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41. Birkhäuser Boston, Boston, MA, 1990.

[12] J. A. Buchmann and H. W. Lenstra, Jr. Approximating rings of integers in number fields. *J. Théor. Nombres Bordeaux*, 6(2):221–260, 1994.

[13] L. M. Butler. Subgroup lattices and symmetric functions. *Mem. Amer. Math. Soc.*, 112(539):vi+160, 1994.

[14] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[15] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[16] H. Cohen and F. Diaz y Diaz. A polynomial reduction algorithm. *Sém. Théor. Nombres Bordeaux (2)*, 3(2):351–360, 1991.

[17] H. Cohen, F. Diaz y Diaz, and M. Olivier. Computing ray class groups, conductors and discriminants. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 49–57. Springer, Berlin, 1996.

[18] H. Cohen, F. Diaz y Diaz, and M. Olivier. Computing ray class groups, conductors and discriminants. *Math. Comp.*, 67(222):773–795, 1998.

[19] H. Cohen, F. Diaz y Diaz, and M. Olivier. A table of totally complex number fields of small discriminants. In J. P. Buhler, editor, *Algorithmic Number Theory*, pages 381–391, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[20] H. Cohen, F. Diaz y Diaz, and M. Olivier. Tables of octic fields with a quartic subfield. *Math. Comp.*, 68(228):1701–1716, 1999.

[21] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[22] H. Cohen and J. Martinet. Class groups of number fields: numerical heuristics. *Math. Comp.*, 48(177):123–137, 1987.

[23] L. El Fadil, J. Montes, and E. Nart. Newton polygons and p-integral bases of quartic number fields. *J. Algebra Appl.*, 11(4):1250073, 33, 2012.

[24] C. Fieker. Computing class fields via the Artin map. *Math. Comp.*, 70(235):1293–1303, 2001.

[25] C. Fieker, W. Hart, T. Hofmann, and F. Johansson. Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, page 157–164, New York, NY, USA, 2017. Association for Computing Machinery.

[26] C. Fieker, T. Hofmann, and C. Sircana. On the construction of class fields. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 239–255. Math. Sci. Publ., Berkeley, CA, 2019.

[27] C. Fieker and J. Klüners. Minimal discriminants for fields with small Frobenius groups as Galois groups. *J. Number Theory*, 99(2):318–337, 2003.

[28] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.0*, 2020.

[29] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[30] K. Grant and J. Leitzel. Norm limitation theorem of class field theory. *J. Reine Angew. Math.*, 238:105–111, 1969.

[31] G.-M. Greuel and G. Pfister. *A Singular introduction to commutative algebra*. Springer, Berlin, extended edition, 2008.

[32] J. Guàrdia, J. Montes, and E. Nart. Higher Newton polygons and integral bases. *J. Number Theory*, 147:549–589, 2015.

[33] A. Gélin and A. Joux. Reducing number field defining polynomials: an application to class group computations. *LMS J. Comput. Math.*, 19(A):315–331, 2016.

[34] D. F. Holt, B. Eick, and E. A. O'Brien. *Handbook of computational group theory*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[35] G. J. Janusz. Crossed product orders and the Schur index. *Comm. Algebra*, 8(7):697–706, 1980.

[36] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[37] J. W. Jones. Minimal solvable nonic fields. *LMS J. Comput. Math.*, 16:130–138, 2013.

[38] J. W. Jones and D. P. Roberts. Galois number fields with small root discriminant. *J. Number Theory*, 122(2):379–407, 2007.

[39] J. W. Jones and D. P. Roberts. A database of number fields. *LMS J. Comput. Math.*, 17(1):595–618, 2014.

[40] J. W. Jones and D. P. Roberts. Mixed degree number field computations. *Ramanujan J.*, 47(1):47–66, 2018.

[41] J. Klüners and G. Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4:182–196, 2001.

[42] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[43] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[44] A. Ledet. Embedding problems with cyclic kernel of order 4. *Israel J. Math.*, 106(1):109–131, Dec 1998.

[45] A. Ledet. *Brauer type embedding problems*, volume 21 of *Fields Institute Monographs*. American Mathematical Society, Providence, RI, 2005.

[46] T. LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2020.

[47] G. Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[48] G. Malle. On the distribution of class groups of number fields. *Experiment. Math.*, 19(4):465–474, 2010.

[49] G. Malle and B. H. Matzat. *Inverse Galois theory*. Springer Monographs in Mathematics. Springer, Berlin, 2018. Second edition.

[50] D. A. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, 1977. Universitext.

[51] 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. Birkhäuser Boston, Boston, MA, 1985.

[52] 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.

[53] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[54] A. M. Odlyzko. Lower bounds for discriminants of number fields, ii. *Tohoku Math. J. (2)*, 29(2):209–216, 1977.

[55] R. A. Parker. The computer calculation of modular characters (the meat-axe). In *Computational group theory (Durham, 1982)*, pages 267–274. Academic Press, London, 1984.

[56] 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.

[57] T. Preu. Effective lifting of 2-cocycles for Galois cohomology. *Cent. Eur. J. Math.*, 11(12):2138–2149, 2013.

[58] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series.* The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[59] J.-P. Serre. Local class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 128–161. Thompson, Washington, D.C., 1967.

[60] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[61] J.-P. Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics.* A K Peters, Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon.

[62] H. D. Stainsby. Triangular bases of integral closures. *J. Symbolic Comput.*, 87:140–175, 2018.

[63] J. T. Tate. Global class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 162–203. Thompson, Washington, D.C., 1967.

[64] C. Thiel. *On the complexity of some problems in algorithmic algebraic number theory.* PhD thesis, Universität des Saarlandes, 1995.

[65] J. Voight. Enumeration of totally real number fields of bounded root discriminant. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 268–281. Springer, Berlin, 2008.

[66] I. R. Šafarevič. Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 18:525–578, 1954.

Acknowledgments

I would like to thank my supervisor Prof. Dr. Claus Fieker for his guidance during these years and for the various challenging tasks he assigned me during my work. They have helped me in my growth and made the PhD stimulating, interesting and enjoyable. I am also grateful to Dr. Tommy Hofmann, for his assistance and collaborations throughout my PhD and the hours spent together in front of a screen searching for bugs in my code. I would like to thank Prof. Dr. Jürgen Klüners, for his willingness to serve as a second supervisor and some interesting ideas he shared with me during his visit in Kaiserslautern.

I want to express my gratitude to everyone I met in Kaiserslautern who spent some time with me: people with whom I shared the office, the "Movies" group, "Malle's group" and the number theory group. I've enjoyed all the activities we did together, that I would have probably never tried without you: I will always remember these experiences.

Finally, I thank Agnese and my family for their unconditional support, the help and the understanding they have shown when I moved to Kaiserslautern and during this time.

Curriculum Vitae

Education

Since 02/2017	Doctoral researcher at the Department of Mathematics, TUK, Advisor: Prof. Dr. Claus Fieker
09/2014 - 09/2016	Laurea magistrale in Matematica - Università di Pisa
09/2011 - 09/2014	Laurea triennale in Matematica - Università di Pisa
07/2011	Diploma Liceo Scientifico - Liceo Mossa, Olbia

Employment

Since 02/2017	Research Assistant in the Collaborative Research Center TRR 195 “Symbolic Tools in Mathematics and their Application”

Wissenschaftlicher Werdegang

Ausbildung

Seit 02/2017	Doktorand am Fachbereich Mathematik der TUK, Advisor: Prof. Dr. Claus Fieker
09/2014 - 09/2016	Laurea magistrale in Matematica - Università di Pisa
09/2011 - 09/2014	Laurea triennale in Matematica - Università di Pisa
07/2011	Diploma Liceo Scientifico - Liceo Mossa, Olbia

Beschäftigung

Seit 02/2017	Wissenshaftlicher Mitarbeiter in Sonderforschungsbereich TRR 195 “Symbolische Werkzeuge in der Mathematik und ihre Anwendung"